Systems Reliability for Phased Missions

By

Rachel La Band

A Doctoral Thesis

Submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy of Loughborough University

March 2005

In Memory of my Dad

Abstract

The concept of a phased mission has been introduced as a sequential set of objectives that operate over different time intervals. During each phase of the mission, the system may alter such that the logic model, system configuration, or system failure characteristics may change to accomplish a required objective.

A new fault tree method has been proposed to enable the probability of failure in each phase to be determined in addition to the whole mission unreliability. Phase changes are assumed to be instantaneous, and component failure rates are assumed to be constant through the mission. For any phase, the method combines the causes of success of previous phases with the causes of failure for the phase being considered to allow both qualitative and quantitative analysis of both phase and mission failure. A new set of Boolean laws is introduced to combine component success and failure events through multiple phases so that the expression for each phase failure can be reduced into minimal form.

The binary decision diagram (BDD) method offers an alternative approach to the fault tree method and reduces the complexity of the problem. For larger fault trees it is more efficient to convert to a BDD prior to analysis, and this is particularly true of the non-coherent phase failure fault trees. The standard BDD technique has been extended to develop a method for use in missions of multiple phases.

Markov methods are considered for the analysis of phased missions where repair of components is possible. A full Markov model is generated by using a single model which works over all phases of the mission, and is constructed by the inclusion of all components featured in every stage. By identifying certain types of phases and components, it is possible to reduce this full Markov model further.

The phases of a mission may be characterised in certain ways. If a phase requires the relevant system function to work at an instant in time it is defined as discrete, and no state transitions may occur during the phase. A continuous phase requires the appropriate system configuration to be reliable for the specified phase duration.

The concept of sequential failure relationships has been introduced to missions of multiple phases. Component failures can be identified as initiating or enabling events, and the function of a component is subject to change through the mission duration. A maintenance policy is considered where components can be subject to scheduled inspection.

Later sections of the thesis consider appropriate importance measures for phase and mission reliability.

Acknowledgements

Firstly I would like to thank my supervisor Professor John Andrews for his guidance, support, and above all belief in me throughout the course of my Ph.D.

Thanks must also be extended to my sponsor Richard Denning for his contributions to this research and also to the MoD for the financial support to make the work possible.

Thanks also to the members of the Aeronautical and Automotive department, particularly Jeni who I have shared an office with for the last three years and has made the whole experience more enjoyable.

I would also like to thank my stepdad, Philip, who has cared for me as a daughter, and my sister, Sophie, for their continuous support. Also to my partner, Phil, for his love and encouragement through the past years, and to my friend Kerry for making me smile every day.

Finally, a special thank you to my mum, Sue, for giving me every opportunity to succeed and being there for me endlessly.

Contents

Appendices

Nomenclature

$a_c(t)$	Availability of component *c*
$A(t)$	Availability function
[A]	State transition matrix
c_{ij}	Event that component *c* fails in any phase from *i* to *j* inclusive
$\overline{c_{ij}}$	Event that component *c* works through phase *i* to *j* inclusive
C	Consequence of an event
C_i	Existence of minimal cut set *i*
C_{i_j}	Existence of minimal cut set *i* in phase *j*
D_l	Path set *l*
$f(t)$	Failure probability density function (p.d.f)
$F_{SYS}(t)$	System unreliability function
$g(t)$	Repair probability density function (p.d.f)
$G_c(\boldsymbol{q})$	Criticality function for event *c* (Birnbaum's measure of importance)
$G_{c_j}(\boldsymbol{q})$	Criticality function for event *c* in phase *j*
$h(t)$	Conditional failure rate (hazard rate)
I_c^{CR}	Criticality measure of component importance
$I_{c_j}^{CR}$	Criticality measure of phase *j* component importance
$I_{c_{MISS}}^{CR}$	Criticality measure of mission component importance
I_c^{FV}	Fussell-Vesely measure of component importance
$I_{c_j}^{FV}$	Measure of phase *j* component importance
$I_{c_{MISS}}^{FV}$	Measure of mission component importance
$I_{C_k}^{FV}$	Fussell-Vesely measure of minimal cut set importance
$I_{\varepsilon_{k_j}}^{FV}$	Measure of phase *j* prime implicant set importance
$I_{\varepsilon_{k_{MISS}}}^{FV}$	Measure of mission prime implicant set importance
I_c^{ST}	Structural measure of component importance
$I_{c_j}^{ST}$	Structural measure of phase *j* component importance

I_e^{DL}	Component enabler importance
$I_{e_j}^{DL}$	Component enabler phase *j* importance
$I_{e_{MISS}}^{DL}$	Component enabler mission importance
I_i^{BP}	Barlow-Proschan measure of initiator importance
$I_{i_j}^{BP}$	Measure of phase *j* initiator importance
$I_{i_{MISS}}^{BP}$	Measure of mission initiator importance
K_i	Existence of prime implicant set *i*
K_{i_j}	Existence of prime implicant set *i* in phase *j*
m	Number of phases in mission
N_c	Total number of components
N_{c_j}	Number of components in phase *j*
N_{C_i}	Number of components in cut set C_i
$N_{C_{i_j}}$	Number of components in cut set C_i in phase *j*
N_{mcs}	Number of minimal cut sets
N_{mcs_j}	Number of minimal cut sets in phase *j*
N_{mps_j}	Number of minimal path sets in phase *j*
N_{pi_j}	Number of prime implicant sets in phase *j*
N_S	Total number of system states
$N_{S\,cont}$	Total number of continuous phase system states
$N_{S\,j}$	Total number of phase *j* system states
NPS	Non-Phase Specific
P	Probability
$[\mathbf{P}]$	State probability vector
$P(C_i)$	Probability of existence of minimal cut set *i*
$P(K_i)$	Probability of existence of prime implicant set *i*
$P(\varepsilon_i)$	Probability of occurrence of prime implicant set *i*
$P(\theta_i)$	Probability of occurrence of minimal cut set *i*
$p_c(t)$	Component reliability (success probability)

p_{c_j}	Component phase *j* reliability (success probability)
$p_{C_{i_j}}$	Cut set C_i phase *j* reliability (success probability)
$P_{S_i}(t)$	Probability that the system is in state S_i at time *t*
$P_{S_{i_j}}(t)$	Probability that the system is in state S_i at time *t* in phase *j*
PS	Phase Specific
$q_c(t)$	Component unavailability (failure probability)
q_{c_j}	Component phase *j* unavailability (failure probability)
$q_{c_{ij}}$	Component *c* unavailability through phases *i* to *j* inclusive
q_{C_i}	Minimal cut set unavailability
$q_{C_{i_j}}$	Minimal cut set unavailability in phase *j*
$Q_{SYS}(t)$	System unavailability function
Q_{IN-EX}	Minimal unreliability bound using the inclusion-exclusion expansion
$Q_{IN-EX(CC)}$	Q_{IN-EX} with cut set cancellation technique
Q_j	Phase *j* unavailability (failure probability)
Q_{MCB}	Minimal unreliability bound using the minimal cut set bound to estimate phase unreliability
$Q_{MCB(CC)}$	Q_{MCB} with cut set cancellation technique
Q_{MCSU}	Minimal cut set upper bound
Q_{MISS}	Mission unavailability (failure probability)
$Q_{SYS}(t)$	System, or top event, unavailability function (failure probability)
R	Risk
$R_{SYS}(t)$	System reliability function
R_j	Phase *j* reliability (success probability)
R_{MISS}	Mission reliability (success probability)
S_n	State *n*
t_{j-1}	Start of phase *j*
t_j	End of phase *j*
T_j	Top event of phase *j*

$Tr(t_{j-1})$	Transition failure probability into phase *j*
$w_{SYS}(t)$	System unconditional failure intensity
$w_c(t)$	Component unconditional failure intensity
$w_j(t)$	Phase *j* unconditional failure intensity
$w_{\theta_i}(t)$	Minimal cut set *i* unconditional failure intensity
$w_{SYS_{MAX}}(t)$	Upper bound for system unconditional failure intensity
$W_{SYS}(0,t)$	Expected number of system failures (top event occurrences) in [0,*t*)
$W_j^{Tr}(t_{j-1})$	Expected number of phase *j* transition failures
$W_j^{I-p}(t_{j-1},t_j)$	Expected number of failures in phase *j*
$W_j(t_{j-1},t_j)$	Total expected number of phase *j* failures
$W_{MISS}(0,t_m)$	Expected number of mission failures in [0,t_m)
x_c	Binary indicator variable for component states
x_{c_j}	Binary indicator variable for component states in phase *j*
λ_c	Component conditional failure rate
λ_{MISS}	Mission frequency
υ_c	Component conditional repair rate
ε_i	Occurrence of prime implicant set *i*
ε_{i_j}	Occurrence of prime implicant set *i* in phase *j*
θ_i	Occurrence of minimal cut set *i*
θ_{i_j}	Occurrence of minimal cut set *i* in phase *j*
$\rho_i(\mathbf{x})$	Binary indicator function for each minimal cut set
τ	Time step in iterative algorithms
$\phi(\mathbf{x})$	Structure function
$\phi_j(\mathbf{x})$	Phase *j* structure function

Chapter 1 Introduction

1.1 Introduction to Risk and Reliability Assessment

The catastrophic consequences due to the failure of systems in industries such as aeronautical, nuclear, offshore, and transport demonstrate the requirement for improved methods of ensuring the reliability and safety of complex systems. Examples of such eventualities are the fire and explosion on the Piper Alpha oil platform in 1988 and the Chernobyl nuclear power plant disaster in 1986, both of which caused multiple fatalities. System assessments applied in a systematic way at the design stage can reduce the possibility of undesirable incidents occurring in the future when the system is operational.

Methods to assess the risk and reliability of systems have been developed over a number of years, with significant advances made since the Second World War. Such methods enable the evaluation of the probability or frequency by which a hazardous event could occur (accounting if necessary for the safety systems failure to respond). The risk, or 'expected loss' of a specific incident, R, is defined as the product of the consequences of the event, C, and the probability or frequency of the event occurrence, P, in equation (1.1).

$$R = C \times P \tag{1.1}$$

For safety studies, the consequence is generally measured by the number of resulting fatalities. The risk can therefore be reduced by reducing either the consequences of the incident or the associated incident probability or frequency. The risk assessment will compare the predicted risk with an acceptable level.

In assessing the adequacy of engineering systems, the Health and Safety Executive (HSE) assume a three-zone approach to define the acceptable level of risk. The highest zone denotes the unacceptable risk levels, where either the consequences of the incident or the associated incident probability or frequency must be reduced to bring the risk into an acceptable level. The lowest zone represents negligible risk levels that are considered to be acceptable. The intermediate zone is defined as the

‘ALARP’ region (As Low As Reasonably Practicable). In this case the risks must be shown to be as low as possible, whilst still being economically feasible.

To determine the zone for a specific hazard requires a quantified risk assessment. This is defined in four basic stages:

1. Identification of the potential safety hazards.
2. Estimation of the consequences of each hazard.
3. Estimation of the probability of occurrence of each hazard.
4. Comparison of the results of the analysis against the acceptability criteria.

The consequences of an equipment failure are generally measured in terms of cost or the number of fatalities. Such consequences can be extremely severe, and are very much dependent on the failure mode and industry involved. Reliability assessment techniques considering the probability or frequency of system failure occurrence are generic and thus are extensively implemented within many industries. Examples of such methods are Failure Mode and Effect Analysis (FMEA), Event Tree Analysis (ETA), Fault Tree Analysis (FTA), and Markov Analysis.

1.2 System Failure Quantification

The reliability performance of a system can be predicted in terms of the reliability performance of its components using suitable techniques. The performance of a system or component is described by the quantification of system and component failure probabilities, using the parameters defined below.

Where failure is tolerated and repair is possible, an appropriate performance measure is the *availability* of a system or component. This is defined as:

> The fraction of the total time that a system (or component) is able to perform its required function.

This parameter can also be defined at a specified time point t as:

> The probability that a system or component is working at time t.

The complement of availability is unavailability, where:

$$\text{Unavailability} = 1 - \text{Availability}$$

The unavailability of a system or component is the probability that the system or component does not work at time *t*, and is denoted by $Q_{SYS}(t)$ for a system and $q_c(t)$ for a component *c*.

The *reliability* of a system or component is the probability of the successful performance of the system or component over a period of time, and is defined by:

> The probability that a system or component will operate without failure for a stated period of time under specified conditions.

The probability that a component or system fails to function successfully over a specified time period under particular conditions is defined as its unreliability, $F(t)$, where:

$$\text{Unreliability} = 1 - \text{Reliability}$$

This parameter is generally more relevant for systems where failure cannot be tolerated and so the system or component is required to function successfully for a specified time duration. If a component or system is non-repairable and is known to be working at time *t*, it must have worked continuously over [0,*t*). In this case the unreliability is equal to the unavailability.

The transition to a failed state of a component or system can be characterised by the hazard rate or conditional failure rate, *h*(*t*). This is a measure of the rate at which failures occur given successful operation to this point in time, i.e. still functioning at time *t* with the potential to fail, and is defined as:

> The probability that a component or system fails in the interval [*t*, *t* + *dt*) given that it has not failed in [0,*t*).

The reliability characteristics of a component family are usually modelled by a 'reliability bath-tub curve', illustrated in Figure 1.1.

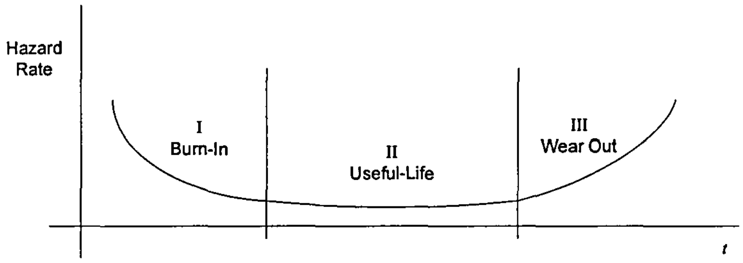


Figure 1.1 Reliability Bath-Tub Curve

In the first phase of Figure 1.1, the hazard rate (failure rate) reduces as the weak components are eliminated. In the second phase, the hazard rate remains approximately constant and this is classed as the useful life of the components. In the final phase, the hazard rate increases as the components start to wear out. Reliability assessment is typically performed on components that are considered to be in their useful-life phase. The reliability of a system, $R_{SYS}(t)$, can be expressed in terms of its constant hazard or failure rate λ by the expression in equation (1.2).

$$R_{SYS}(t) = e^{-\lambda t} \tag{1.2}$$

Further component and system quantification techniques are presented in [1] and [2]. Reliability assessment tools can be applied to evaluate the reliability parameters of a system in terms of the reliability performance of its constituent components. Some of the most common are discussed in the following sections.

1.3 Fault Tree Analysis

The concept of fault tree analysis was first introduced by H.A. Watson in the 1960's, presenting a deductive analysis method of identifying the causes of a particular system failure mode using a 'what can cause this' approach. A fault tree provides a visual symbolic representation of the combination of component failure events resulting in the occurrence of a particular system failure mode. Analysis of the fault tree is a logical, structured process that provides information on the causes of system failure and associated reliability parameters.

The system failure mode of concern is termed the *top event* of the fault tree, with branches below this determining its causes. Events within the fault tree are continually redefined in terms of their causes until component failure events (*basic events*) are reached. The probability of the top event occurrence can then be calculated by the probability of the basic events. This is an example of a 'top-down' approach, in comparison to 'bottom-down' approaches such as FMEA which begin with a set of component failure conditions and implement a 'what happens if' approach to identify possible consequences.

The quantitative analysis of a fault tree is defined as Kinetic Tree Theory, and was developed in the early 1970's by Vesely [3]. This allowed calculations of parameters such as the probability and frequency of top event occurrence to be made in order to determine the risks involved with system failure. The disadvantage involved with fault tree quantification is that for large fault trees the analysis can become computationally demanding. Approximations are often used to quantify large fault trees, however the results will show inaccuracies. A new method has been developed to analyse a fault tree, the Binary Decision Diagram technique.

1.4 Binary Decision Diagrams

The Binary Decision Diagram (BDD) technique does not analyse the fault tree directly, but constructs a BDD to provide an efficient representation of the system with a Boolean equation for the top event. A BDD is a directed acyclic graph, and is dependent on the order in which the basic events of the fault tree are considered. Qualitative and quantitative analysis can be performed on a BDD, and exact solutions can be obtained without the need for approximations of the conventional fault tree approach. The use of BDDs in reliability analysis was initially developed by Rauzy [4].

1.5 Markov Methods

The kinetic tree theory requires the assumption that the basic events in a fault tree are statistically independent. In many cases this assumption cannot be made, such as in systems where standby redundancy, common cause failures, secondary failures, or multiple-component states are possible.

Markov analysis provides a means of analysing the reliability and availability of systems whose components exhibit strong dependencies. The Markov method is a state-space approach. The likelihood of any event in the chain is determined only by the immediately preceding state and is independent of any other past events. A Markov model can be discrete or continuous in both time and space. The disadvantage of this method is that the model can increase rapidly with the number of components.

1.6 Phased Mission Systems

If the success of a system is reliant upon a sequential set of objectives operating over different time intervals, it may be referred to as a *Phased Mission.* During the execution of the phases in a mission, the system is altered such that the logic model, system configuration, or system failure characteristics may change to accomplish a different objective. The phases in a mission may be identified by; phase number, time interval, system configuration, task(s) to be undertaken, performance measure(s) of interest, or maintenance policy.

A multi-phased mission can be characterized as a sequence of discrete events required to complete a task. Many types of system operate for missions which are made up of several phases. For the complete mission to be a success, the system must operate successfully during each of the phases. Examples of such systems include an aircraft flight, and also many military operations for both aircraft and ships. An aircraft mission could be considered as the following phases: taxiing to the runway, take-off, climbing to the correct altitude, cruising, descending, landing and taxiing back to the terminal in Figure 1.2.

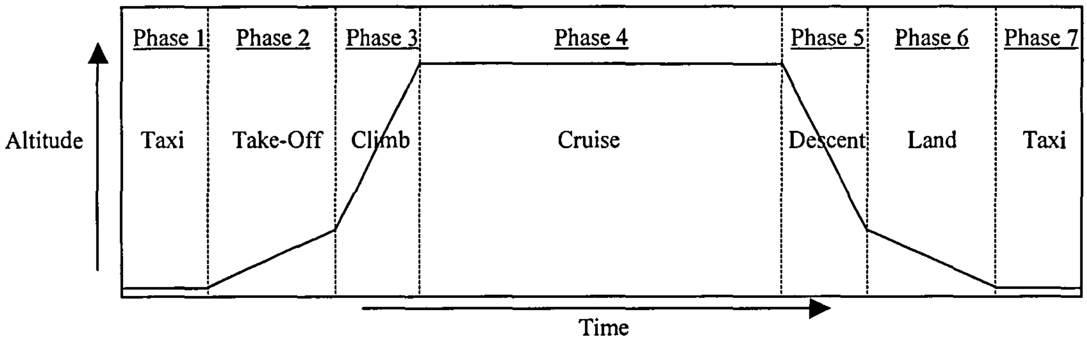


Figure 1.2 Transport phases of an aircraft

Component failures can occur at any point during the mission but their condition may only be critical for one particular phase. As such it may be that the transition from one phase to another is the critical event leading to mission failure, the component failures resulting in the system failure may have occurred during some previous phase.

The reliability of a mission may not be obtained by the simple multiplication of the individual phase reliabilities. This is due to the fact that at the phase change times, the system must occupy a state that allows both of the involved phases to function. The phases of the mission will be statistically dependent. In order to identify possible causes of phase and mission failure, a method is required to express how combinations of component failures (basic events) can occur during the phases throughout the mission and cause system failure. These failure events then require quantification to enable the likelihood and frequency of mission failure to be determined. Mission unreliability is defined as the probability that the system fails to function successfully during at least one phase of the mission. An important problem is to calculate, as efficiently as possible, the exact value for the mission unreliability parameter.

The main techniques that have previously been implemented for the solution to phased mission problems are that of fault tree analysis, Markov analysis and simulation. Fault tree analysis is a commonly used tool to assess the probability of failure of industrial systems. This method may be adapted for analysis of systems comprising of more than one phase, where each phase depends on a different logic model. Hence the complexity of the modelling is significantly more difficult than for single phase systems. Situations may be encountered in phased mission analysis that prevent the assumption of independence between component failure or repair being made. In such circumstances, methods such as the Markov approach must be employed. In some cases it will be difficult to model a system by fault tree or Markov methods. This type of situation will occur if a system is too complex to use deterministic analysis, or if the failure and repair distributions of a component do not have a constant failure or repair rate. In such circumstances, simulation may be necessary. Of the many considered solutions to phased mission problems, simulation techniques typically offer the greatest generality in representation, but are also often the most expensive in computational requirements.

1.7 Research Objectives

The aim of this research is to consider analytical techniques for the efficient representation and solution of phased mission systems. Two distinct types of system will be examined. The first comprises of only non-repairable components and explores the possible methods for the representation of both phase and mission unavailability. The second type of system considers the possibility of repairable components in some or all phases of the mission with added dependencies. Previous work has concentrated on the object of assessing mission success. The presented methods will focus on the probability of success and failure in individual phases, where depending on the phase that the failure occurs, the consequences can be significantly different. The objectives of the project are listed below:

Non-Repairable Systems:

- Review of existing methods for non-repairable phased mission systems.
- Present new techniques to identify the causes of phase and mission failure, and calculate exact phase and mission unavailability and frequency.
- Develop current importance measures to include the importance of components to both individual phase and mission failure in a multi-phased mission.

Repairable Systems:

- Review of existing methods for repairable phased mission systems.
- Present new techniques for calculating exact phase and mission unreliability for systems where some or all phases are repairable.
- Develop the proposed techniques to include the possibility of :
    - Initiating and enabling events.
    - Appropriate maintenance policies.
    - Discrete and continuous phases.

Chapter 2 Reliability Analysis Tools

2.1 Introduction

There are many methods that can be used to predict the reliability performance of a system in terms of the reliability performances of the components of which it is constructed. Three widely used techniques, fault tree analysis, binary decision diagrams, and Markov analysis are discussed in the following sections.

2.2 Fault Tree Analysis

A fault tree provides a visual symbolic representation of the combination of component failure events required for the occurrence of a particular system failure mode. Fault tree analysis is a logical, structured process that provides information on the causes of system failure and associated reliability parameters and thus is very important in the design stages of a system. The entire system as well as human interactions would be analysed by performing a fault tree analysis.

2.2.1 Construction of a Fault Tree

The first step in the construction of a fault tree is to identify the system failure mode of concern. A system may have the potential for more than one undesirable failure mode, and so multiple fault trees would be constructed. The *top event* is defined as a particular system failure mode, with fault tree branches below this determining its causes. Events within the tree are continually redefined in terms of lower resolution events as causes for their occurrence. This process continues until all branches of the fault tree terminate in component failure events, termed *basic events.* Fault tree analysis can then be executed using data on the basic event failure probabilities.

A fault tree comprises of symbols which represent events and gates. An event can be classed as intermediate or basic. The causes of an intermediate event can be expressed by other, lower resolution events, where as a basic event is the termination of a fault tree branch. Event symbols are shown in Table 2.1. Events are linked using a logical structure of gates. The three primary gate types used in fault trees are defined as

'AND', 'OR', and 'NOT' gates, which combine events in the same way as the Boolean operations of 'intersection', 'union', and 'complementation'. Another frequently used gate is the *k/n* vote gate which requires that at least *k* out of *n* inputs occur for the output to be true. The gates are symbolised in Table 2.2.

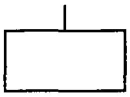
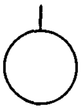
Event Symbols	Meaning of Symbol
	Intermediate event further developed by a gate
	Basic event

Table 2.1 Event Symbols

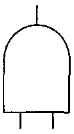
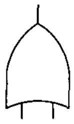
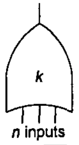
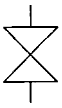
Gate Symbol	Gate Name	Casual Relation
	AND gate	Output event occurs if all input events occur simultaneously
	OR gate	Output event occurs if at least one of the input events occurs
	*k/n* vote gate	Output event occurs if at least *k* out of the *n* input events occur
	NOT gate	Output event occurs if the input event does not occur

Table 2.2 Gate Symbols

A system in which failure can only be caused by component failures and is made up of only 'AND' and 'OR' gates is defined as a *coherent* system. If the failure mode can be expressed by both component failures and successes, the use of 'NOT' gates is required and it is defined as a *non-coherent* system.

The analysis of a fault tree provides two types of result: qualitative and quantitative. Qualitative analysis identifies the combination of basic events that cause system failure. Quantitative analysis predicts system failure parameters in terms of basic event failure probabilities.

2.2.2 Qualitative Analysis

Qualitative analysis allows a system failure mode to be represented logically by combinations of basic events. Each combination of basic events that cause system failure is termed a *cut set*, defined as:

> A cut set is a collection of basic events such that if they all occur, the top event also occurs.

A cut set may contain unnecessary events for the occurrence of the system failure mode. For example, a cut set {A, B, C} would guarantee system failure if all events occur. However if A and B alone can cause system failure, the state of C becomes irrelevant. This defines a *minimal cut set*:

> A minimal cut set is the smallest combination of basic events, such that if any basic event is removed from the set, the top event will not occur.

Fault trees that produce identical minimal cut sets are logically equivalent. The order of a minimal cut set is the number of basic events which are contained in it. In general it is the lower order minimal cut sets that contribute most to system failure, and effort should be concentrated in the system design on the elimination of these. If NOT logic is used or implied in a fault tree, the combinations of basic events that cause system failure are defined as *implicants*. Minimal sets of implicants are termed *prime implicants*.

The minimal cut sets of a fault tree are determined using either a ‘top-down’ or ‘bottom-up’ approach to develop a Boolean logic expression in terms of component failure. The ‘top-down’ approach begins with the top event and continually substitutes Boolean events appearing lower down in the tree until the expression comprises of only basic events. The ‘bottom-up’ approach begins at the base of the tree and works towards the top event. The product, '·' is used to represent 'AND', and the sum, '+' is used to represent 'OR' in the logic expressions. This expansion technique results in a sum-of-products (s-o-p) expression from which the cut sets can be determined. To ensure that the cut sets obtained are minimal, the s-o-p expression must be made minimal by removing redundancies with laws of Boolean algebra.

2.2.2.1 Example – Obtaining the Minimal Cut Sets

The top-down approach for obtaining the minimal cut sets of a system is demonstrated using the example in Figure 2.1.

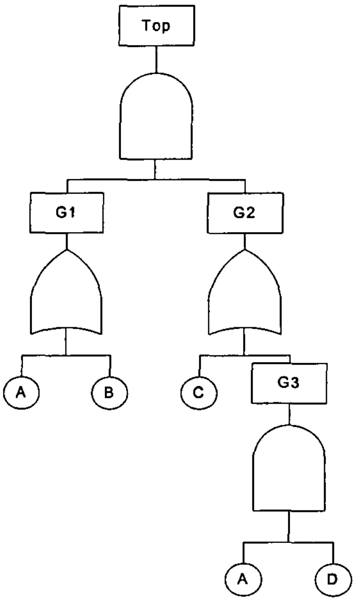


Figure 2.1 Example Fault Tree

The top-down approach begins with the event Top. This is an AND gate with two inputs, G1 and G2, and so can be expressed as the product of the inputs:

$$\text{Top} = \text{G1} \cdot \text{G2}$$

G1 is an OR gate and can be defined in terms of the two input events A and B:

$$\text{G1} = \text{A} + \text{B}$$

This may be substituted into Top to give:

$$\text{Top} = (\text{A} + \text{B}) \cdot \text{G2}$$

Similarly, G2 can be written as the 'sum' of C and G3:

$$G2 = C + G3$$

G2 can then also be substituted into Top:

$$Top = (A + B) \cdot (C + G3)$$

Finally G3 can be expressed as the 'product' of A and D:

$$G3 = A \cdot D$$

And the expression for the Top event becomes:

$$Top = (A + B) \cdot (C + A \cdot D)$$

Since this expression now only contains basic events, Top can be expanded to give:

$$\begin{aligned} Top &= A \cdot C + A \cdot A \cdot D + B \cdot C + B \cdot A \cdot D \\ &= A \cdot C + A \cdot D + B \cdot C + B \cdot A \cdot D \qquad \text{(since } A \cdot A = A\text{)} \end{aligned}$$

This gives the cut sets of the fault tree expressed in s-o-p form. Redundancies can be removed using the absorption law, and the minimal s-o-p expression for Top becomes:

$$Top = A \cdot C + A \cdot D + B \cdot C$$

This is the minimal s-o-p or disjunctive normal form of the logic equation, and each term represents a minimal cut set of the system. In this example there are three minimal cut sets of order two (i.e. contain two basic events). These are {A,C}, {A,D}, and {B,C}.

The minimal cut sets in this example are obtained easily. In some cases a complex system can produce thousands of minimal cut sets which becomes very computationally intensive to analyse. Approximations can be used where only minimal cut sets above a certain order or below a specified probability are removed during the calculation process. This reduces the accuracy of the minimal cut sets leading to further inaccuracies in the quantitative analysis.

2.2.3 Quantitative Analysis

Quantitative analysis of a fault tree provides predictions of the systems performance. Widely used parameters are the top event probability and frequency, along with the expected number of top event occurrences.

2.2.3.1 Top Event Probability

The probability of occurrence of the top event, also termed the *unavailability* of the system, can be directly obtained from the minimal cut sets. This method is known as the *inclusion-exclusion* expansion.

The probability of existence of a minimal cut set C_i is obtained by the product of the probabilities of existence of the events that contribute to the minimal cut set. For example, the probability of existence of C_i={A,B} is obtained by the failure probability of component A multiplied by the failure probability of component B. In general terms, the probability of existence of cut set C_i containing N_{C_i} events, $P(C_i)$, is expressed by equation (2.1).

$$P(C_i) = \prod_{c=1}^{N_{C_i}} q_c(t) \tag{2.1}$$

The top event will occur by the existence of any minimal cut set, C_i. For a system with N_{mcs} minimal cut sets, the system failure probability at time t, $Q_{SYS}(t)$, is given by equation (2.2).

$$Q_{SYS}(t) = P\left(\bigcup_{i=1}^{N_{mcs}} C_i\right) \tag{2.2}$$

This may be expanded as shown in equation (2.3).

$$Q_{SYS}(t) = \sum_{i=1}^{N_{mcs}} P(C_i) - \sum_{i=2}^{N_{mcs}} \sum_{j=1}^{i-1} P(C_i \cap C_j) + \cdots + (-1)^{N_{mcs}-1} P(C_1 \cap C_2 \cap \cdots \cap C_{N_{mcs}}) \tag{2.3}$$

In many cases the top event of a system is made up of a large number of minimal cut sets. In such cases obtaining the top event probability using the inclusion-exclusion expansion is not possible due to the number of calculations required. This is overcome by employing approximation techniques.

2.2.3.1.1 Upper and Lower Bounds for System Unavailability

The terms in equation (2.3) provide less significant contributions as more minimal cut sets are combined. This series can be truncated to give upper and lower bounds for the system unavailability, shown in equation (2.4).

$$\sum_{i=1}^{N_{mcs}} P(C_i) - \sum_{i=2}^{N_{mcs}}\sum_{j=1}^{i-1} P(C_i \cap C_j) \le Q_{SYS}(t) \le \sum_{i=1}^{N_{mcs}} P(C_i) \qquad (2.4)$$

Lower Bound Exact Upper Bound

The upper bound is also known as the *rare event approximation* since it is itself accurate if the component failure events are rare.

2.2.3.1.2 Minimal Cut Set Upper Bound

The *Minimal Cut Set Upper Bound, Q_{MCSU}*, is a more accurate upper bound of the system failure probability. This is derived below and results in equation (2.5).

$$\begin{aligned}\text{P(system failure)} &= \text{P(at least one minimal cut set exists)}\\ &= 1 - \text{P(no minimal cut sets exist)}\end{aligned}$$

Then,

$$\text{P(no minimal cut sets exist)} \ge \prod_{i=1}^{N_{mcs}} \text{P (minimal cut set } i \text{ does not exist)}$$

(equality being when no event appears in more than one minimal cut set)

So,

$$\text{P(system failure)} \le 1 - \prod_{i=1}^{N_{mcs}} \text{P (minimal cut set } i \text{ does not exist)}$$

$$Q_{MCSU} = 1 - \prod_{i=1}^{N_{mcs}} [1 - \text{P}(C_i)] \qquad (2.5)$$

2.2.3.2 Top Event Frequency

The system unconditional failure intensity, $w_{SYS}(t)$, is defined as the probability that the top event occurs at *t* per unit time. The probability that the top event occurs in the time interval [*t*, *t*+*dt*) is given by $w_{SYS}(t)\,dt$. For the top event to occur during [*t*, *t*+*dt*), no minimal cut sets can exist at *t*, and one or more must occur in [*t*, *t*+*dt*). This can be expressed as,

$$w_{SYS}\ (t)dt = P\left[A\bigcup_{i=1}^{N_{mcs}}\theta_i\right] \tag{2.6}$$

where A is the event that no minimal cut set exists at time *t*

$\bigcup_{i=1}^{N_{mcs}}\theta_i$ is the event that one or more minimal cut sets occur in [*t*, *t*+*dt*)

Since $P(A) = 1 - P(\overline{A})$, the right hand side of equation (2.6) can be expressed by equation (2.7),

$$P\left[A\bigcup_{i=1}^{N_{mcs}}\theta_i\right] = P\left[\bigcup_{i=1}^{N_{mcs}}\theta_i\right] - P\left[\overline{A}\bigcup_{i=1}^{N_{mcs}}\theta_i\right] \tag{2.7}$$

where $\overline{A}$ is the event that at least one minimal cut set exists at time *t*

Therefore:

$$w_{SYS}(t)\,dt = P\left[\bigcup_{i=1}^{N_{mcs}}\theta_i\right] - P\left[\overline{A}\bigcup_{i=1}^{N_{mcs}}\theta_i\right] \tag{2.8}$$

The first term on the right hand side of equation (2.8) represents the contribution from the occurrence of at least one minimal cut set. The second term represents the contribution of minimal cut sets occurring while other minimal cut sets already exist (i.e. the system has already failed). The two terms can be denoted by $w_{SYS}{}^{(1)}(t)\,dt$ and $w_{SYS}{}^{(2)}(t)\,dt$ respectively, and equation (2.8) becomes,

$$w_{SYS}(t)\,dt = w_{SYS}{}^{(1)}(t)\,dt - w_{SYS}{}^{(2)}(t)\,dt \tag{2.9}$$

Both of the terms on the right hand side can be obtained using the inclusion-exclusion expansion (equation (2.3)). Since this is even more computationally intensive than the equivalent top event probability calculation, an approximation for the system unconditional failure intensity is used.

2.2.3.2.1 Approximation for the System Unconditional Failure Intensity

In most situations, the event of component failure is very unlikely and so the occurrence of a minimal cut set will be a rare event. The second term of equation (2.9) requires the probability that minimal cut sets exist and then others occur. When the occurrence of a minimal cut set is a rare event, this term becomes negligible, and an upper bound for the system unconditional failure intensity, $w_{SYS_{MAX}}(t)\,dt$, is obtained by considering only the first term of the equation, $w_{SYS}{}^{(1)}(t)\,dt$, as given in equation (2.10),

$$w_{SYS_{MAX}}(t)\,dt \leq w_{SYS}{}^{(1)}(t)\,dt \tag{2.10}$$

$w_{SYS}{}^{(1)}(t)\,dt$ may be expanded using the inclusion-exclusion technique and again truncated after the first term to give the rare event approximation (equation (2.11)),

$$w_{SYS_{MAX}}(t)\,dt \leq \sum_{i=1}^{N_{mcs}} w_{\theta_i}(t)dt$$

$$w_{SYS_{MAX}}(t) \leq \sum_{i=1}^{N_{mcs}} w_{\theta_i}(t) \tag{2.11}$$

where $w_{\theta_i}(t)$ is the unconditional failure intensity of minimal cut set θ_i

The unconditional failure intensity of a minimal cut set θ_i, $w_{\theta_i}(t)$, is the probability of occurrence of the minimal cut set per unit time at *t*. Since only one component failure can occur in a small time element *dt*, the probability of occurrence of minimal cut set θ_i is the probability of any event *c* from the set occurring during [*t*,*t* + *dt*) given that all other basic events in the minimal cut set have already occurred. Considering each of the N_{θ_i} events in turn allows the unconditional failure intensity of the minimal cut set to be expressed in equation (2.12).

$$w_{\theta_i}(t)dt = \sum_{c=1}^{N_{\theta_i}} \left(w_c(t)dt \prod_{\substack{d \neq c \\ d=1}}^{N_{\theta_i}} q_d(t) \right) \tag{2.12}$$

2.2.3.3 Expected Number of System Failures

The expected number of system failures during [0, t) is denoted by $W_{SYS}(0,t)$ and is obtained by the integral of the system unconditional failure intensity in the interval [0,t) shown in equation (2.13),

$$W_{SYS}(0,t) = \int_0^t w_{SYS}(u)\, du \tag{2.13}$$

If the system is reliable, the expected number of system failures can be used as an upper bound for the system unreliability.

2.2.3.4 Structure Functions

The state of a component or system may be considered to either work or fail. This can be represented by a binary indicator variable. A component c is assigned a binary indicator variable x_c, such that,

$$x_c = \begin{cases} 1 & \text{if the component is failed} \\ 0 & \text{if the component is working} \end{cases}$$

Similarly the top event of a system may be assigned a binary function, ϕ, such that,

$$\phi(\mathbf{x}) = \begin{cases} 1 & \text{if the system is failed} \\ 0 & \text{if the system is working} \end{cases}$$

This is known as the *System Structure Function*, and shows the system state in terms of its component states, **x**. The system structure function may be expressed in terms of its component states using equation (2.14).

$$\phi(\mathbf{x}) = 1 - \prod_{i=1}^{N_{mcs}} (1 - \rho_i(\mathbf{x})) \tag{2.14}$$

where $\rho_i(\mathbf{x})$ is the binary indicator variable for each minimal cut set C_i, i=1..N_{mcs}

Then, $$\rho_i(\mathbf{x}) = \prod_{j \in C_i}^{N_{C_i}} x_j \tag{2.15}$$

Where $\rho_i(\mathbf{x}) = \begin{cases} 1 & \text{if cut set } C_i \text{ exists} \\ 0 & \text{if cut set } C_i \text{ does not exist} \end{cases}$

The probability of the top event occurrence can be obtained by the expected value of the structure function, $\mathrm{E}[\phi(\mathbf{x})]$, in equation (2.16),

$$Q_{SYS}(t) = \mathrm{E}[\phi(\mathbf{x})] \tag{2.16}$$

If the minimal cut sets are independent, $\mathrm{E}[\phi(\mathbf{x})] = \phi[\mathrm{E}(\mathbf{x})]$. In most cases the minimal cut sets will not be independent and so a full expansion of the structure function must be performed prior to taking the expectation.

2.2.3.5 Importance Measures

The contribution of a component or cut set to the occurrence of a top event is defined as its *importance*. The measure of importance is a function of time, system structure and failure and repair characteristics. It is clear by the structural arrangement of a system that some components will be more critical to the success of a system than others; a component in a series arrangement will generally be more important than a component placed in a parallel arrangement.

The analysis of importance is a sensitivity study method that allows identification of the weak areas of a system, thus is a very useful tool in the design and optimisation stages. Fault tree analysis is a suitable technique of identifying the basic causes that contribute to system failure. Quantification of a fault tree can be performed if component data is known, and the importance of each individual component may be calculated as a value between 0 and 1.

There are several importance measures that have been developed to analyse the contribution of both individual components and minimal cut sets to the occurrence of the top event. These may be divided into two categories of importance measure, *deterministic* and *probabilistic*. Probabilistic measures can be further categorised as dealing with system unavailability or system unreliability assessment.

2.2.3.5.1 Deterministic Measures of Importance

Deterministic measures of importance analyse the importance of a component to a system with no reference to its probability of occurrence. The *Structural Measure of Importance* is one such measure.

Structural Measure of Importance

For a component c the structural measure of importance is defined by equation (2.17).

$$I_c^{ST} = \frac{\textit{number of critical system states for component } c}{\textit{total number of states for the } (n-1) \textit{ remaining components}} \qquad (2.17)$$

A system is in a critical state for a component c if the remaining (n-1) components are in a state that allows the failure of component c to cause the system to go from a working to a failed state. This can be demonstrated on a single system, shown in Figure 2.2.

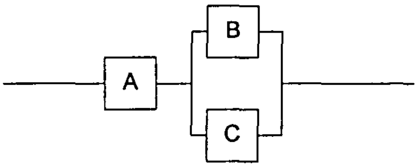


Figure 2.2 Single System

The critical states for each of the components can be summarised in Table 2.3.

	States For Other Components A	 B	 C	Critical State For Component
Component A:	-	0	0	Yes
	-	0	1	Yes
	-	1	0	Yes
	-	1	1	No
Component B:	0	-	0	No
	0	-	1	Yes
	1	-	0	No
	1	-	1	No
Component C:	0	0	-	No
	0	1	-	Yes
	1	0	-	No
	1	1	.	No

where 0 = Component Success, 1 = Component Failure

Table 2.3 Critical States for Components in Single System

The Structural Measure of Importance for each of the components is found in equation (2.18).

$$I_A^{ST} = \frac{3}{4} \qquad I_B^{ST} = \frac{1}{4} \qquad I_C^{ST} = \frac{1}{4} \tag{2.18}$$

Since each component will have a different rate of failure, in reality this measure is not very useful. Probabilistic measures of importance depend on component failure probability and intensity and so are generally of more use than deterministic measures. Such measures for dealing with system unavailability and unreliability assessment are presented in the following sections.

2.2.3.5.2 Probabilistic Measures of Importance

Several probabilistic measures have been developed to compute the importance of both basic events and minimal cut sets to the occurrence of the top event with consideration of system unavailability. Many of these importance measures depend on the criticality function $G(\boldsymbol{q}(t))$. This function may be formally defined as:

$G_c(\boldsymbol{q}(t))$ = The probability that the system is in a critical system state for component *c*

Birnbaum's Measure of Importance

Birnbaum's measure of importance [5] is also known as the criticality function. The criticality function is found by the sum of the probabilities of occurrence of the critical system states for component *c*. To demonstrate this, the example given in Figure 2.2 may be used, and the system state probabilities are summarised in Table 2.4.

Birnbaum's measure of importance for each of the components is found using this method in equations (2.19)

$$\begin{aligned}
G_A(\boldsymbol{q}) &= (1-q_B)(1-q_C) + (1-q_B)q_C + q_B(1-q_C) \\
&= 1 - q_B q_C \\
G_B(\boldsymbol{q}) &= (1-q_A)q_C \\
G_C(\boldsymbol{q}) &= (1-q_A)q_B
\end{aligned} \tag{2.19}$$

	States For Other Components			Probability	Critical State For Component
	A	B	C		
Component A:	-	0	0	$(1-q_B)(1-q_C)$	Yes
	-	0	1	$(1-q_B)q_C$	Yes
	-	1	0	$q_B(1-q_C)$	Yes
	-	1	1	q_Bq_C	No
Component B:	0	-	0	$(1-q_A)(1-q_C)$	No
	0	-	1	$(1-q_A)q_C$	Yes
	1	-	0	$q_A(1-q_C)$	No
	1	-	1	q_Aq_C	No
Component C:	0	0	-	$(1-q_A)(1-q_B)$	No
	0	1	-	$(1-q_A)q_B$	Yes
	1	0	-	$q_A(1-q_B)$	No
	1	1	-	q_Aq_B	No

Table 2.4 Example of Birnbaum's Measure of Importance

Birnbaum's measure of importance can also be directly obtained using equations (2.20) and (2.22):

- $$G_c(q(t)) = Q_{SYS}(1_c, q(t)) - Q_{SYS}(0_c, q(t)) \qquad (2.20)$$

where $Q_{SYS}(t)$ = probability that the system fails

$(1_c, q(t)) = (q_1, \ldots, q_{c-1}, 1, q_{c+1}, \ldots, q_n)$ component c failed

$(0_c, q(t)) = (q_1, \ldots, q_{c-1}, 0, q_{c+1}, \ldots, q_n)$ component c working

Equation (2.20) is the probability that the system fails with component c failed minus the probability that the system fails with component c working. This expression therefore represents the probability that the system fails only when component c fails. Considering the example in Figure 2.2, Birnbaum's importance measure for components A, B, and C is given in equations (2.21).

$$Q_{SYS}(q(t)) = q_A + q_B q_C - q_A q_B q_C$$

$$(1_A, q(t)) = 1 + q_B q_C - q_B q_C = 1$$
$$(0_A, q(t)) = q_B q_C$$
$$G_A(q(t)) = 1 - q_B q_C$$

$$(1_B, q(t)) = q_A + q_C - q_A q_C$$
$$(0_B, q(t)) = q_A$$
$$G_B(q(t)) = q_A + q_C - q_A q_C - q_A = q_C(1 - q_A)$$

$$(1_C, q(t)) = q_A + q_B - q_A q_B$$
$$(0_C, q(t)) = q_A$$
$$G_C(q(t)) = q_A + q_B - q_A q_B - q_A = q_B(1 - q_A)$$

(2.21)

- $$G_c(q(t)) = \frac{\partial Q_{SYS}(q(t))}{\partial q_c(t)} \qquad (2.22)$$

This is equivalent to equation (2.20) since:

$$\frac{\partial Q_{SYS}(q(t))}{\partial q_c(t)} = \frac{Q_{SYS}(1_c, q(t)) - Q_{SYS}(0_c, q(t))}{1 - 0}$$

Equation (2.22) is defined as the partial derivative of the probability that the system fails with respect to the probability of failure of component *c*. Applying this method to the example in Figure 2.2 gives the same results as in equations (2.21).

Birnbaum's measure of importance is not a function of a component's own failure probability. Many further importance measures are defined using this parameter.

Criticality Measure of Importance

The criticality measure of importance is defined as the probability that the system is in a critical state for component *c*, and component *c* has failed (weighted by the system unavailability). This is represented by equation (2.23).

$$I_c^{CR} = \frac{G_c(q(t)) q_c(t)}{Q_{SYS}(q(t))} \qquad (2.23)$$

Applying this to the example in Figure 2.2 gives:

$$I_A^{CR} = \frac{(1-q_B q_C)q_A}{q_A + q_B q_C - q_A q_B q_C} \quad I_B^{CR} = \frac{(1-q_A)q_C q_B}{q_A + q_B q_C - q_A q_B q_C} \quad I_C^{CR} = \frac{(1-q_A)q_B q_C}{q_A + q_B q_C - q_A q_B q_C} \tag{2.24}$$

Fussell-Vesely Measure of Importance

For system failure to take place, it is possible that one or more minimal cut sets could occur simultaneously. Component *c* will contribute to the failure of a system by the occurrence of a minimal cut set containing *c*.

The Fussell-Vesely measure of importance [6] is defined as the probability of the union of the minimal cut sets C_k containing *c* given that the system has failed (equation (2.25)).

$$I_c^{FV} = \frac{P(\bigcup_{k|c\in k} C_k)}{Q_{SYS}(q(t))} \tag{2.25}$$

Application of this measure of importance to the components in the example (Figure 2.2) with minimal cut sets {A} and {B,C} gives:

$$I_A^{FV} = \frac{q_A}{q_A + q_B q_C - q_A q_B q_C} \quad I_B^{FV} = \frac{q_B q_C}{q_A + q_B q_C - q_A q_B q_C} \quad I_C^{FV} = \frac{q_B q_C}{q_A + q_B q_C - q_A q_B q_C} \tag{2.26}$$

The rankings found by the Fussell-Vesely measure of importance are seen to closely relate to those found by the criticality importance measure.

Fussell-Vesely Measure of Minimal Cut Set Importance

The Fussell-Vesely measure of minimal cut set importance ranks the minimal cut sets in the order of their contribution to the top event. The importance of each cut set C_k can be defined as the probability of existence of the minimal cut set given that the system has failed:

$$I_{C_k}^{FV} = \frac{P(C_k)}{Q_{SYS}(q(t))} \tag{2.27}$$

The importance of each of the minimal cut sets for the example in Figure 2.2 can be expressed by equations (2.28).

$$I_A^{FV} = \frac{q_A}{q_A + q_B q_C - q_A q_B q_C} \qquad I_{BC}^{FV} = \frac{q_B q_C}{q_A + q_B q_C - q_A q_B q_C} \tag{2.28}$$

2.2.3.5.3 Probabilistic Measures for Initiating and Enabling Events

The original, pioneering work, in fault tree analysis held the assumption that the sequence of occurrence of basic events is not important, thus a minimal cut set will cause system failure regardless of the order of component failures. However, in some cases the top event of a fault tree may only be caused by a certain sequence of basic event occurrences. An example of such a situation would be a safety protection system designed to protect against a specific hazard. If the hazardous event occurs while safety protection devices are functioning, the top event will not occur and a shutdown would be instigated. If the hazardous event occurs while safety protection devices are not working a more catastrophic system level failure will occur. This introduces a limited ordering requirement on the basic events. In this case the last event to occur needs to be the hazardous one. If the safety features have failed (in any order) prior to this then the system failure represented by the fault tree will occur.

Such a system, with limited sequential aspects, can be modelled using component failure events classified as *initiating* or *enabling* events.

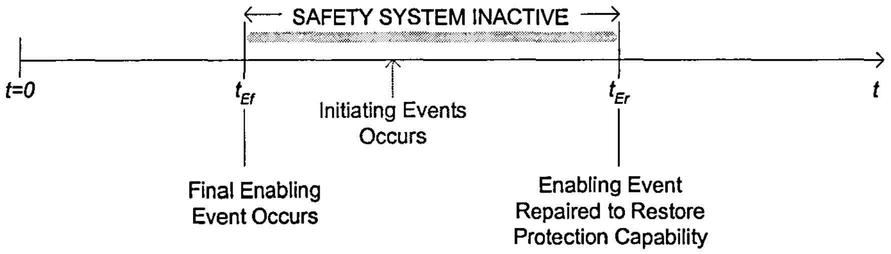

SAFETY SYSTEM INACTIVE
t=0
t_{Ef}
Initiating Events Occurs
t_{Er}
t
Final Enabling Event Occurs
Enabling Event Repaired to Restore Protection Capability

Figure 2.3 Example of A Safety System

Consider the situation illustrated in Figure 2.3. The final safety feature fails at $t=t_{Ef}$, and the protection capability is restored again at $t=t_{Er}$. During the period of time from t_{Ef} to t_{Er}, the system is in a critical state and vulnerable to the occurrence of the hazard. If the hazardous event occurs prior to t_{Ef}, the safety systems will respond as required and the system will not fail. If the hazardous event occurs while the safety system is inactive, the safety system is unable to respond and so a hazardous system failure will occur. Thus the order in which components fail will be of importance to the system outcome. In this type of situation, failed safety features are known as enabling events. The occurrence of the hazardous event is known as an initiator. Initiating and enabling events may be formally defined as:

Initiating Events : Perturb system variables and place a demand on control or protective systems to respond.

Enabling Events : Inactive control or protective systems which permit initiating events to cause the top event.

In a system, an initiator may act as either an enabler or an initiator, whereas an enabler can only act in this capacity. Every minimal cut set of the system requires at least one initiator in order to cause system failure.

The importance measures described in the previous sections assume that the order of component failures in a minimal cut set is irrelevant. Probabilistic measures of importance are presented to deal with the interval reliability of a system where the order of component failures is important. All such measures are weighted according to the expected number of system failures, $W_{SYS}(0,t)$.

Expected Number of System Failures

The system unconditional failure intensity, $w_{SYS}(t)$, is defined as the probability that the top event occurs per unit time at *t*. This is the sum of the probabilities that the system is in a critical state for each initiator *i* and the frequency that *i* occurs at *t*, and is given in terms of the criticality function in equation (2.29).

$$\begin{aligned} w_{SYS}(t)\, dt &= \sum_{\substack{i=1 \\ i \text{ initiator}}}^{N_I} G_i\big(q(t)\big)\cdot w_i(t)dt \\ &= \sum_{\substack{i=1 \\ i \text{ initiator}}}^{N_I} \left(\frac{\partial Q_{SYS}(q(t))}{\partial q_i(t)}\right)\cdot w_i(t)dt \end{aligned} \tag{2.29}$$

where N_i is the number of initiating events

The expected number of system failures can be calculated by the integral of the system unconditional failure intensity over the interval [0,*t*) (equation (2.30)).

$$W_{SYS}(0,t) = \int_0^t w_{SYS}(u)\,du \; = \int_0^t \sum_{\substack{i=1 \\ i \text{ initiator}}}^{N_I} \left(\frac{\partial Q_{SYS}(q(u))}{\partial q_i(u)} \right) \cdot w_i(u)du \qquad (2.30)$$

Barlow-Proschan Measure of Initiator Importance

The Barlow-Proschan measure of importance is the probability that initiating event *i* causes system failure over the interval [0,*t*). This is defined in terms of the criticality function and weighted according to the expected number of system failures, $W_{SYS}(0,t)$, in equation (2.31)

$$I_i^{BP} = \frac{\int_0^t \{Q_{SYS}(1_i, q(u)) - Q_{SYS}(0_i, q(u))\} w_i(u)du}{W_{SYS}(0,t)} \qquad (2.31)$$

Measures of Enabler Importance

The sequential contributory measure of enabler importance was introduced by Lambert [7], and is defined as the probability that enabling event *e* permits an initiating event *i* to cause system failure over [0,*t*). The failure of the enabler *e* is considered only a factor when it is contained in the same minimal cut set as the initiating event *i*. Again, since the interval reliability is the parameter of interest, Lambert's measure is weighted by the expected number of system failures and is given in equation (2.32).

$$I_e^{SC} = \frac{\sum\limits_{\substack{i \\ e \neq i \\ e \text{ and } i \in C_k \\ \text{for some } k}} \int_0^t \{Q(1_e, 1_i, q(u)) - Q(1_e, 0_i, q(u))\} q_e(u) w_i(u)du}{W_{SYS}(0,t)} \qquad (2.32)$$

where *i* runs over each initiating event in the same minimal cut set as *e*

This expression is an approximation since it does not account for the separate roles of events *e* and *i* in causing or contributing to system failure. For enabling event *e* to allow initiating event *i* to cause system failure, *e* and *i* must occur in at least one minimal cut set together and it must be the existence of one such minimal cut set that causes system failure.

A method has been developed by Beeson and Andrews [8] to obtain the exact importance of an enabler *e* when initiating event *i* causes system failure, however this technique is very computationally intensive to perform. In recognition that equation (2.32) is not an accurate calculation, a better approximation is presented by Dunglinson and Lambert [9]. This is defined as the fraction of time that minimal cut sets containing event *e* have caused the top event to occur given that the top event has occurred, and is expressed in equation (2.33).

$$I_e^{DL} = \frac{\int_0^t \sum_{i=1}^{N_I} P\left(\bigcup_{k|i,e\in k} E_k\right) w_i(u)\,du}{W_{SYS}(0,t)} \tag{2.33}$$

where E_k is the event that minimal cut set *k* occurs with initiating event *i* set to true

This Dunglinson-Lambert measure is only an approximation since the existence of other minimal cut sets that do not contain both events *e* and *i* has not been accounted for.

2.3 Binary Decision Diagrams

The size of a fault tree problem can become very large, especially when considering the possibility of multiple phased missions. An alternative method to assess the reliability performance of a system is by converting the fault tree to a Binary Decision Diagram (BDD) prior to analysis. A BDD provides an efficient representation of a system with a Boolean equation for the top event. BDDs are often preferred structures to that of fault trees due to the fact that the logic expression offers efficient mathematical manipulation. Qualitative and quantitative analysis can be performed on a BDD, and exact solutions can be obtained without the need for approximations of the conventional fault tree approach. The use of BDDs in reliability analysis was initially developed by Rauzy [4].

2.3.1 Properties of the BDD

A BDD is a directed acyclic graph, and so paths through a BDD can only travel in one direction without the possibility of looping. A BDD comprises of both terminal and non-terminal nodes (also called vertices) which are connected by branches. The non-terminal nodes of a BDD represent the basic events of the fault tree and the terminal nodes represent the final state of the system. The terminal nodes of a BDD are defined by:

0	-	System works
1	-	System fails

An example of a binary decision diagram is given in Figure 2.4.

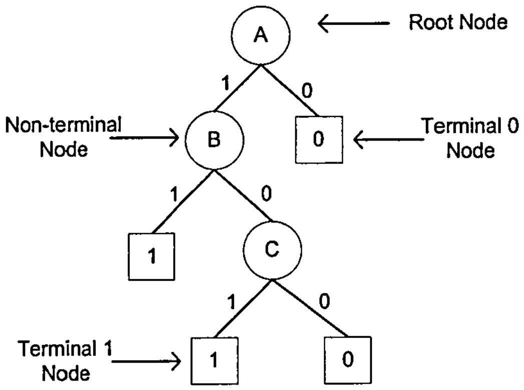


Figure 2.4 Example Binary Decision Diagram

Each non-terminal node has two outgoing branches. Generally, the left '1' branch represents the occurrence of the basic event (the component fails), and the right '0' branch represents the non-occurrence of the basic event (the component works). The size of a BDD is defined by the number of non-terminal nodes.

Each path through a BDD begins at the root node and moves through the diagram until a terminal node is reached. Paths that terminate in a '1' node can be used to generate the cut sets of a system. On these paths the cut sets are produced by listing all basic event occurrences as these lead to system failure. Only the branches representing the occurrence of a basic event are included in the cut set. For example, there are two paths in the BDD in Figure 2.4 that end in a terminal '1' node:

1. A, B
2. $A, \overline{B}, C$

The cut sets obtained by only the occurrence of basic events become:

1. A, B
2. A, C

There are various methods of obtaining the BDD for a system. All methods require an ordering of the variables (basic events of the fault tree). This ordering represents the sequence of the basic events in the construction of the BDD, and can be chosen to define an optimal BDD for analysis. Further work on the qualification and quantification of BDDs is developed by Sinnamon and Andrews [10], [11].

2.3.2 Formation of a BDD Using Structure Functions

The structure function of a fault tree can be used to demonstrate the formation of a BDD by successively substituting one and zero into the structure function equation in the sequence of the chosen ordering. This is demonstrated using the example fault tree in Figure 2.5.

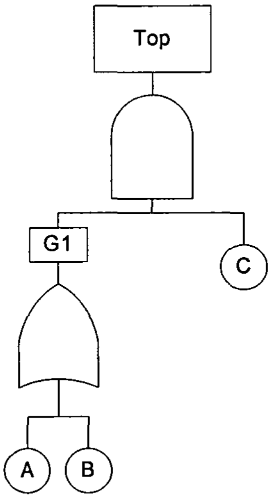


Figure 2.5 Example Fault Tree

The minimal cut sets of this example are {A,C} and {B,C}, and the structure function is given by:

$$\phi = 1 - (1 - x_A \cdot x_C)(1 - x_B \cdot x_C)$$

If the variable ordering is chosen as the events appear from left to right on the fault tree, A<B<C, A is considered first, followed by B and then C. The first non-terminal node ‘A’ is drawn with 2 outgoing branches denoting the failure (occurrence) and the success (non-occurrence) of the event. The result of the failure and success branches is obtained by substituting ‘1’ and ‘0’ respectively for x_A in the structure function equation. The same is then done for B and C until terminal nodes are reached which determines the system state. The resulting BDD with Boolean equations is shown in Figure 2.6.

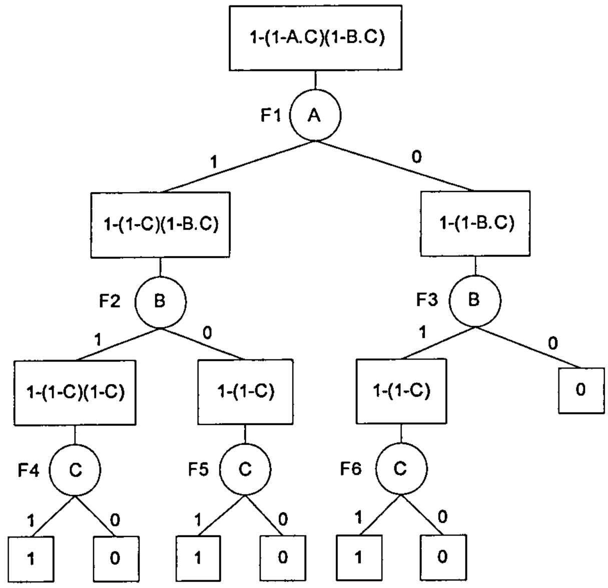


Figure 2.6 Binary Decision Diagram with Boolean Variables

2.3.2.1 Reduction of the BDD

A series of operations may be applied to reduce the size of a BDD:

1. If the two sons of a node ‘a’ are equivalent, then delete node ‘a’ and direct all of its incoming branches to its left son.
2. If nodes ‘a’ and ‘b’ are equivalent, then delete node ‘b’ and direct all of its incoming branches to ‘a’.

where the *son* of a node is the node which either branch leads to.

This reduction technique may be applied to the example BDD in Figure 2.6. The first operation may be applied to delete node F2 since both of its sons are equivalent. Node

F1 passes directly to its left son, F4. Node F5 is deleted. Application of the second operation identifies the identical nodes F4 and F6. F6 and sons can be deleted and the incoming branch from node F3 passes instead to node F4. The resulting BDD is given in Figure 2.7.

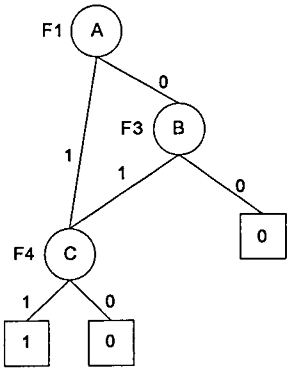


Figure 2.7 Reduced BDD from Figure 2.4.

The reduced BDD is considerably smaller than the original BDD in Figure 2.6, with three non-terminal nodes rather than six.

Although this method results in a significant reduction in the size of a BDD, it does not always result in the minimal BDD. A minimisation procedure to obtain the minimal cut sets of a BDD is presented in Section 2.3.4. The use of structure functions to form the BDD clearly demonstrates the relationship between the fault tree and the BDD, however an obvious disadvantage is that the cut sets must be determined to define the system structure function prior to construction of the BDD.

2.3.3 Formation of a BDD using If-Then-Else Structure

An alternative method to construct a BDD was developed by Rauzy [4] where each gate of a fault tree is defined using an **if-then-else (ite)** technique. The top event of a fault tree can be expressed as a Boolean function, f(x), and pivoted about any variable X1. Shannon's formula can then be expressed in equation (2.34).

$$f(\mathbf{x}) = \mathrm{X1} \cdot \mathrm{f1} + \overline{\mathrm{X1}} \cdot \mathrm{f2} \tag{2.34}$$

where f1 and f2 are functions with X1=1 and X1=0 respectively

The **ite** structure for this is represented as **ite**(X1, f1, f2), and is defined by '**if** X1 fails, **then** consider f1, **else** consider f2'. In the BDD, f1 is achieved by the '1' branch of the X1 node (occurrence of X1), and f2 is achieved by the '0' branch of the X1 node (non-occurrence of X1). This structure is shown in Figure 2.8.

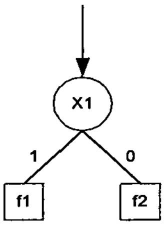


Figure 2.8 A Binary Decision Diagram Vertex of **ite**(X1, f1, f2)

To begin the construction of the full BDD, each basic event x is given the structure **ite**(x, 1, 0). To combine basic events within the BDD, the following rules must be applied:

To combine two basic events (X and Y) using a logical operation $\oplus$,

$$\begin{array}{ll} \textit{If} & J = \textbf{ite}(X, f1, f2) \\ \textit{and} & H = \textbf{ite}(Y, g1, g2) \end{array}$$

$$\begin{array}{ll} \text{If X} < \text{Y} & J \oplus H = \textbf{ite}(X, f1 \oplus H, f2 \oplus H) \\ \text{If X} = \text{Y} & J \oplus H = \textbf{ite}(X, f1 \oplus g1, f2 \oplus g2) \end{array}$$

This method has the advantage of automatically eliminating the repetition of nodes. The **ite** method may be applied to the fault tree in Figure 2.5, again using the ordering A<B<C:

G1 is defined as:

$$\begin{aligned} \text{G1} &= \text{A} + \text{B} \\ &= \textbf{ite}(\text{A}, 1, 0) + \textbf{ite}(\text{B}, 1, 0) \\ &= \textbf{ite}(\text{A}, 1, \textbf{ite}(\text{B}, 1, 0)) \end{aligned}$$

Top is then found as:

$$\begin{aligned} \text{Top} &= \text{G1} \cdot \text{C} \\ &= \textbf{ite}(\text{A}, 1, \textbf{ite}(\text{B}, 1, 0)) \cdot \textbf{ite}(\text{C}, 1, 0) \\ &= \textbf{ite}(\text{A}, \textbf{ite}(\text{C}, 1, 0), \textbf{ite}(\text{B}, \textbf{ite}(\text{C}, 1, 0), 0)) \end{aligned}$$

The BDD can then be constructed by considering the '1' and '0' branches of each variable in turn until the terminal vertices are reached. The resulting BDD is given in Figure 2.9.

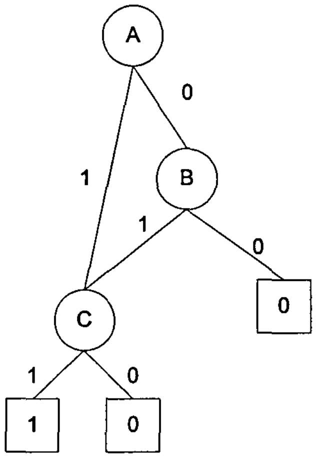


Figure 2.9 BDD of fault tree in Figure 2.3 using **ite** technique

The paths terminating in '1' give the cut sets of the system: {A,C} and {B,C}.

2.3.4 BDD Minimisation

In most cases, the BDD will not be minimal and so the cut sets that are obtained will also not be minimal. A minimisation process has been developed by Rauzy [4] to create a new BDD that encodes the minimal cut sets of the fault tree.

A general node in the BDD is defined by equation (2.35).

$$\mathrm{F} = \mathbf{ite}(x, \mathrm{G}, \mathrm{H}) \tag{2.35}$$

If δ is a minimal solution of G, which is not a minimal solution of H, then the intersection of δ and x ($\{\delta\} \cap x$) will be a minimal solution of F. The set of all minimal solutions of F, $\mathrm{sol_{min}(F)}$ will also include the minimal solutions of H, and can be expressed in equations (2.36) and (2.37).

$$\mathrm{sol_{min}(F)} = \{\sigma\} \tag{2.36}$$

$$\text{where } \sigma = [\{\delta\} \cap x] \cup [\mathrm{sol_{min}(H)}] \tag{2.37}$$

Rauzy has also defined the *without* operator which removes all paths from G_{min} that are included in H_{min}. This ensures that by removing any minimal solutions of G that are also minimal solutions of H, equation (2.37) becomes minimal.

2.4 Markov Analysis

Markov methods provide a means of analysing the reliability and availability of systems whose components exhibit strong dependencies. Markov diagrams for large systems are generally exceedingly large and complex and are often difficult to construct. Markov models are more suitable for analysis of smaller systems. The Markov approach assumes that the system is characterised by a lack of memory, where the future behaviour of the system is only dependent on the immediately preceding state and not on the full history. Each event is determined only by the present system state and is independent of any other past events. A Markov process features a constant transition rate between the system states, and can be used for solution to systems that vary discretely or continuously with respect to time or space.

A Markov Model consists of two elements: states and transitions. Only transitions between linked states are possible. In reliability problems it is possible that a state can cause terminal system failure. This is defined as an *absorbing* state and no transitions may be made from it.

For the method described below it is assumed that the system has a fixed number of identifiable discrete states and that the rate of transition between states is constant with time. This implies that the times to failure and repair of the components are associated with (negative) exponential distributions. This Markov method is discrete in space and continuous in time.

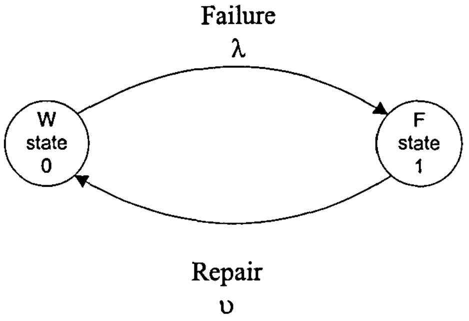
2.4.1 Markov Model Concepts

To begin Markov analysis a directed graph is constructed where each node represents one of the discrete system states, and the edges represent the transition rates between the states in the direction of the arrow.

Considering a single repairable component that may exist in one of two states, working (0-W) or failed (1-F), and can be represented by $x(t)$ in equation (2.38).

$$x(t) = \begin{cases} 1 & \textit{Component Failed} \\ 0 & \textit{Component Working} \end{cases} \tag{2.38}$$

The state of a repairable component with failure rate λ and repair rate υ can be represented by a transition diagram in Figure 2.10.



where $P_0(t)$ = Probability that component is in the working state at time t

$P_1(t)$ = Probability that component is in the failed state at time t

Figure 2.10 Single Repairable Component Markov Transition Diagram

The parameters λ and υ are referred to as *state transition rates* since they represent the rate of communication between the states.

The failure and repair density functions, *f(t)* and *g(t)*, of a component with failure rate λ and repair rate υ are given in equations (2.39).

$$f(t) = \lambda e^{-\lambda t} \qquad\qquad g(t) = \upsilon e^{-\upsilon t} \tag{2.39}$$

To begin the solution of a Markov model, incremental intervals of time *dt* must be considered. Each interval must be sufficiently small so that there is an insignificant chance of two or more events occurring and so a maximum of one state transition may take place in any one interval.

A set of differential equations may be obtained from the state transition diagram in Figure 2.10. The probability of a component being in the working state at a time *t+dt* is dependent only on the state of the component at time *t*, and can be defined as,

$P_0(t+dt)$ = [Probability of component working at time *t* AND not failing in time *dt*]
+ [Probability of component failed at time *t* AND repaired in time *dt*]

The probability that the component is in the working state at time *t+dt* may be represented by equation (2.40).

$$P_o(t+dt) = P_o(t)(1-\lambda dt) + P_1(t)(\upsilon dt) \qquad (2.40)$$

This may be expressed as a differential equation as shown in equation (2.41)

$$\frac{P_o(t+dt)-P_o(t)}{dt} = -\lambda P_o(t) + \upsilon P_1(t)$$

$$\text{As } dt \to 0 \quad \left.\frac{P_o(t+dt)-P_o(t)}{dt}\right|_{dt\to 0} = \frac{dP_o(t)}{dt} = \dot{P}_0(t) \qquad (2.41)$$

Thus equation (2.40) can be expressed by equation (2.42).

$$\dot{P}_o(t) = -\lambda P_o(t) + \upsilon P_1(t) \qquad (2.42)$$

Similarly the probability that the component is in the failed state at time *t+dt* may be derived to form equation (2.43).

$$\dot{P}_1(t) = \lambda P_o(t) - \upsilon P_1(t) \qquad (2.43)$$

A more simple way to represent such systems of differential equations is by the use of matrices. In matrix form these equations are represented in equation (2.44).

$$\begin{bmatrix}\dot{P}_0(t) & \dot{P}_1(t)\end{bmatrix} = \begin{bmatrix}P_0(t) & P_1(t)\end{bmatrix}\begin{bmatrix}-\lambda & \lambda \\ \upsilon & -\upsilon\end{bmatrix}$$

Or,

$$[\dot{\mathbf{P}}] = [\mathbf{P}][\mathbf{A}] \qquad (2.44)$$

where $P_0(0)$ and $P_1(0)$ are the known initial system state probabilities at *t*=0

This square matrix **A** can easily be found from the transition diagram where,

- There are the same number of rows and columns of the matrix as there are states in the diagram.
- Each row has a sum of zero.
- All non-diagonal elements in row *i* and column *j* represent the transition from state *i* to state *j*.
- All diagonal elements *ii* represent the transition rate out of state *i*.

The sum of the system state probabilities at any time *t* must be equal to 1, $\sum_{j=1}^{N_s} P_j(t) = 1$.

In reliability problems, a system failure mode may be catastrophic. In this case a state is entered that cannot be left, and is known as an *absorbing state.* For a single component, this would be represented by the state transition diagram in Figure 2.11.

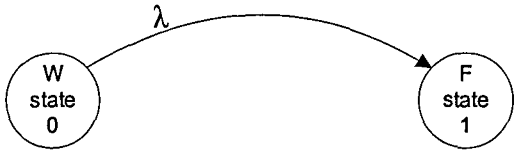


Figure 2.11 Single Non-Repairable Component Markov Transition Diagram

Again using matrices, this system can be represented by equation (2.45).

$$\begin{bmatrix}\dot{P}_0(t) & \dot{P}_1(t)\end{bmatrix} = \begin{bmatrix}P_0(t) & P_1(t)\end{bmatrix}\begin{bmatrix}-\lambda & \lambda \\ 0 & 0\end{bmatrix} \tag{2.45}$$

2.4.2 Laplace Solution of Markov Differential Equations

Since the state equations are linear differential equations with constant coefficients, one method for solution is using Laplace transforms. This technique may be applied to both the non-repairable and repairable single component systems in the following sections.

2.4.2.1 Non-Repairable Single Component

Since $P_0(t)+P_1(t)=1$, transition to the failed state 1 is obtained by the matrix set of differential equations (2.45) and can be represented as given in equation (2.46).

$$\frac{dP_1(t)}{dt}=\lambda[1-P_1(t)] \tag{2.46}$$

Applying Laplace transforms to this differential equation gives equation (2.47).

$$sP_1(s)-P_1(0)=\frac{\lambda}{s}-\lambda P_1(s) \tag{2.47}$$

If the component is known to be working at *t=0*, the initial condition $P_1(0)=0$ holds and equation (2.47) may be written as shown in equation (2.48).

$$\begin{aligned} sP_1(s)&=\frac{\lambda}{s}-\lambda P_1(s)\\ (s+\lambda)P_1(s)&=\frac{\lambda}{s}\\ P_1(s)&=\frac{\lambda}{s(s+\lambda)}\\ P_1(s)&=\frac{1}{s}-\frac{1}{s+\lambda} \end{aligned} \tag{2.48}$$

Inverting equation (2.48) gives the unavailability (unreliability) of the non-repairable component with time in equation (2.49).

$$P_1(t)=1-e^{-\lambda t} \tag{2.49}$$

The availability (reliability) of the component with time is given in equation (2.50).

$$P_0(t)=e^{-\lambda t} \tag{2.50}$$

2.4.2.2 Repairable Single Component

The Laplace transform of the repairable single component failure state in equation (2.43) is given in equation (2.51).

$$sP_1(s) - P_1(0) = \lambda P_o(s) - \upsilon P_1(s) \tag{2.51}$$

Equation (2.51) may be rearranged to give equation (2.52).

$$P_1(s) = \frac{\lambda}{s+\upsilon} P_o(s) + \frac{1}{s+\upsilon} P_1(0) \tag{2.52}$$

Similarly the Laplace transform of the working state in equation (2.42) can be rearranged to form equation (2.53).

$$P_0(s) = \frac{\upsilon}{s+\lambda} P_1(s) + \frac{1}{s+\lambda} P_0(0) \tag{2.53}$$

Equations (2.52) and (2.53) may be solved simultaneously to give equations (2.54).

$$\begin{aligned} P_0(s) &= \frac{\upsilon}{\lambda+\upsilon}\left[\frac{P_0(0)+P_1(0)}{s}\right] + \frac{1}{\lambda+\upsilon}\cdot\frac{1}{s+\lambda+\upsilon}\left[\lambda P_0(0) - \upsilon P_1(0)\right] \\ P_1(s) &= \frac{\lambda}{\lambda+\upsilon}\left[\frac{P_0(0)+P_1(0)}{s}\right] + \frac{1}{\lambda+\upsilon}\cdot\frac{1}{s+\lambda+\upsilon}\left[\upsilon P_1(0) - \lambda P_0(0)\right] \end{aligned} \tag{2.54}$$

Inverting the Laplace transforms back to the real time domain gives equations (2.55).

$$\begin{aligned} P_0(t) &= \frac{\upsilon}{\lambda+\upsilon}\left[P_0(0) + P_1(0)\right] + \frac{e^{-(\lambda+\upsilon)t}}{\lambda+\upsilon}\left[\lambda P_0(0) - \upsilon P_1(0)\right] \\ P_1(t) &= \frac{\lambda}{\lambda+\upsilon}\left[P_0(0) + P_1(0)\right] + \frac{e^{-(\lambda+\upsilon)t}}{\lambda+\upsilon}\left[\upsilon P_1(0) - \lambda P_0(0)\right] \end{aligned} \tag{2.55}$$

The component will begin life in the working state and so the initial conditions are $P_0(0) = 1$ and $P_1(0) = 0$. This reduces equations (2.55) to give equations (2.56).

$$\begin{aligned} P_0(t) &= \frac{\upsilon}{\lambda+\upsilon} + \frac{\lambda e^{-(\lambda+\upsilon)t}}{\lambda+\upsilon} = 1 - \frac{\lambda}{\lambda+\upsilon}\left[1 - e^{-(\lambda+\upsilon)t}\right] \\ P_1(t) &= \frac{\lambda}{\lambda+\upsilon} - \frac{\lambda e^{-(\lambda+\upsilon)t}}{\lambda+\upsilon} = \frac{\lambda}{\lambda+\upsilon}\left[1 - e^{-(\lambda+\upsilon)t}\right] \end{aligned} \tag{2.56}$$

2.4.3 Numerical Solution of Markov Differential Equations

For complex problems it is more suitable to solve the set of N_s differential equations using numerical methods. Equation (2.44) may be written in expanded form by equation (2.57).

$$[\dot{\mathbf{P}}] = [\mathbf{P}][\mathbf{A}]$$

$$\left[\dot{P}_1, \dot{P}_2, \cdots, \dot{P}_{N_s}\right] = \left[P_1, P_2, \cdots, P_{N_s}\right][\mathbf{A}] \tag{2.57}$$

Since,

$$\dot{P}_i(t) = \frac{P_i(t+dt) - P_i(t)}{dt} \tag{2.58}$$

Equation (2.57) may be represented by equation (2.59).

$$\left[P_1(t+dt), P_2(t+dt), \cdots, P_{N_s}(t+dt)\right] = \left[P_1(t), P_2(t), \cdots, P_{N_s}(t)\right]\left[\mathbf{I} + [\mathbf{A}]dt\right] \tag{2.59}$$

The general numerical solution to the set of differential equations is therefore given by equation (2.60).

$$[\mathbf{P}(t+dt)] = [\mathbf{P}(t)][\mathbf{K}] \qquad \text{where} \qquad [\mathbf{K}] = [\mathbf{I} + [\mathbf{A}]dt] \tag{2.60}$$

This leads to a recursive solution to the differential equations over a duration of time.

Chapter 3 Review of Existing Methods for Phased Mission Systems

3.1 Introduction

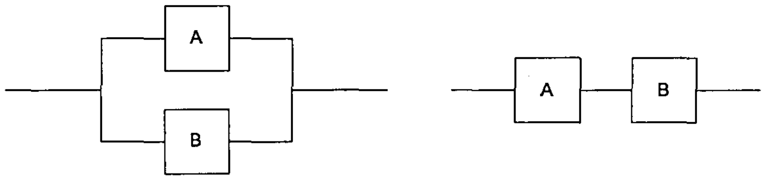
The topic of phased mission analysis has been the focus of several researchers in the broader field of risk and reliability assessment. Methods have been investigated to identify possible causes of phase and mission failure by the combination of basic event occurrences throughout the mission. The quantification, using the failure event probabilities, enables the likelihood and frequency of mission failure to be determined.

The methods that have been developed for solution to phased mission problems can be categorised as those appropriate for non-repairable or repairable systems. In the case of non-repairable systems, a component failure will be permanent and the component will remain failed for the duration of the mission. In the case of repairable systems, it is possible for a component to be restored to new condition after failure. The techniques that have been found appropriate for solution to these cases are discussed in the following sections.

3.2 Non-Repairable Systems

The earliest consideration of the analysis of phased missions was made by Esary and Ziehms [12] using fault tree analysis. A mission is split into consecutive phases, and each phase performs a specified task. The system at any time may be represented by one of two states - working or failed. The success of the mission depends on the non-repairable components used during each phase, and the probability of the successful completion of all phases is referred to as the *Mission Reliability*, R_{MISS}.

The reliability of a phased mission cannot simply be obtained by the multiplication of the reliabilities of each of the individual phases. This involves the false assumptions that all components are in the working state at the beginning of each phase and that components are not shared between the phases, and results in an appreciable over-prediction of system reliability. This point is illustrated using the example in Figure 3.1.



Phase 1 Phase 2

Figure 3.1 Example Mission with Two Phases

Let ρ_{c_1} be the probability that component c functions through phase 1, and ρ_{c_2} be the conditional probability that component c functions through phase 2 given that it has functioned through phase 1. The system reliability for phases 1 and 2 would be found by:

Phase 1 $R_1 = \rho_{A_1} + \rho_{B_1} - \rho_{A_1}\rho_{B_1}$

Phase 2 $R_2 = \rho_{A_2}\rho_{B_2}$

The multiplication of the separate phase reliabilities would give the incorrect value of mission reliability, R_{MISS}^{*}, shown in equation (3.1)

$$R_{MISS}^{*} = R_1R_2 = (\rho_{A_1} + \rho_{B_1} - \rho_{A_1}\rho_{B_1})(\rho_{A_2}\rho_{B_2}) \tag{3.1}$$

For the mission to be achieved successfully, both components must function through both phases. The correct mission reliability defined by Esary and Ziehms is obtained by the probability that the components both function through phases 1 and 2, and is given in equation (3.2). This is less than the inaccurate mission reliability calculated by the multiplication of individual phases in equation (3.1).

$$R_{MISS} = \rho_{A_1}\rho_{A_2}\rho_{B_1}\rho_{B_2} \tag{3.2}$$

It can easily be seen that the mission reliability defined in equation (3.2) is also incorrect. The multiplication of the component reliability in individual phases assumes that the probability of success in each phase is independent. Since the success of each component in phase 2 implies that the component must have worked successfully through phase 1, the reliabilities should be combined to a single term.

Since a component cannot be repaired or replaced, it will function continuously until failure occurs and will subsequently remain in the failed state. A method is presented by Esary and Ziehms to transform and reduce a multi-phase mission into an equivalent single-phase mission, allowing existing techniques to be applied to calculate the mission reliability. This is discussed in the following section.

3.2.1 Transformation of a Multi-Phased Mission to an Equivalent Single-Phase Mission

In a multi-phased mission, the performance of a component in a phase depends on its behaviour through previous phases. It will only be in the working state in a phase if it has performed successfully through all preceding phases.

A single component c in phase j may be replaced by a series system of components which represent the performance of component c in all phases up to and including phase j, $c_1, c_2, ..., c_j$, demonstrated in Figure 3.2.

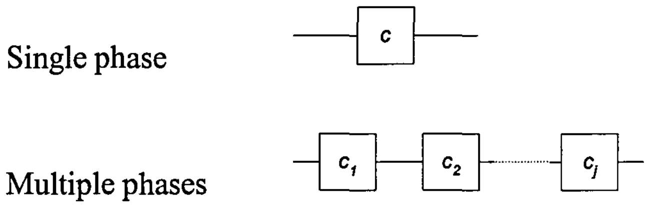


Figure 3.2 Single and Multiple Phase Component Block Diagrams

Similarly using fault tree analysis, the single event input of the failure of component c is replaced by an OR combination of the failure of component c in any phase up to and including phase j, shown in Figure 3.3.

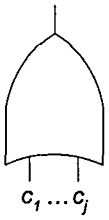


Figure 3.3 Component Failure in Fault Tree of a Multi-Phased Mission

The individual phase configurations can then be joined in series to form a single system. As a demonstration this will be applied to a simple mission network comprising of three phases and three components, A, B, and C given in Figure 3.4.

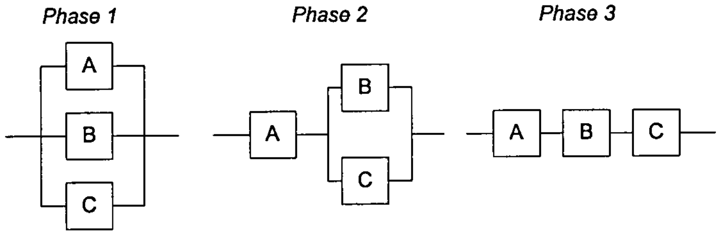


Figure 3.4 Reliability Network of a Simple Phased Mission System

This multi-phased mission can be transformed to a single-phase mission as demonstrated in Figure 3.5.

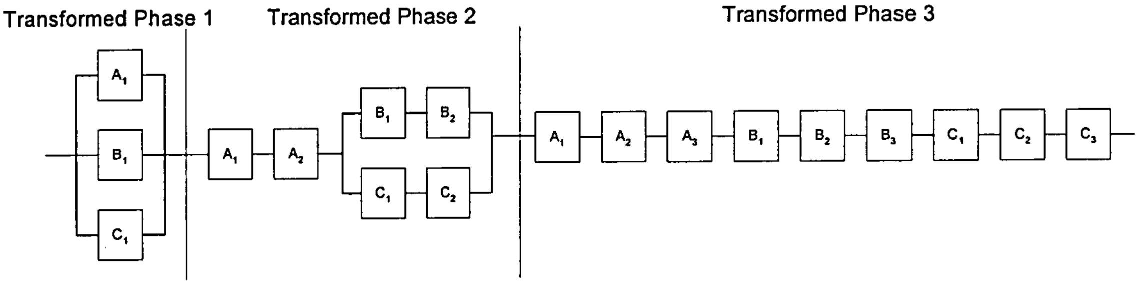


Figure 3.5 Equivalent Single Phase Mission

The three original sequential phase configurations have been transformed to a single network comprising of three sub-systems in a series arrangement. Since the subsystems will generally have components in common, they will not function independently. In this case the product of the subsystem reliabilities will not be equal to the mission reliability.

The subsystem reliabilities become,

Phase 1 $R_1 = \rho_{A_1} + \rho_{B_1} + \rho_{C_1} - \rho_{A_1}\rho_{B_1} - \rho_{A_1}\rho_{C_1} - \rho_{B_1}\rho_{C_1} + \rho_{A_1}\rho_{B_1}\rho_{C_1}$

Phase 2 $R_2 = \rho_{A_1}\rho_{A_2}(\rho_{B_1}\rho_{B_2} + \rho_{C_1}\rho_{C_2} - \rho_{B_1}\rho_{B_2}\rho_{C_1}\rho_{C_2})$

Phase 3 $R_3 = \rho_{A_1}\rho_{A_2}\rho_{A_3}\rho_{B_1}\rho_{B_2}\rho_{B_3}\rho_{C_1}\rho_{C_2}\rho_{C_3}$

(3.3)

where ρ_{c_j} is the conditional reliability of component *c* in phase *j*:

$\rho_{c_1} = P[x_c(t_1) = 0]$ then, $\rho_{c_j} = P[x_c(t_j) = 0 \mid x_c(t_{j-1}) = 0]$ for *j* = *2,..,m*

The product of the subsystem reliabilities would be less than the true system reliability, $R_{MISS} = \rho_{A_1}\rho_{A_2}\rho_{A_3}\rho_{B_1}\rho_{B_2}\rho_{B_3}\rho_{C_1}\rho_{C_2}\rho_{C_3}$ which is found by the simplest form of Figure 3.5, shown in Figure 3.6.

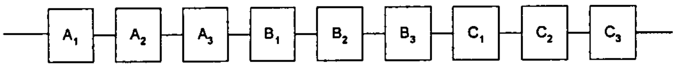


Figure 3.6 Simplest Form of Figure 3.5

3.2.1.1 Cut Set Cancellation

Further simplification of the phase configurations may be made prior to the transformation of the multi-phased mission to an equivalent single phase mission. This is achieved by the technique of cut set cancellation.

If minimal cut sets of an earlier phase contain any minimal cut sets from a later phase, they may be removed from the earlier phase. Since mission success is the only consideration, there is no need to repeat such events as later phases take into account the failure of components in all phases up to the inspected phase.

Phase fault trees for the example given in Figure 3.4 can be constructed and are shown in Figure 3.7.

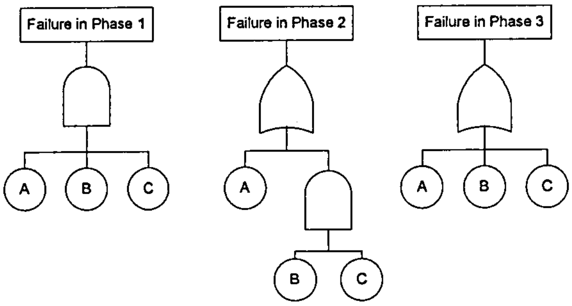


Figure 3.7 Phase Fault Tree Representation of Figure 3.4

The minimal cut sets for each phase are:

Phase 1	Phase 2	Phase 3
{A,B,C}	{A}	{A}
	{B,C}	{B}
		{C}

Minimal cut set {A,B,C} can be removed from phase 1 as A failing in phase 1 means it will still be failed in phase 2 which will fail the mission and make the states of components B and C irrelevant. In the same way, the phase 2 minimal cut sets may be removed since they contain the single order phase 3 minimal cut sets. The phase minimal cut sets become,

Phase 1	Phase 2	Phase 3
-	-	{A}
	-	{B}
		{C}

Both systems are equivalent and result in the same mission reliability, however the cut cancellation technique presents a more simple transformation to a single-phase mission.

In summary, Esary and Ziehms present a suitable method of transforming a multi-phased mission into an equivalent single phased mission to allow the use of existing reliability techniques. The cut set cancellation technique presents a more simple transformation process. However if minimal cut sets are removed from a phase, it is not possible to determine individual phase unreliability or reliability, and calculations can only be made for the entire mission.

3.2.2 Obtaining Bounds for Mission Unreliability

Mission unreliability is defined as the probability that the system fails to function successfully during at least one phase of the mission. An important problem is to calculate as efficiently as possible either the exact value or bounds for this parameter. The developments by Esary and Ziehms in this area are reviewed by Burdick et al [13] with presentation of mission reliability approximation methods. These methods use only statistically independent, non-repairable components to find approximation techniques that can be applied to systems containing a large number of components.

The method presented by Esary and Ziehms can be applied to an original fault tree of a multi-phased mission assuming zero-duration phase boundaries. However, the transformation of each basic event *c* in phase *j* into a series of events, $c_1..c_j$ leads to a large increase in the number of cut sets of the mission. The exact unreliability becomes difficult to calculate and may become costly. Methods have been developed to estimate the system unreliability without the use of basic event transformation. Four of the most accurate and conservative were found to be:

- Inclusion-Exclusion Expansion of Phase Unreliabilities

The minimal cut sets are obtained for each phase of the original model. The unreliability of phase *j*, Q_j, is calculated using the inclusion-exclusion expansion of the phase *j* minimal cut sets (equation (2.3)) using unconditional basic event unreliabilities. The conditional basic event *c* reliability ρ_{c_j} was obtained in equation (3.3), and the unconditional basic event *c* reliability p_{c_j} is derived from this in equation (3.4).

$$p_{c_j} = P[x_c(t_j) = 0] = \prod_{i=1}^{j} \rho_{c_i} \quad \text{for } j=1,..,m \tag{3.4}$$

An approximation for mission reliability, $\overline{Q}_{IN-EX}$, can be expressed by the product of the individual phase reliabilities in equation (3.5).

$$\overline{Q}_{IN-EX} = \prod_{j=1}^{m} R_j \tag{3.5}$$

This is usually expressed as an approximation of mission unreliability, Q_{IN-EX}, and is obtained by the sum of the individual phase unreliabilities in equation (3.6).

$$Q_{IN-EX} \leq \sum_{j=1}^{m} Q_j \tag{3.6}$$

This approximation technique may also be applied after the cut set cancellation method has been implemented to give another approximation of the mission unreliability, $Q_{IN-EX(CC)}$. The result will generally be less than with no cut set cancellations due to the fact that there are fewer cut sets in each phase.

- Minimal Cut Set Bound

The minimal cut sets are obtained from the original logic model. The probability of failure of cut set C_i in phase j, $q_{C_{ij}}$, is calculated using equation (3.7).

$$q_{C_{ij}} = \prod_{c=1}^{N_{C_{ij}}} P\{c\} \tag{3.7}$$

where c occurrence of basic event c in cut set C_i of phase j

$N_{C_{ij}}$ number of basic events in minimal cut set C_i of phase j

The reliability of phase j can then be estimated using the minimal cut bound in equation (3.8).

$$R_j = \prod_{i=1}^{N_{mcs_j}} p_{C_{ij}} \tag{3.8}$$

where N_{mcs_j} number of minimal cut sets in phase j

$p_{C_{ij}}$ is the probability of success of cut set C_i in phase j

The approximation for the reliability of the mission using the minimal cut set bound, $\overline{Q}_{MCB}$, can then be obtained in the same way as for equation (3.5). This method may again be used after applying the cut set cancellation technique to give another approximation of the mission unreliability, $Q_{MCB(CC)}$.

The four mission unreliability approximation methods are ordered in terms of their accuracy in equation (3.9).

$$Q_{MISS} \le Q_{IN-EX(CC)} \le \begin{Bmatrix} Q_{MCB(CC)} \\ \overline{Q}_{IN-EX} \end{Bmatrix} \le Q_{MCB} \tag{3.9}$$

Since the outcome of previous phases in each calculation is not accounted for, the bounds are only estimates. However such approximation techniques can be useful in finding estimations for systems containing a large number of components where an exact solution would be costly or difficult to calculate.

A further technique is presented by Veatch [14] to approximate the unreliability of a phased mission by constructing a lower bound structure function with application to periodic systems.

3.2.3 Redundancy

The reliability of a system can be improved by adding redundant elements that are not required for the successful operation of the system. The number of redundant elements for a system whose parameters do not vary with time are determined at the start of the mission time. In the case of phased missions, failure rates and number of redundancies can vary with time and it becomes more difficult to calculate the exact mission reliability. This problem is identified and an optimisation solution is presented by Vujosevic and Meade [15].

The redundancy issue is also considered by Lee and Hong [16] with derivation of an expression for system reliability. A system is presented whereby the failure rate of a component and added redundancy levels are subject to change during the period of the mission. However this method concentrates on only a simple series and parallel arrangement and performs calculations based on the difference in the number of working components at the start and end of each phase. This technique does not demonstrate the general case of the combination of series and parallel systems as represented by fault trees.

3.2.4 Expected Number of Failures

The expected number of system failures in a single phase mission can be obtained using the method presented in Sections 2.2.3.2 and 2.2.3.3. When considering a multi-phased mission, this parameter becomes more difficult to calculate. The boundary between two phases involves a change in failure logic model. This phase transition may cause the system to fail without the occurrence of a component failure. Montague and Fussell [17] present a method to determine the expected number of system failures for a phased-mission system.

The standard method for obtaining the top event frequency of a system is given in equation (2.8). This is the contribution from the occurrence of at least one minimal cut set minus the contribution of the occurrence of minimal cut sets when the system has already failed. The expected number of system failures is then obtained by the integral of this parameter over a specified time interval in equation (2.13).

This principle is adapted for use in phased-mission systems by Montague and Fussell. The expected number of failures for a phased-mission system with m phases may be expressed in equation (3.10).

$$W_{MISS}(t_0, t_m) = \sum_{j=1}^{m} \int_{t_{j-1}}^{t_j} w_j(t)dt + \sum_{j=1}^{m-1} boundary\ condition\ W_j(t_j) \qquad (3.10)$$

The first term of equation (3.10) represents the number of failures during each phase j of the mission, using a separate integral term to define a new function in each phase j. Montague and Fussell state that this function may be estimated by application of the inclusion-exclusion expansion to the occurrence of phase j cut sets to approximate the rate of phase j failure, $w_j(t)$.

The second term accounts for the occurrence of the top event when a boundary is crossed. This allows for the possibility of failure when entering a new phase due to the basic events that exist from the previous phase. The boundary condition may be expressed as the expected number of system failures in an arbitrary small time interval, Δt, in equation (3.11).

$$W_j(t_j) = (0\ failures\ in\ \Delta t) \cdot P\left[\overline{S}(t_j - \frac{\Delta t}{2}) \cap S(t_j + \frac{\Delta t}{2})\right] + (1\ failure\ in\ \Delta t) \cdot P\left[\overline{S}(t_j - \frac{\Delta t}{2}) \cap S(t_j + \frac{\Delta t}{2})\right] + ... \qquad (3.11)$$

where $\overline{S}(t_j)$ top event does not exist at time t_j

$S(t_j)$ top event exists at time t_j

Taking the limit of equation (3.11) as $\Delta t \to 0$, the expected number of failures across the phase j boundary becomes as given in equation (3.12).

$$W_j(t_j) = P\left[\overline{S}(t_{j-}) \cap S(t_{j+})\right] \qquad (3.12)$$

where $\overline{S}(t_{j-})$ top event does not exist at the instant before the transition

$S(t_{j+})$ top event exists at the instant after the transition

This boundary expression is the probability that the system is in the working state before the transition and is in the failed state after the transition. Since the transition is assumed to be instantaneous, it does not include the possibility that a basic event has changed state during the transition. Equation (3.12) may be expanded to represent every possible combination of a minimal path set existing before the phase boundary and a minimal cut set occurring due to the phase transition, and is summarised in equation (3.13).

Top event does not exist at t_{j-} $\qquad \bar{S}(t_{j-}) = D_{1_{j-1}}(t_{j-}) \cup D_{2_{j-1}}(t_{j-}) \cup \ldots \cup D_{N_{mps\,j-1}}(t_{j-})$

Top event exists at t_{j+} $\qquad S(t_{j+}) = C_{1_j}(t_{j+}) \cup C_{2j}(t_{j+}) \cup \ldots \cup C_{N_{mcs_j}}(t_{j+})$

where $D_{l_{j-1}}(t_{j-})$ Path set *l* of phase *j-1* exists at $t = t_{j-}$

$C_{k_j}(t_{j+})$ Cut set *k* of phase *j* exists at $t = t_{j+}$

$N_{mps_{j-1}}$ Number of minimal path sets in phase *j-1*

Then,

$$\begin{aligned}\bar{S}(t_{j-}) \cap S(t_{j+}) &= [D_{1_{j-1}}(t_{j-}) \cup D_{2_{j-1}}(t_{j-}) \cup \ldots \cup D_{N_{mps\,j-1}}(t_{j-})] \cap [C_{1_j}(t_{j+}) \cup C_{2_j}(t_{j+}) \cup \ldots \cup C_{N_{mcs_j}}(t_{j+})] \\ &= [D_{1_{j-1}}(t_{j-}) \cap C_{1_j}(t_{j+})] \cup [D_{1_{j-1}}(t_{j-}) \cap C_{2_j}(t_{j+})] \ldots \cup [D_{1_{j-1}}(t_{j-}) \cap C_{N_{mcs\,j}}(t_{j+})] \\ &\quad \ldots [D_{N_{mps\,j-1}}(t_{j-}) \cap C_{1_j}(t_{j+})] \cup \ldots [D_{N_{mps\,j-1}}(t_{j-}) \cap C_{N_{mcs\,j}}(t_{j+})]\end{aligned} \tag{3.13}$$

Each path set and cut set pair can be further expanded in terms of basic events. If a basic event is common and complementary between the pair, the intersection becomes zero since it is not possible for an event to change state during the phase transition. The probability of each combination is then calculated by the product of the collective component availabilities or unavailabilities at the time of transition. Since this can be computationally intensive, approximation methods are presented to estimate the expected number of failures across each phase boundary.

The method presented by Montague and Fussell to obtain the expected number of failures in equation (3.10) successfully identifies the problems faced across a phase boundary. The first term in this equation represents the expected number of failures during each phase of the mission, however this cannot be derived using a simple inclusion-exclusion expansion of the occurrence of the phase cut sets since the outcome of previous phases is not accounted for. The second term of equation (3.10) represents the expected number of failures across each phase boundary, and is obtained using equation (3.13). However, the combination of all path and cut sets at each phase transition will be computationally time consuming, and approximation techniques would not generate an accurate result. In general, this method does not produce an accurate calculation of the expected number of mission failures since for each phase calculation the outcome of earlier phases is not included.

3.2.5 Laws of Boolean Phase Algebra

Previous methods have considered the performance of a component *c* as a separate event in different phases, with the system reliability parameters obtained as a product of the event probabilities. A set of Boolean algebraic laws have been developed by Dazhi and Xiaozhong [18] to represent combinations of component behaviour. A basic event *A* may be represented in the following way:

A_j Basic event *A* occurs in phase *j*, i.e. failure occurs in one phase.

$A_{(j)}$ Basic event *A* exists in phase *j*, i.e. failure could have occurred in phases 1..*j*.

If phases *j* and *k* are taken in the order of $j \geq k \geq 1$, the intersection and union concept rules given in equations (3.14), (3.15), and (3.16) can be applied to phased mission systems:

1.
$$\begin{aligned} A_{(j)} &= A_1 \cup A_2 \cup \cdots \cup A_j \\ &= \bigcup_{i=1}^{k} A_i \bigcup_{i=k+1}^{j} A_i \\ &= A_{(k)} \bigcup_{i=k+1}^{j} A_i \end{aligned} \tag{3.14}$$

2.
$$\begin{aligned} A_{(k)} \cap A_{(j)} &= A_{(k)} \cap \left(A_{(k)} \bigcup_{i=k+1}^{j} A_i \right) \\ &= A_{(k)} \bigcup_{i=k+1}^{j} \left(A_{(k)} A_i \right) \\ &= A_{(k)} \end{aligned} \tag{3.15}$$

3. $$A_{(k)} \cup A_{(j)} = A_{(k)} \cup \left(A_{(k)} \bigcup_{i=k+1}^{j} A_i \right)$$

$$= A_{(k)} \bigcup_{i=k+1}^{j} A_i$$

$$= A_{(j)} \qquad (3.16)$$

For the system to be failed in phase *j*, $X_{(j)}$, phase failure could have occurred in any phase up to and including phase *j*. This can be expressed in equation (3.17).

$$X_{(j)} = X_1 \cup X_2 \cup \cdots \cup X_j \qquad (3.17)$$

where X_i is the event that the system fails first in phase *i*

$X_i = \bigcup_{i=1}^{N_{msc\,j}} C_{(i)_j}$, and $C_{(i)_j}$ is the existence of cut set C_i in phase *j*

The mission unreliability can then be expressed in equation (3.18).

$$Q_{MISS} = P[X_{(m)}]$$

$$= P\left(\bigcup_{j=1}^{m} X_j \right) = P\left[\bigcup_{j=1}^{m} \left(\bigcup_{i=1}^{N_{msc\,j}} C_{i_{(j)}} \right) \right] \qquad (3.18)$$

Equation (3.18) automatically implements the cut set cancellation technique presented in Section 3.2.1.1. The Boolean laws described above are applied to the solution of accident sequences by Dazhi and Xiaozhong. Further Boolean laws are presented by Kohda et al [19] using the minimal cut sets and path sets of each phase to eliminate the requirement of converting the mission into a single phase system.

The introduction of Boolean laws to the solution of phased missions overcomes the false assumption made in Esary and Ziehms method that the performance of a component through different phases is separate. The algebraic combination of the separate phase events implements the cut set cancellation method and presents a correct representation of the events that cause phase or mission failure.

Somani and Trivedi [20] present further methods for phased mission system reliability analysis based on Boolean algebraic methods of fault trees. Rather than manipulating a multi-phased mission into an equivalent single phase mission where combination techniques encounter the problem of multiple repeated events, the phase fault trees are solved individually. However, this requires that information must be carried from phase to phase since phases are not independent.

This proposed method is based on the concept of cumulative distribution functions with a mass at the origin. A random variable *X* has a cumulative distribution function with time *t* given by equation (3.19).

$$q_X(t) = (1 - e^{-\lambda T_1}) + e^{-\lambda T_1}(1 - e^{-\lambda t}) \qquad (3.19)$$

where T_1 is the time at the start of the phase

This function has a mass at the origin given by $P(X = 0) = (1 - e^{-\lambda T_1})$ which is the probability that the component exists in the failed state at the start of the phase, and $e^{-\lambda T_1}(1 - e^{-\lambda t})$ represents the continuous part of the function which is the failure probability distribution of the component in the current phase. Failure probabilities of individual components may be represented using such distribution functions.

Somani and Trivedi consider the simple situation where each phase has the same system configuration and failure criteria. The only difference between phases is the component failure rates. Three situations are considered – phase-dependent failure rates, age-dependent failure rates, and random phase durations. Further considerations are made for situations where the system configuration varies between the phases. Reasons for this may include the change of operational level requirements of components, or addition or removal of redundant modules during operation. It is possible that a combination of component failures in a phase will not cause the phase to fail, but on transition to a later phase may cause an instant failure to occur. Four possible scenarios across a phase boundary are considered,

1. A combination of component failures does not lead to system failure in either phase *j* or *j+1*.
2. A combination of component failures leads to system failure in both phase *j* and *j+1*.

3. A combination of component failures does not lead to system failure in phase *j* but leads to system failure in phase *j+1*.
4. A combination of component failures leads to system failure in phase *j* but not in phase *j+1*.

The failure criteria do not change with respect to the failure combination under consideration between phases for the first two situations. The failure combinations in the third situation can also be treated as failure in both phases (as failure will occur at the transition point). The mission reliability for all three cases are treated in the same way as for a mission where all phase configurations are identical by solution of the fault tree for the final phase.

A method is presented to solve the fourth situation to account for the probability of occurrence of failure combinations in phase *j*. The unreliability of a system can be divided into two parts – common failure combinations, and phase failure combinations.

Common Failure Combinations

This involves the probability of the component failure combinations that are common to all phases. If a combination leads to failure in phase *j+1* it is also considered to be a failure combination of phase *j*. The unreliability due to such common failure combinations is solved using the same method as for a mission with phase independent failure criteria, the failure distribution for each component is evaluated and the fault tree for the last phase is solved.

Phase Failure combinations

This involves the probability of failures specific to individual phases - the probability of occurrence of component combinations that cause failure in phase *j* but in no subsequent phases. Phase failure combinations for phase *j* (*PFC_j*), that are treated as success combinations for all the subsequent phases are given by equation (3.20).

$$PFC_j = (...((E_j \cap \overline{E_{j+1}}) \cap \overline{E_{j+2}})... \cap \overline{E_m}) \qquad (3.20)$$

where E_j represents Boolean expression for the failure combinations of phase *j*

This can be simplified in equation (3.21).

$$PFC_j = E_j \cap (\overline{E_{j+1} \cup \ldots \cup E_m}) \tag{3.21}$$

The phase failure combinations for phase j require the same notation as for the Esary and Ziehms' method where a separate symbol (a_j) is assigned to denote the occurrence of an event in each phase j. A new notation is defined, where A_j represents the failure of component A in any phase up to and including phase j,

$$A_j = a_1 + a_2 + \cdots a_j$$

and $\overline{A_j}$ represents the success of component A from the start of the mission to the end of phase j,

$$\overline{A_j} = \overline{a_1} \cdot \overline{a_2} \cdots \overline{a_j}$$

Since the phase failure combinations expression represents both component failure and success events, simplification will merge combinations of both terms. Algebraic rules are required to simplify such success and failure combinations. If i and j are two phases in a mission where $i<j$, the Boolean laws can be summarised in equations (3.22).

$$\begin{array}{ll}
1. & \overline{A_i} \cdot \overline{A_j} \to \overline{A_j} \\
2. & A_i \cdot A_j \to A_i \\
3. & A_i \cdot \overline{A_j} \to 0 \\
4. & \overline{A_i} + \overline{A_j} \to \overline{A_i} \\
5. & A_i + A_j \to A_j \\
6. & \overline{A_i} + A_j \to 1 \\
7. & A_i + \overline{A_j} \to \text{no physical meaning}
\end{array} \tag{3.22}$$

The phased mission Boolean laws presented in equation (3.22) show a deficiency. The sixth law represents the event that component A succeeds up to and including phase i OR component A fails in any phase up to and including phase j. By the Boolean law of complementation, an event or its complement is equal to 1, implying the expression

$\overline{A_i} + A_i \to 1$. Although this sixth law for phased mission algebra is correct, the combination technique could be misleading.

This method also becomes complex when combining terms that cannot be simplified, for example $\overline{A_i} \cdot A_j$. Somani and Trivedi express this as the event that component A is operational until the end of phase *i*, and then fails sometime between the end of phase *i* and the end of phase *j*. This is not consistent with the original definition of A_j as the event that component A fails in any phase up to and including phase *j*. The probability of this combination of events is obtained in equation (3.23).

$$\begin{aligned} P(\overline{A_i} \cdot A_j = 1) &= E[\overline{A_i} \cdot A_j] = E[\overline{A_i} \cdot (1 - \overline{A_j})] \\ &= E[\overline{A_i}] - E[(\overline{A_i} \cdot \overline{A_j})] = P(\overline{A_i} = 1) - P(\overline{A_j} = 1) \end{aligned} \qquad (3.23)$$

It can be seen from equation (3.23) that the probability of event $\overline{A_i} \cdot A_j$ is the same as the probability that component A fails between the end of phase *i* and the end of phase *j*. It would be useful if this term could be directly obtained without the inclusion of the component success probabilities.

The system unreliability is obtained by computing the phase failure combinations for all phases and is given in equation (3.24).

$$Q_{MISS} = P(E_m) + \sum_{j=1}^{m-1} P(PFC_j) \qquad (3.24)$$

The unreliability at the end of each phase *j* can be expressed in equation (3.25).

$$Q_j = \sum_{i=1}^{j} P(PFC_{i,j}) \qquad (3.25)$$

where $PFC_{i,j}$ is the *PFC* of phase *i* (*i*<*j*), assuming *j* is the last phase

$PFC_{i,j} = PFC_{i,j-1} \cap \overline{E_j}$

At a phase transition, a jump in unreliability may be seen. This may be due to more stringent failure criteria in a later phase, and is described as a latent failure.

The method presented by Somani and Trivedi successfully identifies the possible situations that can occur across a phase boundary. The Boolean laws defined in equations (3.22) allow further possible combinations of component failure and success events in a phased mission system, however it can be seen that there are representation problems in the rules. In all previous methods, the event of phase failure would cause failure of the entire mission. This assumption means that it is not possible for the mission to continue after the failure of a phase, and so a phase *j* failure combination could not become a successful combination in phase *j+1*. Somani and Trivedi's method allows the phases of a mission to occur in any order, and so this situation becomes possible. The calculation of the system performance parameters involves the combination of the current phase failure combinations with the success combinations for all subsequent phases. This leads to lengthy calculations for situations where there are numerous phases or cut sets in each phase.

This work is extended by Ma and Trivedi [21] who obtain the mission unreliability in the form of the sum of disjoint products using a computational algorithm and implement the algorithm using the SHARPE software package.

3.2.6 Binary Decision Diagrams

A single phase system can easily be represented in BDD form using the method demonstrated in Section 2.3. When considering the possibility of multiple phases, the state of a component in a phase is dependent on the performance of the component through all previous phases, and the BDD technique becomes more complex.

Trivedi et al [22] present a method whereby this binary decision diagram technique can be applied to missions of multiple phases. The behaviour of a component in a phase is represented by the performance of the component up to and including the phase in question using a series of sub-components as described in Section 3.2.1.

The failure function for component *c* in phase $j, q_{c_j}(t)$, is the probability that component *c* is failed in phase *j*, and is expressed in equation (3.26).

Since all c_i, $i = 1,2,\ldots,j$ are in series,

$$q_{c_j}(t) = \left[1 - \prod_{i=1}^{j-1}\left[1 - q_{c_i}(T_i)\right]\right] + \left[\prod_{i=1}^{j-1}\left[1 - q_{c_i}(T_i)\right]\right] \cdot q_{c_j}(t) \qquad (3.26)$$

where t is measured from the start of phase j, $0 \le t \le T_j$

The first term of equation (3.26) represents the probability that the component has already failed during the previous 1...*j*-1 phases. The second term represents the failure probability distribution of the component in phase *j*.

In the same way as for a single phase mission, an ordering sequence is required to enable the construction of the BDD. Trivedi et al present two possible ordering schemes, where each component *c* is expanded into its series of sub-components in the following ways:

- Forwards Phase-Dependent Operation (PDO): The variables are ordered in the same pattern as the phase order, $c_1, c_2, \ldots, c_m$.
- Backwards Phase-Dependent Operation (PDO): The variables are ordered in the reverse pattern of the phase order, $c_m, c_{m-1}, \ldots, c_1$.

The **ite** structure of the performance of component *c* in two phases *i* and *j* can be represented by E_i and E_j respectively,

$$E_i = \textbf{ite}(c_i, G_1, G_2)$$
$$E_j = \textbf{ite}(c_j, H_1, H_2)$$

The logic operation between E_i and E_j can be represented by BDD manipulations as:

$$\text{Forwards PDO}: \textbf{ite}(c_i, G_1, G_2) \oplus \textbf{ite}(c_j, H_1, H_2) = \textbf{ite}(c_i, G_1 \oplus H_1, G_2 \oplus E_j)$$
$$\text{Backwards PDO}: \textbf{ite}(c_i, G_1, G_2) \oplus \textbf{ite}(c_j, H_1, H_2) = \textbf{ite}(c_j, E_i \oplus H_1, G_2 \oplus H_2)$$

The ordering of variables is very important to the size of a BDD. Methods such as heuristics may be implemented to select the most appropriate or efficient ordering sequence of variables in the BDD. Once the components are ordered, each component is replaced by a series of sub-components in either a forwards or backwards phase ordering pattern. If backwards PDO is used, generally a smaller BDD is produced using Trivedi's approach and common component cancellation is achieved without requiring additional operations.

An algorithm is presented to construct a BDD for a phased mission system:

1. Obtain the failure function for each variable using equation (3.26).
2. Order the mission components using a heuristic method.
3. Generate the BDD for each phase using logic equations.
4. Use phase algebra and the backwards PDO to combine each phase BDD using OR logic to obtain a mission BDD.
5. Calculate the unreliability of the PMS from the mission BDD.

In a backwards PDO BDD, the '0' branches (non-occurrence of the basic events) always links two variables that belong to different components. However, the '1' branches (occurrence of the basic events) can connect nodes in two ways:

1. The '1' branch links variables of different components.
2. The '1' branch links variables of the same component.

Considering a BDD for function G,

$$G = \mathbf{ite}(c_j, G_1, G_2) = c_j \cdot G_1 + \overline{c_j} \cdot G_2$$

Since the '0' branch always links events of different components, G_2 will not represent any event of component c. This implies that c_j and G_2 are always statistically independent events and so,

$$P(\overline{c_j} \cdot G_2 = 1) = P(\overline{c_j} = 1) \cdot P(G_2 = 1)$$

In the case where the '1' branch links nodes from different components, G_1 also does not represent any variable of c, and the same method can be applied as for a single phase system shown in equation (3.27).

$$\begin{aligned}
\mathrm{P}(\mathrm{G}=1) &= \mathrm{E}[\mathrm{G}] = \mathrm{E}[c_j \cdot G_1 + \overline{c_j} \cdot G_2] \\
&= \mathrm{E}[c_j] \cdot \mathrm{E}[G_1] + \mathrm{E}[\overline{c_j}] \cdot \mathrm{E}[G_2] \\
&= \mathrm{E}[G_1] + (1 - \mathrm{E}[c_j]) \cdot (\mathrm{E}[G_2] - \mathrm{E}[G_1]) \\
&= \mathrm{P}(G_1 = 1) + (1 - \mathrm{P}(c_j = 1)) \cdot (\mathrm{P}(G_2 = 1) - \mathrm{P}(G_1 = 1)) \qquad (3.27)
\end{aligned}$$

For a '1' branch that links two nodes belonging to the same component, G_1 will also be dependent on a variable of c. Since the two events are not independent, the following structures apply:

$$\mathrm{G} = \mathbf{ite}(c_j, G_1, G_2) = c_j \cdot G_1 + \overline{c_j} \cdot G_2$$

$$G_1 = \mathbf{ite}(c_i, H_1, H_2) = c_i \cdot H_1 + \overline{c_i} \cdot H_2$$

Also,

$$\begin{aligned}
\mathrm{P}(\mathrm{G}=1) &= \mathrm{E}[\mathrm{G}] = \mathrm{E}[c_j \cdot G_1 + \overline{c_j} \cdot G_2] \\
&= \mathrm{E}[c_j \cdot (c_i \cdot H_1 + \overline{c_i} \cdot H_2) + \mathrm{E}[\overline{c_j}] \cdot \mathrm{E}[G_2] \\
&= \mathrm{E}[c_j \cdot c_i \cdot H_1 + c_j \cdot \overline{c_i} \cdot H_2) + \mathrm{E}[\overline{c_j}] \cdot \mathrm{E}[G_2]
\end{aligned}$$

Using the rules of phase algebra in equations (3.22), a branch linking two nodes belonging to the same component is given in equation (3.28).

$$\begin{aligned}
\mathrm{P}(\mathrm{G}=1) &= \mathrm{E}[c_i \cdot H_1 + \overline{c_i} \cdot H_2] - \mathrm{E}[\overline{c_j}] \cdot \mathrm{E}[H_2] + \mathrm{E}[\overline{c_j}] \cdot \mathrm{E}[G_2] \\
&= \mathrm{E}[G_1] + \mathrm{E}[\overline{c_j}] \cdot (\mathrm{E}[G_2] - \mathrm{E}[H_2]) \\
&= \mathrm{P}(G_1 = 1) + (1 - \mathrm{P}(c_j = 1)) \cdot (\mathrm{P}(G_2 = 1) - \mathrm{P}(H_2 = 1)) \qquad (3.28)
\end{aligned}$$

Depending on whether the '1' branch links events of different components or the same component, equations (3.27) or (3.28) respectively would be applied.

Trivedi et al also identify the possibility of latent failures across phase boundaries. The phase BDDs can be used to obtain the system unreliability at the instant before and after the phase boundary to calculate the unreliability jump across the phase transition.

The limitations of Trivedi et al's approach are identified by Xing and Dugan [23]. The developed phase dependent operation will only generate the correct phased mission system binary decision diagram if the following rules are adhered to:

1. Orderings implemented in the generation of each phase BDD must be consistent or the same for all phases.

2. Variables belonging to the same component in different phases must stay together in the ordering scheme. This is achieved by expanding each component into sub-component form after the ordering of components has been defined using heuristics.

If an arbitrary ordering scheme is implemented, the phase dependent operation is not complete enough to combine the single phase BDDs into an equivalent mission BDD. The problem with the method is that a BDD with backwards PDO may represent an impossible situation, for example the success of an event in a later phase ordered before the failure of the same event in an earlier phase. An example mission to demonstrate this is shown in Figure 3.8.

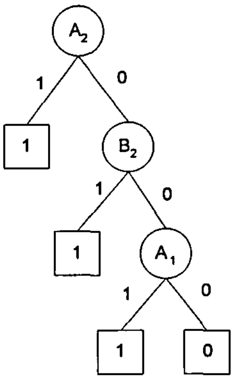


Figure 3.8 BDD Ordering Pattern

If A is successful in phase 2, it is not possible for it to have failed in phase 1. Node combinations that represent such impossibilities can be removed from the BDD. The incoming branch to each impossible node is then passed to the node on its right '0' son, since this implies for the component to work in a later phase, it must have worked through earlier phases. Any nodes below the left son are also removed, along with any redundant nodes. The example in Figure 3.8 becomes as shown in Figure 3.9.

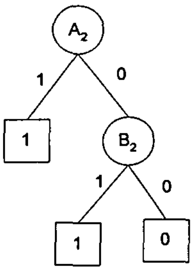


Figure 3.9 BDD of Figure 3.8 with Impossible Nodes Removed

A similar method must be applied to remove impossible nodes using the forwards ordering scheme.

If all impossible node combinations are removed from the BDD, any arbitrary ordering scheme may be used to obtain the final phased mission BDD.

The BDD method presented by Trivedi et al demonstrates an efficient representation of the failure logic of a phased mission. Xing and Dugan identify some limitations in this method by the way in which the variables are ordered. A further deficiency is that each phase j BDD is constructed from only the phase j failure conditions. Although each phase j basic event is expanded into its series of sub-events, the outcome of previous phases is not accounted for and so the phase BDDs will be incorrect.

3.2.7 Imperfect Coverage

Xing and Dugan [24], [25] consider the possibility of imperfect coverage in phased mission analysis. This means that a single point failure could cause system failure despite the fault-tolerant mechanisms in place. A system can exhibit one of two failure modes: *covered failure* which is local to the affected component and does not lead to system failure, and *uncovered failure* which causes immediate system failure. A generalized phased-mission technique is proposed to take these factors into account.

3.2.8 Markov Methods

An alternative to combinatorial techniques is by application of Markov methods. There are two general approaches to the solution of multi-phased missions using Markov methods; treating each phase individually, or analysing the entire mission with a single model. If the phases of the mission are treated separately, each individual Markov model must be solved separately and linked by a state probability vector. The alternative is to solve a single large model with state space at least equal to the size of the sum of the components in each individual phase model. This problem is considered by Dugan [26] who presents a method to construct a single continuous-time discrete-space Markov model for phased mission systems where the state space is the size of the union of the components in each phase model. The

Markov model is constructed from the set of phase fault trees, and can be used to calculate many reliability measures.

The example in Figure 3.4 may be examined with the following assumptions:

- Failure rates for the components are constant for the duration of the phase, but can be different for each phase.
- The system fails due to failure in any phase of the mission.
- Phase change times are deterministic.

Problems are encountered using this Markov model when a set of components is not consistent between phases, or when components are not subject to failure in a phase, since the system states do not match. The phase fault trees of a mission represent the failure conditions of the system and can be converted to Markov chains for further analysis. The phase fault trees in Figure 3.7 can be converted to separate Markov models with system states representing the states of components A, B, and C in the form {A,B,C} with 0 as working and 1 as failed in Figure 3.10.

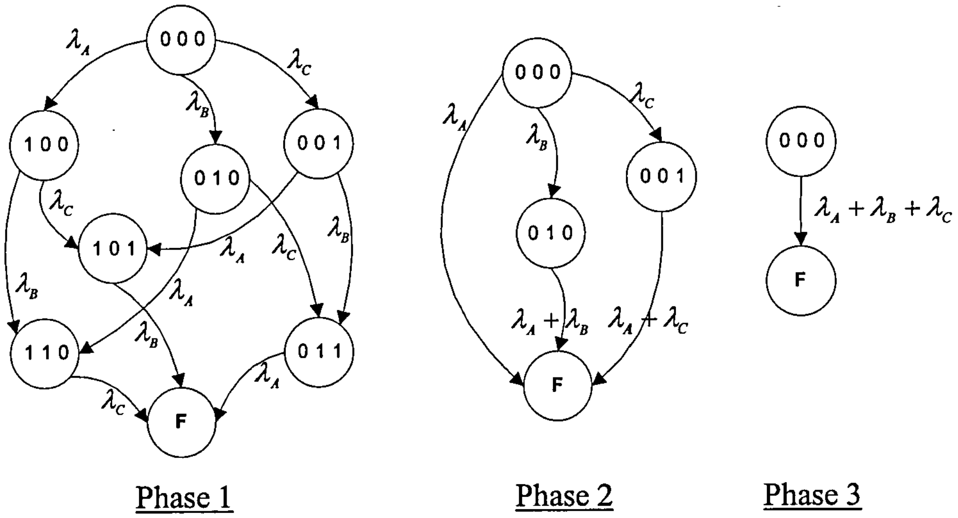


Figure 3.10 Phase Markov Models for Figure 3.4

To combine the three separate Markov models into a single mission Markov model, a multiplicative factor Φ_i is appended to each phase i transition. The combined Markov chain has a state space defined by the union of the individual phase Markov models, and transitions that are defined by the sum of corresponding phase transitions, and is given in Figure 3.11.

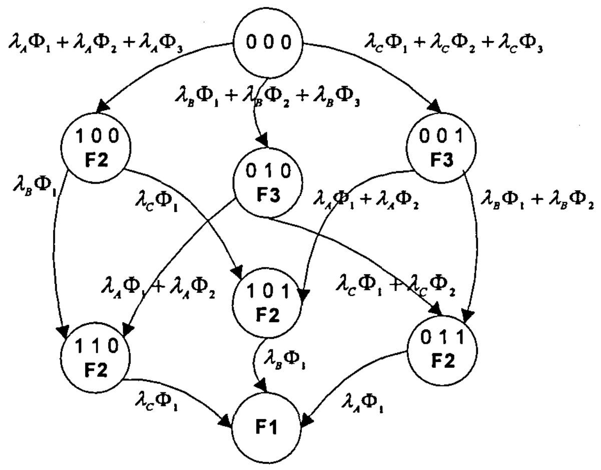

$\lambda_A\Phi_1 + \lambda_A\Phi_2 + \lambda_A\Phi_3$
0 0 0
$\lambda_C\Phi_1 + \lambda_C\Phi_2 + \lambda_C\Phi_3$
$\lambda_B\Phi_1 + \lambda_B\Phi_2 + \lambda_B\Phi_3$
1 0 0
F2
0 1 0
F3
0 0 1
F3
$\lambda_B\Phi_1$
$\lambda_C\Phi_1$
$\lambda_A\Phi_1 + \lambda_A\Phi_2$
$\lambda_B\Phi_1 + \lambda_B\Phi_2$
$\lambda_A\Phi_1 + \lambda_A\Phi_2$
1 0 1
F2
$\lambda_C\Phi_1 + \lambda_C\Phi_2$
1 1 0
F2
0 1 1
F2
$\lambda_B\Phi_1$
$\lambda_C\Phi_1$
F1
$\lambda_A\Phi_1$

Figure 3.11 Combined Mission Markov Model

This combined model may be solved using a standard numerical technique. For solutions to phase *i* ($t_{i-1} \leq t \leq t_i$), Φ_i is set to one, and all other Φ_j, $i \neq j$ are set to zero thus removing any transition that does not belong to the current phase. The state space does not change and rather than transforming the state probabilities, the state transitions change as the phases change.

In the case that the components are not the same in each phase, a full Markov state listing is formed by the expansion of all components that contribute at some point during the mission. For each source state in the combined Markov model, the destination state corresponding to the failure of a component can be different in different phases, and so each component must be considered several times for each phase of the mission. A state in one phase that causes the system to fail is not necessarily a failure state of previous phases. However, if a system failure state is reached in phase *i*, it becomes absorbing for all later phases. The system states are then defined as 'operational for all phases' or 'failed in phase *i*', where phase *i* is the first phase in which the system fails. Dugan also considers this method for systems with imperfect coverage.

The final combined mission Markov model results in a set of differential equations which must be solved numerically using methods such as Runge-Kutta. The initial conditions for the first phase are known, and the failure and success probability of each phase can be obtained using the Markov state probabilities at the end of the phase. The final state probability vector of each phase is passed directly to the following phase for further analysis.

This approach provides an efficient representation of the multi-phased mission. The construction of a single model eliminates the problems faced across a phase boundary if the state-space of the phases is not the same. However, the single model has a state space defined by all components required in the mission. In some cases a mission may require a large number of components that are not necessarily required through all phases. The resulting state space of the single model will become large and the set of differential equations will also increase and become very complex to solve. It is also not correct to assume that if a system failure state is reached in phase *i*, it becomes absorbing for all later phases. A state may be possible and reachable in a later phase even when it was an absorbing state in an earlier phase. The possibility of transition failures is not identified in this model.

3.2.9 Modular Solution of Missions with Static and Dynamic Phases

All of the methods discussed so far have applied to only static phases, where AND and OR gates are used to represent the phase failure configuration. In some cases, failure will only occur if components fail in a specific order, and dynamic gates are required. The possibility of static and dynamic phases in a multi-phased mission is considered by Ou and Dugan [27]. A modular solution is presented to combine BDD solution techniques for static modules with Markov methods for dynamic modules. The main deficiency of this method is that the modules must represent an independent subtree throughout all phases. In many cases, the configuration of a phased mission system will vary considerably across phases, and it will not be possible to identify distinct modules through the mission. Each module is solved using the same technique throughout the phases, and so the methods already identified can be implemented.

3.2.10 Summary

Much research has been employed into the analysis of non-repairable phased mission systems. The main features of the methods presented are:

- The expansion of each basic event into a series of sub-events representing the separate performance of a component in each phase of the mission.

- Transformation of a multi-phased mission into an equivalent single phase mission to allow existing fault tree techniques to be implemented.

- Cut set cancellation for cut sets of an earlier phase that contain cut sets of a later phase.

- Parameter of interest is mission success, either by full calculation or appropriate approximation techniques using negative exponential component failure distributions.

- Phase changes are assumed to be instantaneous, and failure rates are assumed to be constant within each phase.

- Boolean algebra phase laws can be applied to combine component success and failure events through multiple phases.

- Binary decision diagrams can be applied to provide an alternative representation of the top event of phase and mission failure with appropriate ordering schemes.

- Markov methods represent the dynamic nature of component failures.

However, it is also seen that the methods presented result in some deficiencies. The cut set cancellation method by Esary and Ziehms allows analysis only for the total mission rather than for individual phases. Also the concentration of research into mission success does not identify the causes of individual phase failure. The BDD approach is seen to provide an efficient representation of mission failure and success, but does not take account of the outcome of previous phases when representing each individual phase BDD. It would be useful to be able to identify the causes and quantify each phase failure with account for previous phase successes, as well as for the entire mission.

The Markov model suffers a state explosion problem as the number of components and phases in the mission increases. As components are not necessarily required through all phases of the mission, it would become time consuming to expand all possible states for every component in the mission, and the single Markov model presented would become very complex.

A simple combinatorial method is required to allow straightforward qualification and quantification of both phase and mission reliability to account for the dependency between phases.

3.3 Repairable Systems

The methods presented so far have only been appropriate for non-repairable systems. In systems on-board an aircraft or spacecraft it would be very difficult to perform a repair whilst carrying out a mission, and so these methods are suitable for such system analysis. However, in many practical situations it will be possible for maintenance to be performed on a system, and the change in requirements between phases of a multi-phased mission leads to the possibility of component repair. Methods presented for analysis of repairable multi-phased missions are discussed in the following sections.

3.3.1 Combinatorial Approaches

An extension of the work by Trivedi and Somani [20] is presented using combinatorial approaches for the solution of repairable components in a multi-phased mission by Somani [28]. However, this approach is very limited since a component can only be repaired if it is not required in a particular phase. Whilst a component is required for successful operation of a phase, repair cannot be initiated.

If c is a component whose failure and repair rates in phase p are denoted by λ_{c_p} and μ_{c_p}, the failure and repair times are assumed to follow an exponential distribution. The definitions in equations (3.29) are made:

$$\alpha_{c_p}(t) = e^{-(\lambda_{c_p}+\mu_{c_p})*t} \quad \text{and} \quad \beta_{c_p} = \frac{\mu_{c_p}}{\mu_{c_p}+\lambda_{c_p}} \tag{3.29}$$

where t is the time after the system entered phase p.

Four possible cases must be considered for the component in a phase – the component may begin in the working or failed state, and may end in either the working or failed state. Using notation whereby the first suffix is the name of the component, the second represents the state of the component at the start of the phase (u=up, f =failed), the third represents the state of the component at the end of the phase and the fourth is the phase number, formulae are developed.

If the component c is up at the start of the phase, the probability that it will be in the working or failed state at the end of the phase is given by:

$$p_{c_{uup}}(t)=\alpha_{c_p}(t)+\beta_{c_p}*(1-\alpha_{c_p}(t)) \qquad p_{c_{ufp}}(t)=(1-\alpha_{c_p}(t))*(1-\beta_{c_p})$$

If the component c is failed at the start of the phase, the probability that it will be in the working or failed state at the end of the phase is given by:

$$p_{c_{fup}}(t)=\beta_{c_p}*(1-\alpha_{c_p}(t)) \qquad p_{c_{ffp}}(t)=1-\beta_{c_p}*(1-\alpha_{c_p}(t))$$

If the probability that component c is up at the start of a phase is represented by $p_{c_{ubp}}$, and down at the start of a phase is represented by $p_{c_{fbp}}$ then the state of the component after time t has elapsed may be represented by equations (3.30).

$$P_{c_{uep}}(t) = p_{X_{ubp}} * p_{c_{uup}}(t) + p_{c_{fbp}} * p_{c_{fup}}(t)$$

$$P_{c_{fep}}(t) = p_{c_{ubp}} * p_{c_{ufp}}(t) + p_{c_{fbp}} * p_{c_{ffp}}(t) \qquad (3.30)$$

The main deficiency of this approach is that the reparability is not considered for all components, and is only applicable to the idle components in a phase. A method is required to model the situation where any components in a phase can be repaired.

Another combinatorial approach is presented by Vaurio [29] who considers calculations for the system unavailability and failure intensity for each phase of the mission separately. The unavailability and failure intensity for a component c that is known to be working at the start of the mission is obtained using Laplace transforms and given in equations (3.31) and (3.32) respectively.

$$q_c(t) = \frac{\lambda_c}{\lambda_c + \upsilon_c}\left(1 - e^{-(\lambda_c+\upsilon_c)t}\right) \tag{3.31}$$

$$w_c(t) = \frac{\lambda_c}{\lambda_c + \upsilon_c}\left(\upsilon_c + \lambda_c e^{-(\lambda_c+\upsilon_c)t}\right) \tag{3.32}$$

This method does not model the dependencies that arise in repairable systems and so the component unavailability is only an approximation. The unavailability function for phase *j*, *Qj*, is obtained for each phase interval using the phase specific fault tree, where $t \in (t_{j-1}, t_j)$. The system failure intensity in each phase and expected number of phase failures is then calculated using equations (3.33).

$$w_j(t) = \sum_{\substack{i=1 \\ i \text{ initiating event}}}^{N_i} \frac{\partial Q_j(t)}{\partial q_i} w_i(t) \qquad W_j(t_{j-1}, t_j) = \int_{t_{j-1}}^{t_j} w_j(t')\, dt' \tag{3.33}$$

At each phase boundary, a joint fault tree is constructed to represent the top event of phase *j* failure (*Zj*) AND phase *j+1* failure (*Zj+1*), $Z_j \cap Z_{j+1}$. The probability of occurrence of this top event is then calculated using the basic event probabilities at *t=tj*. The probability of system failure at the phase transition, Δ_j, can then be represented by equation (3.34).

$$\begin{aligned}\Delta_j &= [P(Z_{j+1}) - P(Z_j \cap Z_{j+1})]_{at\, t_j} \\ &= Q_{j+1}(t_j) - P(Z_j \cap Z_{j+1})\,|_{at\, t_j}\end{aligned} \tag{3.34}$$

The expected number of mission failures is then obtained by equation (3.35).

$$W_{MISS}(0, t_m) = \Delta_0 + \sum_{j=1}^{m-1} \Delta_j + \sum_{j=1}^{m} W_j \tag{3.35}$$

It can easily be seen that this method does not model the dependencies that arise in the situation of repairable systems. The phase unavailability and failure intensities will be approximations of the exact values, and thus not very useful in the solution of many reliability problems. Also the phase calculations involved do not include the outcome of previous phases.

3.3.2 Markov Methods

The consideration of repairable phases in a multi-phased mission means that the phase algebra can no longer be applied. In such circumstances, combinatorial methods may not be used as only approximations could be calculated, and so other techniques must be employed. The Markov approach is a very useful technique for the solution of repairable systems, and much research has been undertaken in this area. Many applications of the Markov approach in phased mission systems have been considered.

The reliability of a mission cannot be obtained by the simple multiplication of the individual phase reliabilities since at the phase change times, for the system to function, it must occupy a state that allows both of the involved phases to be successful. Markov methods offer a means of overcoming this.

3.3.2.1 Homogeneous Markov Model

The homogeneous property of a Markov model means that the state transitions are not dependent on time, and are instead governed by a constant rate. Certain assumptions must be made:

- The system is comprised of elements that may be good or bad with independently exponentially distributed failure and repair times.
- Repair of a component restores it to the perfect condition.
- Each phase may have more than one purpose. However if a system fails in a phase, the mission will fail.
- Transition between successive phases occurs instantaneously.

Early investigations into the use of Markov methods to solve phased mission problems were carried out by Clarotti et al [30].

Consider the example in Figure 3.12,

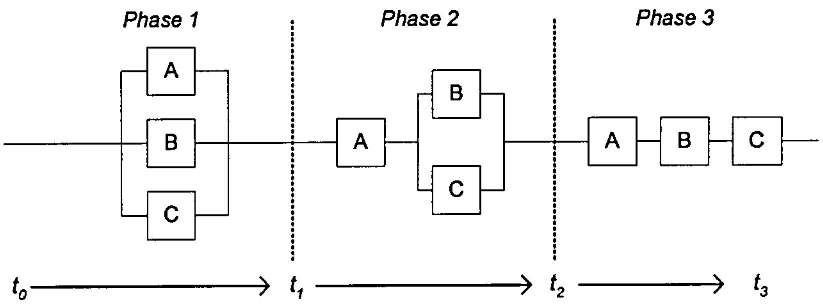


Figure 3.12 Simple Three-Phased Mission

There are eight possible states of the system, $S_1..S_8$, defined in terms of the states of its components. The states are defined in Table 3.1.

State	A	B	C
S_1	0	0	0
S_2	1	0	0
S_3	0	1	0
S_4	1	1	0
S_5	0	0	1
S_6	1	0	1
S_7	0	1	1
S_8	1	1	1

where 0 working
1 failed

Table 3.1 System States of Component Combinations

Considering each of the three phases:

- Phase 1 $(0, t_1)$

The probability vector expresses the likelihood that the system resides in each of the eight possible states. The mission begins with all components in the working state, and so the initial condition probability vector, **P**(0), can be represented by equation (3.36).

$$\mathbf{P}(0) = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0] \qquad (3.36)$$

For the system to function successfully during the first phase, at least one component must be in the working state (Figure 3.12). If all three components reside in the failed state at the same time, the phase will fail. The state representative of this phase failure is S_8 where no components are functional.

In matrix form as defined in equation (2.44), the evolution of phase 1 may be represented by matrix equations (3.37).

$$\begin{bmatrix} \dot{P}_{S_1}(t) \\ \dot{P}_{S_2}(t) \\ \dot{P}_{S_3}(t) \\ \dot{P}_{S_4}(t) \\ \dot{P}_{S_5}(t) \\ \dot{P}_{S_6}(t) \\ \dot{P}_{S_7}(t) \\ \dot{P}_{S_8}(t) \end{bmatrix}^T = \begin{bmatrix} P_{S_1}(t) \\ P_{S_2}(t) \\ P_{S_3}(t) \\ P_{S_4}(t) \\ P_{S_5}(t) \\ P_{S_6}(t) \\ P_{S_7}(t) \\ P_{S_8}(t) \end{bmatrix}^T \begin{bmatrix} -\sum_1 & \lambda_A & \lambda_B & 0 & \lambda_C & 0 & 0 & 0 \\ \upsilon_A & -\sum_2 & 0 & \lambda_B & 0 & \lambda_C & 0 & 0 \\ \upsilon_B & 0 & -\sum_3 & \lambda_A & 0 & 0 & \lambda_C & 0 \\ 0 & \upsilon_B & \upsilon_A & -\sum_4 & 0 & 0 & 0 & \lambda_C \\ \upsilon_C & 0 & 0 & 0 & -\sum_5 & \lambda_A & \lambda_B & 0 \\ 0 & \upsilon_C & 0 & 0 & \upsilon_A & -\sum_6 & 0 & \lambda_B \\ 0 & 0 & \upsilon_C & 0 & \upsilon_B & 0 & -\sum_7 & \lambda_A \\ 0 & 0 & 0 & - & 0 & - & - & - \end{bmatrix} \qquad (3.37)$$

where: 0 represents an impossible state transition

$-$ represents an absorbing state (no transition is possible out of the state)

$\sum_i$ is the sum of the non-diagonal entries in the i^{th} row

At the phase change time t_1, the system must occupy a successful state for both phases 1 and 2. For phase 2 success (Figure 3.12), component A must be working along with either component B or C. To successfully be able to enter phase 2, the system must reside in one of the states representative of this, S_1, S_3, or S_5 in Table 3.1. The probability of the system residing in each of these states at $t=t_1$ is represented by $P_{S_1}(t_1)$, $P_{S_3}(t_1)$, and $P_{S_5}(t_1)$ respectively. The probability that the system successfully completes the first phase and is able to enter the second phase is given by the sum of these probabilities in equation (3.38).

$$R(t_1) = P_{S_1}(t_1) + P_{S_3}(t_1) + P_{S_5}(t_1) \qquad (3.38)$$

- Phase 2 (t_1, t_2)

The system will only begin this second phase if it is in one of the states S_1, S_3, or S_5, and will evolve from these states at the start of the phase. All other states are considered to be absorbing at the phase change time since mission failure would be caused. The vector of initial phase 2 system state probabilities has all entries equal to zero apart from those corresponding to working states for both phases 1 and 2, $P_{S_1}(t_1), P_{S_3}(t_1)$, and $P_{S_5}(t_1)$, and is shown in equation (3.39).

$$\mathbf{P}(t_1) = [\,P_{S_1}(t_1)\;\; 0\;\; P_{S_3}(t_1)\;\; 0\;\; P_{S_5}(t_1)\;\; 0\; 0\; 0] \qquad (3.39)$$

The matrix equations for solution of phase 2 are given in equation (3.40).

$$\begin{bmatrix} \dot{P}_{S_1}(t) \\ \dot{P}_{S_2}(t) \\ \dot{P}_{S_3}(t) \\ \dot{P}_{S_4}(t) \\ \dot{P}_{S_5}(t) \\ \dot{P}_{S_6}(t) \\ \dot{P}_{S_7}(t) \\ \dot{P}_{S_8}(t) \end{bmatrix}^T = \begin{bmatrix} P_{S_1}(t) \\ P_{S_2}(t) \\ P_{S_3}(t) \\ P_{S_4}(t) \\ P_{S_5}(t) \\ P_{S_6}(t) \\ P_{S_7}(t) \\ P_{S_8}(t) \end{bmatrix}^T \begin{bmatrix} -\sum_1 & \lambda_A & \lambda_B & 0 & \lambda_C & 0 & 0 & 0 \\ - & -\sum_2 & 0 & \lambda_B & 0 & \lambda_C & 0 & 0 \\ \upsilon_B & 0 & -\sum_3 & \lambda_A & 0 & 0 & \lambda_C & 0 \\ 0 & - & - & -\sum_4 & 0 & 0 & 0 & \lambda_C \\ \upsilon_C & 0 & 0 & 0 & -\sum_5 & \lambda_A & \lambda_B & 0 \\ 0 & - & 0 & 0 & - & -\sum_6 & 0 & \lambda_B \\ 0 & 0 & - & 0 & - & 0 & -\sum_7 & \lambda_A \\ 0 & 0 & 0 & - & 0 & - & - & - \end{bmatrix} \qquad (3.40)$$

For the second phase to be considered successful, the system must occupy a working state for both phases 2 and 3 at the end of the phase. For successful entry to phase 3 (Figure 3.12), all components must be working (state S_1) at time t_2 when it enters the third and final phase. The probability that the system has successfully achieved the second phase and is able to enter the third and final phase is given in equation (3.41).

$$R(t_2) = P_{S_1}(t_2) \qquad (3.41)$$

- Phase 3 (t_2, t_f)

To successfully complete the mission, the system must remain in state S_1 with all components working for the duration of the phase. The initial phase 3 state probability vector is given in equation (3.42).

$$\mathbf{P}(t_2) = [\,P_{S_1}(t_2)\ 0\,0\,0\,0\,0\,0\,0]\tag{3.42}$$

The matrix equations for solution of phase 3 are given in equation (3.43).

$$\begin{bmatrix} \dot{P}_{S_1}(t) \\ \dot{P}_{S_2}(t) \\ \dot{P}_{S_3}(t) \\ \dot{P}_{S_4}(t) \\ \dot{P}_{S_5}(t) \\ \dot{P}_{S_6}(t) \\ \dot{P}_{S_7}(t) \\ \dot{P}_{S_8}(t) \end{bmatrix}^T = \begin{bmatrix} P_{S_1}(t) \\ P_{S_2}(t) \\ P_{S_3}(t) \\ P_{S_4}(t) \\ P_{S_5}(t) \\ P_{S_6}(t) \\ P_{S_7}(t) \\ P_{S_8}(t) \end{bmatrix}^T \begin{bmatrix} -\sum_1 & \lambda_A & \lambda_B & 0 & \lambda_C & 0 & 0 & 0 \\ - & -\sum_2 & 0 & \lambda_B & 0 & \lambda_C & 0 & 0 \\ - & 0 & -\sum_3 & \lambda_A & 0 & 0 & \lambda_C & 0 \\ 0 & - & - & -\sum_4 & 0 & 0 & 0 & \lambda_C \\ - & 0 & 0 & 0 & -\sum_5 & \lambda_A & \lambda_B & 0 \\ 0 & - & 0 & 0 & - & -\sum_6 & 0 & \lambda_B \\ 0 & 0 & - & 0 & - & 0 & -\sum_7 & \lambda_A \\ 0 & 0 & 0 & - & 0 & - & - & - \end{bmatrix}\tag{3.43}$$

The success probability of the mission is given by the probability that the system resides in state S_1 with all components working at the end of the mission $(t=t_3)$ in equation (3.44)

$$R_{MISS} = P_{S_1}(t_3)\tag{3.44}$$

This method identifies that the main difference between the application of a Markov model to a single-phase system and a multi-phased system is the need to determine the initial conditions at the start of each phase. This initial condition problem is also identified by Gray [31] using parallel subgroups with identical components. The deficiencies in the method presented by Clarotti et al. are that the entire mission is solved using phase Markov models with the same state space. In some cases, the number of components required in a mission will be very large, and not all components will be required in every phase. The resulting Markov model will become very complex and difficult to solve. Also, the phase reliabilities are determined by the probability that the system is in a final successful state that is also a success state of the subsequent phase. The correct reliability should be obtained by the probability that the phase has completed successfully, regardless of the requirements for the following phase. The failure upon transition to the following phase will contribute to the subsequent phase failure.

3.3.2.1.1 Random Phase Durations

The methods presented so far have assumed that the duration of phases in a multi-phased mission are deterministic and thus defined at the start of the mission. Wells and Bryant [32] begin to consider the principle of random durations by application to only a single-phase system. Alam and Al-Saggaf [33] consider two approaches to determine an appropriate description of the marginal distributions of the mission phase change times (MPCTs) when the phase-change times are random variables.

The first approach investigates a general formula for the joint probability density function of the MPCTs, which may be statistically dependent. The second models the MPCTs as order statistics of a continuous random variable. The solution to a probabilistic MPCT is then similar to the deterministic approach. The example demonstrated in Section 3.3.2.1 by Clarotti et al. produced the probability that the system completed each phase successfully, and was able to enter the next phase. The initial conditions in each phase were given in equations (3.36), (3.39), and (3.42). The solutions for probabilistic MPCTs require a modification to be made to these initial conditions, shown in equations (3.45).

$$\begin{array}{lccccccccl}
\mathbf{P}(0) = [& 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0]^T \\
\mathbf{P}(T_1) = [& \mathrm{E}\{\mathrm{P}_1(T_1)\} & 0 & \mathrm{E}\{\mathrm{P}_3(T_1)\} & 0 & \mathrm{E}\{\mathrm{P}_5(T_1)\} & 0 & 0 & 0]^T \\
\mathbf{P}(T_2) = [& \mathrm{E}\{\mathrm{P}_1(T_2)\} & 0 & 0 & 0 & 0 & 0 & 0 & 0]^T
\end{array} \tag{3.45}$$

where T_j is the random variable of the mission phase change time for phase j

The expected probability values are obtained using the probability density functions of the random phase change time variables over the phase durations. This method is further developed by Kim and Park [34] using the system eigenvalues for solution to the differential equations established by the Markov model.

Random phase durations are also considered by Somani et al [35] using phase Markov models. The change in system failure criteria between individual phase Markov models requires mapping of the system states from phase i to phase $i+1$. The reliability of the mission is then obtained by the successful system state probabilities at the end of the final phase.

It is possible that for a particular state in a phase, there may not be an equivalent state in the immediately succeeding phase. Similarly, there may be numerous system states that have the same equivalent state in the next phase. Such situations arise due to the operational requirements of the components through the phases. Components may only be required in certain phases of the mission, and also redundancy and spares may be added into particular phases. The mapping of system states between phases can be implemented using the Hybrid Automated Reliability Predictor (HARP) software for phased mission systems, and is discussed by Somani et al.

In summary, the time-homogeneous Markov model provides a suitable method for the solution of phased mission systems where each phase has the same state space but may have different failure and repair characteristics. The phase models can be combined sequentially, and the success initiation of a phase depends on the probability that the system resides in a successful state for both phases across the transition. The state probability vector at the end of each phase represents the phase success or failure probability and is linearly transformed into the initial probability vector for the next phase. The state probability vector at the end of the last phase represents the mission success or failure probability. The limitation of this approach is that the state space is defined by all components required in the mission, and so can be susceptible to state explosion problems. It would be useful if only the components required in a phase were included in each phase model.

3.3.2.1.2 State Dependent Phase Sequences

It is possible that phases may have a pre-determined time duration, but the next phase to be performed is chosen depending on the system state. This is discussed by Mura and Bondavalli [36] who present a two-level analysis method of a phased mission system. The higher level method models the structure of the mission with regards to only the pattern of phases, and the lower level method models the configuration of the individual phases.

The components can be subject to different failure and repair rates in each phase due to environmental conditions. Since both remain constant through the phase duration, the conditions are homogeneous within each phase. The order of phases in the mission can be dynamically adjusted depending on the state of the system at the end of a phase. An example system is presented of the case study of a spacecraft with phases:

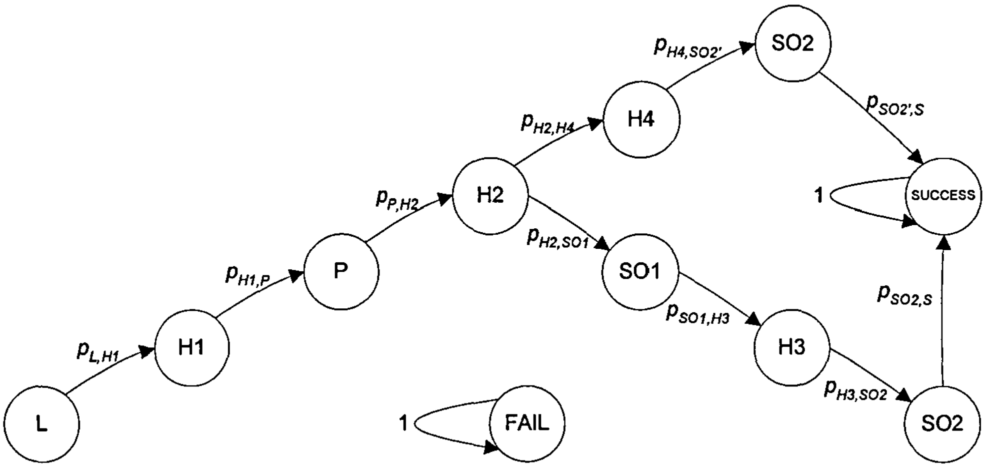
Launch (L): Launch of spacecraft. Short phase with stressing conditions.

Hibernation (H): Long dormancy periods for cruise navigation characterised by minimal activity.

Planet (P): In range of planet. Short phase with stressing conditions.

Scientific Observations (SO): Conducted while cruising in close proximity to space objects and represent the goals of the mission.

The upper level model of the spacecraft mission is given in Figure 3.13. The failure of any phase causes failure of the mission, but this is not represented in this upper level model since only the possible phase sequences need to be clarified.



where $p_{S1,S2}$ is the probability of executing state *S2* after state *S1*

Figure 3.13 Upper-Level Model of a Spacecraft Mission

Each phase requires a minimum number of processors to function successfully. The requirements can be summarised as:

Phase		Number of Processors Required
Hibernation		1 (2 if possible)
Launch		3
Planet		3
Scientific Observations	Cruise	3
	Perform Observations	1

There are 4 identical processors to meet the requirements of the phases. The primary objective is SO2 which must be performed, and SO1 is a secondary goal. At the end of phase H2 if there are any faulty processors, SO1 will be skipped and the next phase to be performed will be H4. If there are no faulty processors, the system is capable of executing SO1 and so this will be the next phase. The determination of the subsequent phase to H2 is therefore state dependent. Reward rates can be cumulated to determine the benefits when a particular phase is executed.

The lower level models can be represented using generalised stochastic petri nets, and translated into a continuous time Markov model. Each state in phase H, L, and P of the Markov model can be represented by the number of working, spare, and failed components in the form: {#Working, #Spare, #Failed}. {F} is the absorbing failure state. In the SO phases, since all components are required, the states are represented by the number of working and failed components in the form: {#Working, #Failed}.

A separate phase transition model is presented between phases to map the final state probabilities of one phase to the initial state probabilities of the subsequent phase. If there is no choice of possible following phases, such as between phases H1 and P, a deterministic model is applied. For the transition between phases H1 and P, with the probability of successful reconfiguration denoted by *c*, the non-failure states would be mapped as shown in Figure 3.14.

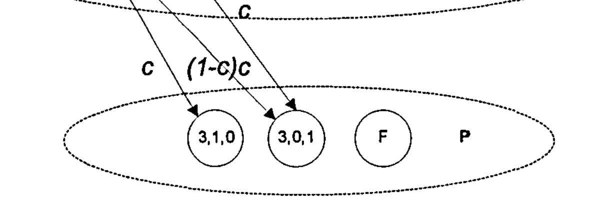


Figure 3.14 Deterministic Phase Transition model from H1 to P

Since three processors are required in phase P, a successful transition from phase H1 will only occur if there are sufficient working or spare components to satisfy the phase P requirement. The mapping technique of this deterministic model can be translated into a transition matrix where the number of rows is equal to the number of states in the originating phase, and the number of columns is equal to the number of states in the successive phase. The entries in the matrix represent the probability on each arc of the phase transition model.

A probabilistic phase transition model represents the state dependencies between phases, and can be shown for the possible transitions from phase H2 in Figure 3.15.

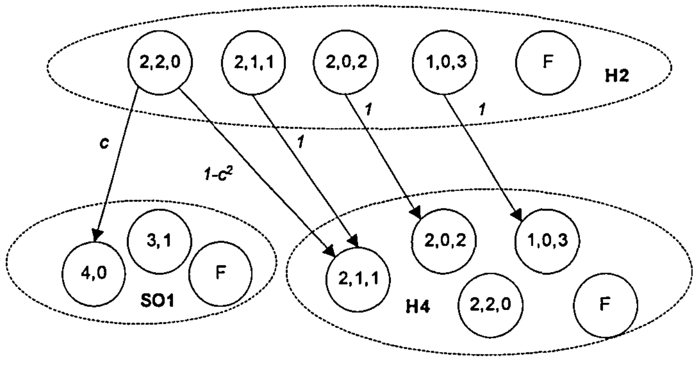


Figure 3.15 Probabilistic Phase Transition model from H2 to SO1 and H4

The transition matrix for a probabilistic transition model is obtained in the same way as for a deterministic model apart from the number of columns is equal to the sum of the state space of all possible subsequent phases.

Each lower level model is solved in the order of the phase sequences in the upper level model, where the initial state probability vector for each phase is obtained by application of the appropriate transition model to the state probabilities at the end of the previous phase. The upper level model can then be solved to evaluate parameters of interest. Further methods for solution to phased mission systems using deterministic and stochastic petri nets are discussed by Mura et al [37].

3.3.2.2 Non-Markovian Models

The traditional Markov approach involves each phase being treated separately to obtain a state probability vector at the time of the phase change. Each probability vector is then linearly transformed into the appropriate initial condition vector for the next phase. This continues until the vector of the last phase is found, representing the predicted reliability of the total mission. However, this method is limited due to the assumption that phase changes occur at specified discrete points in time and are instantaneous and state-dependent, i.e. the system will only begin a phase if the state is successful for both the preceding and succeeding phases. Such a model alone is not able to represent the amount of work performed or the relative values of task accomplishment in many practical situations.

A non-Markovian model represents the general case where the transition matrix [**A**] of equation (2.44) contains globally time-dependent coefficients ($\lambda(t)$ and $\upsilon(t)$). The homogenous case is the special case where these transition rates are constant (λ and υ).

The deficiencies of the homogeneous method are identified by Smotherman and Zemoudeh [38]:

- Phase changes and phase change times depend only on the current phase, and not individual states. This cannot represent, for example, that a degraded system would require longer to complete a phase than a fully functional system would.
- The number of phases with a random time duration is limited, or requires the computation of order statistic integrals.
- Failure and repair rates must be constant within each phase. This does not allow representation of burn-in effects or wear out effects of mechanical components.

A generalised method is presented where the performance of the system is modelled by a continuous time finite-state Markov process. The distributions of phase change times are considered to be non-overlapping uniform distributions that are ordered according to the sequence of phases, and the failure and repair rates are assumed to be globally time-dependent.

Transitions are generalised to represent phase changes as well as component failure and repairs so that arbitrary distributions of phase change times can be established in hazard rate form as time-varying transition rates in the non-Markovian model. The numerical solution to the non-Markovian matrix set of differential equations is then solved using the fifth order Runge-Kutta method. This is extended for time-dependent transition rates, and includes information on each type of phase change; exiting state, entry state(s), and the branching possibility for multiple entry states. Fixed-time phase changes do not affect the transition matrix but cause an instantaneous transfer of probability from the exiting state to the entry state(s).

This work is continued by Smotherman and Geist [39] who introduce measures of effectiveness for a single non-Markovian mission model using reward rates to provide more information on system effectiveness. This model can be applied in situations where component failure is not exponentially distributed, and failure rates are not constant.

If $\{X(t)|t \geq 0\}$ is a finite state stochastic process with state probabilities $P_{S_j}(t) = P[X(t) = j]$, the set of state differential equations can be expressed by equation (3.46).

$$\dot{P}_{S_j}(t) = \sum_{i=1}^{N_s} P_{S_i}(t) a_{ij}(t) \tag{3.46}$$

where N_s is the number of system states.

This is represented in matrix from in equation (2.44), however in this case the transition matrix is time dependent, [A(t)]. Each phase is represented as a separate subset of states of the single model. Phase changes are represented by time-varying transitions among these subsets, and are state dependent. Phase changes that are not instantaneous are modelled by including intermediate states. This allows representation of different phase change durations and also multi-objective missions.

A reward model applies instantaneous and cumulative measures of weighted state occupancy. Each state S_i has an associated weight called a reward rate, $R_{S_i}(t)$, which represents the relative value of the system residing in the state. Reward rates may also be time-dependent.

The vector of system state reward rates, **R**(*t*) is defined by equation (3.47).

$$\mathbf{R}(t) = [R_{S_1}(t), R_{S_2}(t), \ldots, R_{S_{N_s}}(t)]^T \tag{3.47}$$

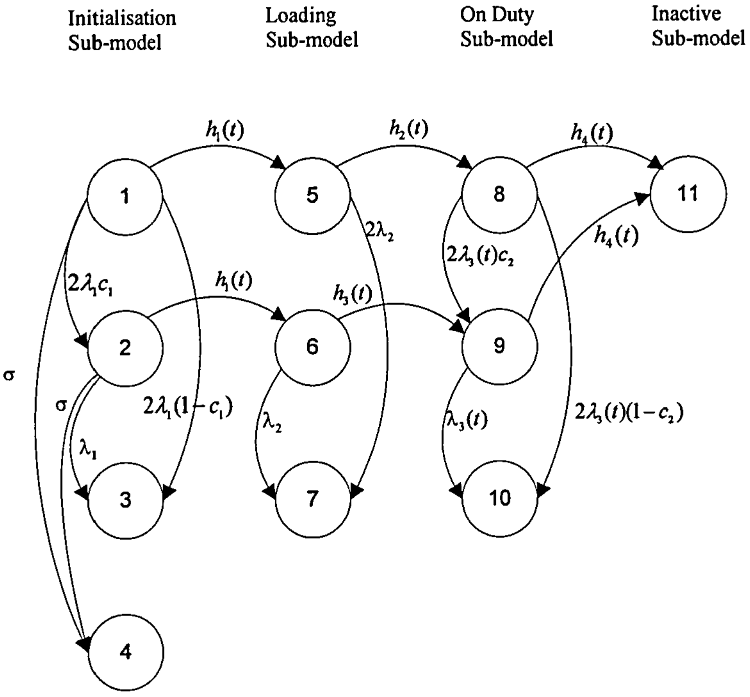
The instantaneous reward rate of the system at time *t* is then given by **P**(*t*) **R**(*t*). The expected value of the accumulated reward until time *t*, Y(*t*), is obtained in equation (3.48).

$$E[Y(t)] = \int_0^t \mathbf{P}(u)\mathbf{R}(u)du = \sum_{i=1}^{N_S} P_{S_i}(u)R_{S_i}(u)du \tag{3.48}$$

If used with proper reward rates this may give information on the expected time spent in a certain subset of states, and may be used as a measure for providing life cycle measures such as expected duty time and expected time under repair.

A standard initial-value solution algorithm may be used to find the state probabilities of the system of differential equations with appropriate reward rates. The transition rate matrix must be re-evaluated at each time step of the algorithm since the matrix entries are time-varying rates. If a transition rate approaches a discontinuity, increasingly smaller step sizes are required and the solution process becomes computationally longer. Models of complex systems have potentially large state spaces due to the representation of all states in all phases. The possible extra computational effort is the main disadvantage when considering the increase in flexibility of the model.

This method can be applied to an example system comprising of two components that is initialised and loaded and then remains on duty until the end of a 100 hour period, summarised in Figure 3.16.



Where:

State	
1	3 components available
2	2 components available
3	1 component available
4	0 components available (unrecoverable system failure)
5	3 components available
6	2 components available
7	1 component available
8	3 components available
9	2 components available
10	1 component available
11	Unrecoverable System Failure

σ	Initialisation system failure rate
$h_i(t)$	Phase change rate
$\lambda_i(t)$	Time-dependent component failure rate in phase *i*
c_1	Coverage probability during initialization
c_2	Coverage probability on duty

Figure 3.16 Non-Markovian Model Example

This example demonstrates the possibility of state dependent phase change times. In the loading phase if two components are operational (state 5) then loading is completed at rate $h_2(t)$, however if only one component is operational (state 6), the loading requires a longer interval and the phase change rate $h_3(t)$ is used. This also demonstrates the possibility of time-dependent failure rates, for example $\lambda_3(t)$ in phase 3. Reward rates can be assigned by the number of components that are operational in the state per unit time. This example is quantified by Smotherman and Geist and further examples are considered to represent multi-objective and pipe leakage models. This work is also developed using semi-Markov models with fixed (maximum) durations in a given set of system states by Becker et al [40].

3.3.3 Summary

The methods that have been presented for solution to repairable phased mission systems exhibit the following properties:

- Combinatorial approaches do not account for possible dependencies between components and phases, and thus produce only an approximation for phase and mission unreliability.

- Markov methods implementing a single model eliminate the problem of state mapping across a phase boundary. Markov methods based on separate phase models result in state mapping problems at each phase transition.

- Homogeneous Markov models require constant state transition rates within each phase. Non-Markovian models allow for varying state transition rates within a phase.

- Phase durations can be deterministic or random. Phase sequences can be deterministic or state-dependent.

A method is required to suitably represent the dynamic and dependent behaviour of a multi-phased mission. Since combinatorial approaches allow only approximations of phase and mission unreliability, Markov methods are preferred. However, Markov models are susceptible to state explosion problems as the number of components increases and so a technique is required to eliminate this. A state mapping procedure is required across phase transition boundaries if using separate phase Markov models.

The presented methods have considered all phases in a mission to be of a single type, either non-repairable or repairable. There are many phased mission features that have not been identified. It is possible that a phase can be either discrete or continuous in duration. Also, little research has been undertaken into the possibility of sequential failure relationships with scheduled inspection policies. Therefore a general method is required to include the possibility of a combination of discrete and continuous phase durations, with non-repairable and repairable phase types and the consideration of sequential failures and scheduled inspection.

Chapter 4 Non-Repairable Phased Missions

4.1 Introduction

The method of calculating the reliability of a phased mission cannot simply be obtained by the multiplication of the reliabilities of each of the individual phases as this involves the false assumptions that the phases are independent and all components are in the working state at the beginning of each phase. To make these assumptions results in an appreciable over-prediction of system reliability. Other techniques must be applied.

For the case of a multi-phased system containing only non-repairable components, various methods have been developed to assess the mission reliability. Past research has demonstrated that the Markov approach is susceptible to potential explosions in the number of state equations for even moderate sized problems. For the more simple case of a system allowing no repairs, the preferred approaches are that of the fault tree and binary decision diagram techniques.

Previous methods have provided means of estimating the failure probability of a mission as a whole, but little investigation has been made into the additional possibility of the attainment of individual phase failure. A new fault tree method is proposed to enable the probability of failure in each phase to be determined in addition to the whole mission unreliability. For any phase, the method combines the causes of success of previous phases with the causes of failure for the phase being considered to allow both qualitative and quantitative analysis of both phase failure and mission failure. This will overcome some of the deficiencies of other fault tree techniques. The proposed method is also presented in [41].

The binary decision diagram method offers an alternative approach to the fault tree method in the aim of reducing the complexity of the problem, thus making the solution process more accurate and efficient. The standard binary decision diagram technique is consequently modified to produce a more general method for use in missions of multiple phases.

Once the probability of phase and mission failure has been determined by either the fault tree or binary decision diagram method, it is possible to calculate the frequency of phase and mission failure.

4.2 Fault Tree Method

The proposed method considers the performance of a system not only for the duration of the phase in question, but also for all preceding phases. A component that is known to be in the failed state in a phase could have failed at any point up to that time. By considering the component failing in each phase as a separate event, component failure in a particular phase fault tree is replaced by an OR combination of the events for the component failing in that and all preceding phases. The event of component failure in phase *i* is represented as the event that the component could have failed during any phase up to and including phase *i*. For example, component A failure in phase 2 would be represented by the OR of the failure of the component in phase 1 (A_1) and in phase 2 (A_2) since the component is non-repairable, shown in Figure. 4.1.

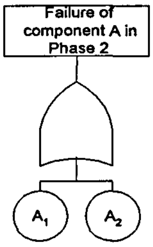


Figure 4.1 Replacement OR combination

System failure in phase *i* is represented by the AND of the success of phases 1..*i*-1 and the failure during phase *i*, demonstrated in Figure. 4.2. All phase failures may then be combined using an OR gate to represent causes of overall mission failure as the event that any phase does not complete successfully.

This method allows for the evaluation of individual phase failures, and also accounts for the condition where components are known to have functioned to enable the system to function in previous phases. However, owing to the fact that cut sets are not removed until a later stage in the analysis, the fault tree can be much more complex and require significantly more effort to solve.

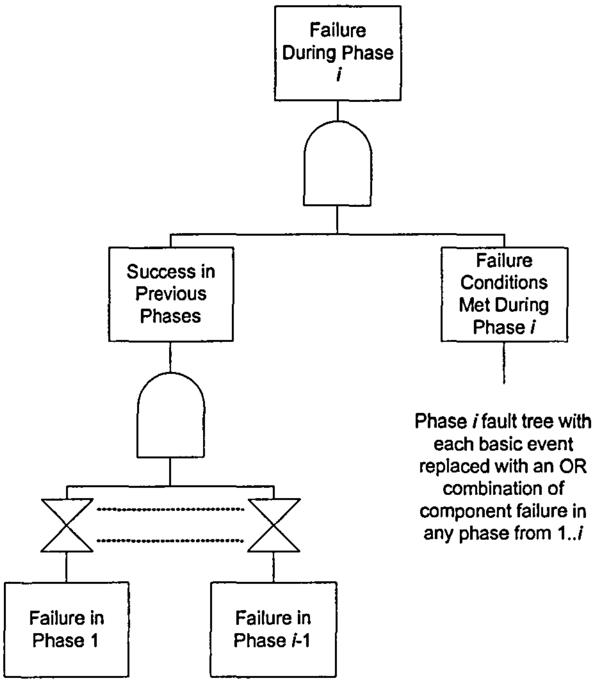

Failure During Phase *i*
Success in Previous Phases
Failure Conditions Met During Phase *i*
Phase *i* fault tree with each basic event replaced with an OR combination of component failure in any phase from 1..*i*
Failure in Phase 1
Failure in Phase *i*-1

Figure 4.2 Generalised Phase Failure Fault Tree

4.2.1 Qualitative Analysis

The failure of a system can occur in many different ways. Each unique way is referred to as a *system failure mode*, and involves the failure of either a single component, or the combination of failures of multiple components.

To determine the minimal cut sets of a phase or mission, either a top-down or a bottom-up approach is applied to the relevant fault tree. For any phases after the first phase, the incorporation of the success of previous phases means that the fault tree will be non-coherent and not simply consist of 'AND' and 'OR' gates. NOT logic will be required to represent this success (not failed), and the combinations of basic events that lead to the occurrence of the top event will be referred to as *implicants*. These implicant sets are not always minimal and so simplification techniques are required for reduction to prime implicant sets in phased mission systems.

This proposed method may be applied for the simple three-phase mission given in Figure 4.3.

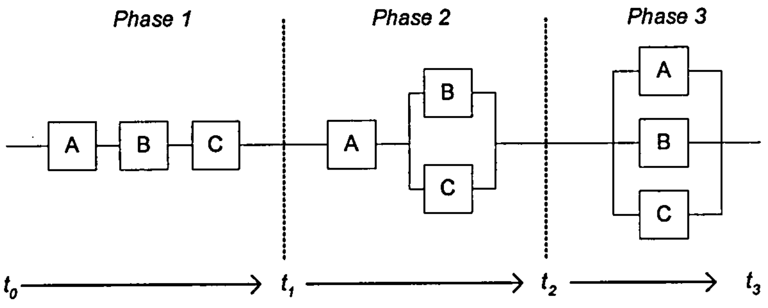


Figure 4.3 Reliability Network of a Simple Phased Mission System

The failure causes for each phase may be expressed using separate fault trees in Figure 4.4.

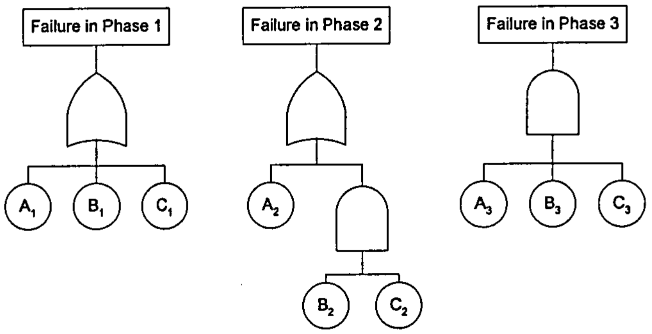


Figure 4.4 Fault Tree Representation of Individual Phase Failures

The fault tree to represent the initial phase failure of the mission remains identical to the fault tree representation of the individual phase failure of phase 1 shown in Figure 4.4. Failure during phase 2 can then be shown as the combination of phase 1 success and failure in phase 2, using the basic event expansion, in Figure 4.5.

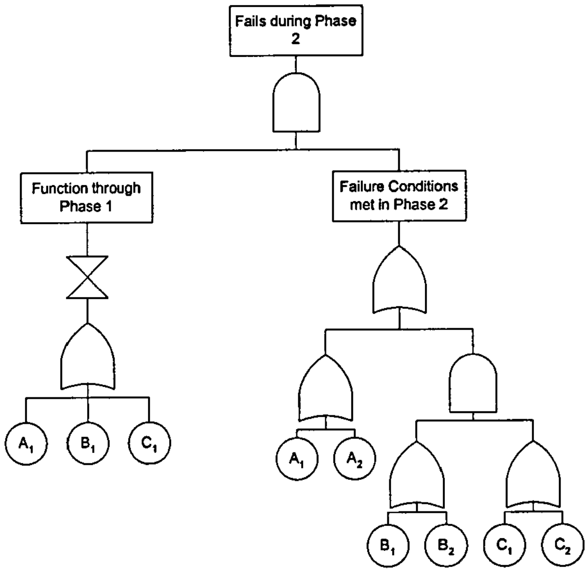


Figure 4.5 Phase 2 Failure Fault Tree

Similarly, phase 3 failure can be represented as the combination of phase 1 and 2 successes, and failure in phase 3 in Figure 4.6.

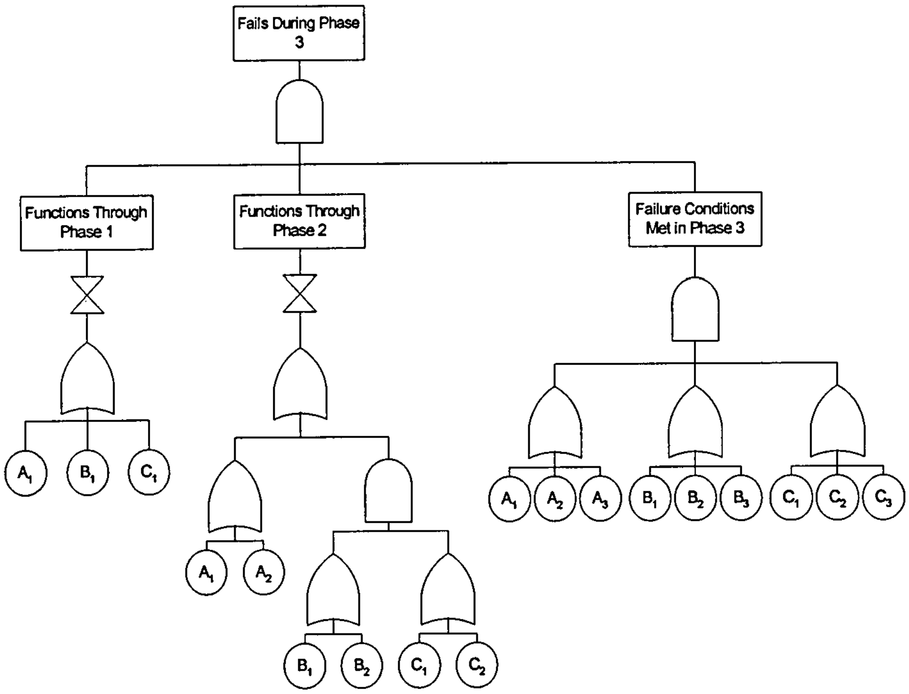


Figure 4.6 Phase 3 Failure Fault Tree

4.2.1.1 Fault Tree Modularisation

Fault tree modularisation techniques are helpful to reduce the size of a fault tree to enable prime implicants to be found more efficiently. These modularisation techniques reduce both memory and time requirements. A non-coherent extension of a modularisation technique has been employed in this work [42]. It repeatedly applies the stages of contraction, factorisation and extraction to reduce the complexity of the fault tree diagram. The stages are identified as:

1. Contraction

Subsequent gates of the same type are contracted to form a single gate. The resulting tree structure is then an alternating sequence of OR and AND gates.

2. Factorisation

Identification of basic events that always occur together in the same gate type. The combination of events and gate type is replaced by a complex event. However, since

NOT logic is included in order to combine phase success and failure, in this stage the primary basic events that are found to always occur together in one gate type must have complements that always occur together in the opposite gate type by De Morgans' laws, e.g.

$$2000 = A + B \qquad 2001 = A \cdot B$$
$$\overline{2000} = \overline{A} \cdot \overline{B} \qquad \overline{2001} = \overline{A} + \overline{B}$$

3. Extraction

Searches for structures within the tree, of the form shown in Figure 4.7, that may be simplified by extracting an event to a higher level.

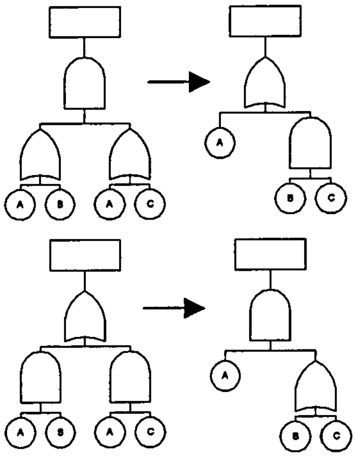


Figure 4.7 Extraction Stage of the Modularisation Technique

4.2.2 Prime Implicants in Phased Mission Systems

Owing to the non-coherent nature of the fault trees, the combinations of basic events that lead to the occurrence of the top event of either phase or mission failure are expressed as prime implicants. The notation used to represent the failure of component A in phase i is A_i. $\overline{A_i}$ represents the functioning of component A throughout phase i. The notation used to indicate the failure of a component in phase i through to and including phase j is A_{ij}, i.e. component A fails at some time from the start of phase i to the end of phase j. Conversely, the success of component A in phase i through to and including phase j is $\overline{A_{ij}}$.

This notation enables us to define a new algebra over the phases to manipulate the logic equations. What is of concern in later phases is the phase during which the component failures occur. So we can produce a combination of events for component A e.g. it works successfully through phases 1 and 2 and fails in either phase 3 or phase 4. This is expressed algebraically as:

$$\overline{A_1}\,\overline{A_2}(A_3 + A_4)$$

This means that the top event will only occur if A fails in phases 3 or 4 i.e. A_{34} where,

$$q_{A_{34}} = q_A(t_2, t_4) = \int_{t_2}^{t_4} f_A(t)dt$$

where $q_{A_{34}}$ is the failure probability for component A in phases 3 or 4

$f_A(t)$ is the density function of failure times for component A

The top event of phase or mission failure can contain multiple events belonging to the same component. Since each phase is obtained as a combination of current phase failure with previous phase successes, the events can represent either component failure or success in various phases. A new set of Boolean laws is required to reduce the expression for each phase failure into minimal form. The application of these laws will allow the prime implicant sets to be obtained for each phase.

A summary of the new algebraic laws where phase *i*<*j* is:

1. $A_i \cdot A_i = A_i$ Component A fails in phase *i* AND phase *i*. Repeated Event.

2. $A_i \cdot A_j = 0$ Component A fails in phase *i* AND phase *j*. These are mutually exclusive events so cannot both occur.

3. $A_i \cdot A_{ij} = A_i$ Component A fails in phase *i* AND between phase *i* and phase *j*. As the failure of component A in phase *i* and any other phase from *i+1* to *j* are mutually exclusive events, they cannot occur together. The common event is the failure of component A in phase *i*.

4. $\overline{A_i} \cdot A_i = 0$ Component A works in phase *i* AND fails in phase *i*. An event and its compliment cannot occur at the same time.

5. $\overline{A_i} \cdot A_j = A_j$ Component A works through phase *i* AND fails in phase *j*. The failure of component in phase *j* implies that it must have worked up to the start of phase *j*, and so the success event in phase *i* can be eliminated.

6. $\overline{A_i} \cdot A_{ij} = A_{i+1,j}$ Component A works in phase *i* AND fails between phase *i* and phase *j*. The success and failure of component A in phase *i* cannot be combined. The combination is the event of component A failure in phase *i*+1 up to and including phase *j*.

7. $\overline{A_i} \cdot \overline{A_{i+1}} \ldots \overline{A_j} = \overline{A_{ij}}$ Component A works through phase *i* up to phase *j* inclusive. Combine to standard notation.

8. $A_i + A_{i+1} .. + A_j = A_{ij}$ Component A fails in any phase through phase *i* up to phase *j* inclusive. Combine to standard notation.

If two prime implicant sets contain exactly the same components where all but one of which occur over the same time intervals and the other is a failure in contiguous phases, the two prime implicant sets may be combined with the period of failure for the component having time index adjusted, eg:

$$\begin{array}{c} A_1B_1 \\ A_1B_2 \end{array} \xrightarrow{\qquad\qquad} A_1B_{12}$$

As the components are non-repairable, the event of component failure will only be possible during one of the contiguous phases.

This simplification approach allows the prime implicants for the example with phase fault trees given in Figures 4.4, 4.5, and 4.6 to be obtained as follows:

Phase 1

$$T_1 = A_1 + B_1 + C_1$$

Minimal Cut Sets: A_1, B_1, C_1

Phase 2

The top event of failure during phase 2 is obtained by the combination of phase 1 success with phase 2 failure:

$$T_2 = \overline{A_1}\,\overline{B_1}\,\overline{C_1}(A_1 + A_2 + B_1C_1 + B_1C_2 + B_2C_1 + B_2C_2)$$

The full expansion of this becomes:

$$T_2 = \overline{A_1}\,\overline{B_1}\,\overline{C_1}A_1 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}A_2 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}B_1C_1 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}B_1C_2 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}B_2C_1 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}B_2C_2$$

Using law 4, an event and its compliment cannot occur at the same time. The top event becomes:

$$T_2 = \overline{A_1}\,\overline{B_1}\,\overline{C_1}A_2 + \overline{A_1}\,\overline{B_1}\,\overline{C_1}B_2C_2$$

By law 5, the failure of a component in phase 2 implies that it must have worked through phase 1, and so the success of the component in phase 1 can be eliminated. The minimised top event of phase 2 failure becomes:

$$T_2 = A_2\overline{B_1}\,\overline{C_1} + \overline{A_1}B_2C_2$$

The prime implicant sets for the failure of phase 2 are: $A_2\overline{B_1}\,\overline{C_1}$, $\overline{A_1}B_2C_2$

Phase 3

The top event of failure during phase 3 is obtained by the combination of phase 1 and 2 successes with phase 3 failure:

$$T_2 = \left(\overline{A_1}\,\overline{B_1}\,\overline{C_1}\right)\cdot\left((\overline{A_1}\,\overline{A_2}(\overline{B_1} + \overline{C_1})\cdot(\overline{B_1} + \overline{C_2})\cdot(\overline{B_2} + \overline{C_1})\cdot(\overline{B_2} + \overline{C_2})\right)\cdot$$
$$\left((A_1 + A_2 + A_3)\cdot(B_1 + B_2 + B_3)\cdot(C_1 + C_2 + C_3)\right)$$

In the same way as for phase 2, using the laws of phase algebra this expression can be expanded and reduced to:

$$T_2 = A_3B_3C_{23} + A_3B_{23}C_3$$

The prime implicant sets for the failure of phase 3 are:

$$\begin{array}{lcl} A_3B_3C_{23} & \longrightarrow & \begin{array}{l} A_3B_3C_2 \\ A_3B_3C_3 \end{array} \\ A_3B_{23}C_3 & \longrightarrow & \begin{array}{l} A_3B_2C_3 \\ A_3B_3C_3 \end{array} \end{array} \longrightarrow \begin{array}{l} A_3B_3C_2 \\ A_3B_3C_3 \\ A_3B_2C_3 \end{array}$$

If it is assumed that the success events of a phase have a very high likelihood of occurrence, the prime implicant sets can be expressed as minimal cut sets. Events that appear in their negated form in the prime implicant sets are deleted thus reducing the list to a coherent approximation.

4.2.3 Quantitative Analysis

Having established the prime implicants for each phase failure, they may now be used to quantify the probability of phase and mission failure.

The probability density function of a component A with constant failure rate in a non-repairable single phase mission is found by the negative exponential distribution given in equation (4.1).

$$f(t) = \lambda_A e^{-\lambda_A t} \qquad \text{for } t > 0 \qquad (4.1)$$

It is assumed that the component is subject to a constant failure rate through all phases, regardless of whether it is required for a particular phase success. The unavailability of the component, $q_A(t)$, over a duration of time $[0,t)$ is modelled by the cumulative probability function $F_A(t)$ in equation (4.2).

$$q_A(t) = F_A(t) = \int_0^t f_A(t)\,dt = \left[-e^{-\lambda_A t}\right]_0^t = 1 - e^{-\lambda_A t} \qquad (4.2)$$

The unavailability of the component over a phase i is derived in a similar way to equation (4.2) by integration of the probability density function (equation (4.1)). The integration time limits for phase *i* will be $t=t_{i-1}$ to $t=t_i$, and the component A unavailability in phase *i* is derived in equation (4.3).

$$q_{A_i} = \int_{t_{i-1}}^{t_i} f_A(t)\,dt = \left[-e^{-\lambda_A t}\right]_{t_{i-1}}^{t_i} = e^{-\lambda_A t_{i-1}} - e^{-\lambda_A t_i} \qquad (4.3)$$

The probability of failure of a non-repairable component A during phases *i* to *j* in time period $[t_{i-1}, t_j)$ is given by $q_{A_{ij}}$ in equation (4.4).

$$q_{A_{ij}} = e^{-\lambda_A t_{i-1}} - e^{-\lambda_A t_j} \qquad (4.4)$$

The unreliability, Q_i, for each individual phase *i* is found using the inclusion-exclusion expansion for the existence of phase *i* prime implicant sets, K_{l_i}, in equation (4.5).

$$Q_i = \sum_{l=1}^{N_{pi_i}} P(K_{l_i}) - \sum_{l=2}^{N_{pi_i}} \sum_{n=1}^{l-1} P(K_{l_i} \cap K_{n_i}) + \cdots + (-1)^{N_{pi_i}-1} P(K_{1_i} \cap K_{2_i} \cap \cdots \cap K_{N_{pi_i}}) \qquad (4.5)$$

where N_{pi_i} is the number of prime implicant sets in phase *i*

The event of phase failure for the simple three-phase mission with prime implicant sets given in Section 4.2.2 can be obtained using the inclusion-exclusion expansion (equation (4.5)), and is expressed in equations (4.6).

Phase 1: $Q_1 = q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}$

Phase 2: $Q_2 = q_{A_2}(1-q_{B_1})(1-q_{C_1}) + (1-q_{A_1})q_{B_2}q_{C_2} - q_{A_2}q_{B_2}q_{C_2}$ (4.6)

Phase 3: $Q_3 = q_{A_3}q_{B_3}q_{C_2} + q_{A_3}q_{B_3}q_{C_3} + q_{A_3}q_{B_2}q_{C_3}$

As the failure of each of the phases produces mutually exclusive causes, the probability of mission failure, Q_{MISS}, may be expressed as a sum of the unreliabilities of the individual phases in equation (4.7).

$$Q_{MISS} = \sum_{i=1}^{m} Q_i \qquad (4.7)$$

where m is the total number of phases

4.2.4 Summary

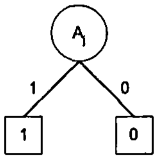
This method allows for the evaluation of individual phase failures, and also accounts for the condition where components are known to have functioned to enable the system to function in previous phases. However, due to the fact that cut sets are not removed until a later stage in the analysis compared with methods based on the technique by Esary and Ziehms [12], the fault tree can be much more complex and require significantly more effort to solve, especially in later phases.

4.3 Binary Decision Diagram Method

A fault tree structure very efficiently represents system failure logic, but is not an ideal form for mathematical analysis. Binary decision diagrams represent a logic expression and offer efficient mathematical manipulation, although it is very difficult to construct directly from the system definition. For larger fault trees it is more efficient to convert to a BDD prior to analysis. The approach of performing the quantification process after first converting the fault tree to a BDD form offers significant advantages for large complex fault trees. This is particularly true of structures that are non-coherent, such as the phase failure fault trees.

4.3.1 Construction of a Phased Mission BDD

The phased mission BDD is constructed using a similar method to the single system BDD (Section 2.3). The basic event of the failure of component A in phase *j*, A_j, can be represented in Figure 4.8.



1 - Occurrence of A_j

0 - Non-Occurrence of A_j

Figure 4.8 Binary Decision Diagram Vertex for Component A Failure in Phase *j*

The failure of component A in phase *j* can be represented using *if-then-else* form in equation (4.8).

$$A_j = \textbf{ite}(A_j, 1, 0) \qquad (4.8)$$

One of the features of the BDD structure is the ease with which the dual can be formulated. If the primary (system failure) BDD represents the structure function $\phi(\mathbf{x})$, the dual function of system success, $\bar{\phi}(\mathbf{x})$, is constructed from $\bar{\phi}(\mathbf{x}) = 1 - \phi(\mathbf{x})$. The dual BDD of a phase j represents the top event of phase success, $\overline{T_j}$, and is created by switching the terminal nodes, i.e. a terminal *1* node is replaced by a terminal *0*, and a terminal *0* node by a terminal *1*. It must be noted that in the formulation of the dual of the BDD, the non-terminal nodes still represent the failure event of components. The dual of Figure 4.8 to demonstrate the success of component A in phase *j* can therefore be represented by Figure 4.9.

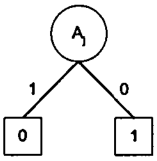


Figure 4.9 Binary Decision Diagram Vertex for Component A Success in Phase *j*

The success of component *A* in phase *j* can be represented using *if-then-else* form in equation (4.9).

$$\overline{A_j} = \textbf{ite}(A_j, 0, 1) \tag{4.9}$$

An ordering of the basic events in the fault tree must be chosen. At this stage, the components are ordered first ($A<B<C$), and then each component is expanded into its series of sub-components in a forwards phase ordering sequence ($A_1<A_2<A_3<B_1<B_2<B_3<C_1<C_2<C_3$). Ordering techniques are discussed further in Section 4.3.5.

To combine basic events within a phased mission BDD, the following rules are applied:

- To combine two different basic events (X_i and Y_j) using a logical operation $\oplus$,

$$\begin{array}{ll} \textit{If} & J = \textbf{ite}(X_i, f1, f2) \\ \textit{and} & H = \textbf{ite}(Y_j, g1, g2) \end{array}$$

$$\begin{array}{ll} \text{If } X_i < Y_j & J \oplus H = \textbf{ite}(X_i, f1 \oplus H, f2 \oplus H) \\ \text{If } X_i = Y_j & J \oplus H = \textbf{ite}(X_i, f1 \oplus g1, f2 \oplus g2) \end{array}$$

These rules are general for all variable combinations. Since the Boolean laws for phase algebra (Section 4.2.2) are applied to the implicant sets once the BDD is constructed, no special laws are applied for combinations of events belonging to the same component.

The simple 3-phase mission given in Figures 4.4, 4.5, and 4.6 may be represented in BDD form for each phase and quantified. However, the proposed method combines the failure in a phase with the success of all preceding phases. This is achieved using the logical operation methods, where the AND of previous phase successes and current phase failure is required, and is presented in Section 4.3.4.

4.3.2 Qualitative Analysis

The paths through a binary decision diagram terminate in either a '1' or a '0' vertex. A terminal '1' vertex signifies system failure, and thus those paths leading to such a vertex indicate the system failure modes. These disjoint paths leading to system failure represent implicant sets. The simplification technique is applied as in the fault tree approach given in section 4.2.2 using the Boolean laws to reduce the implicant sets to prime implicant sets.

4.3.3 Quantitative Analysis

The top event probability of a BDD is derived from Shannon's formula (pivotal decomposition). The state of a component x_i in phase j is denoted by:

$$x_{i_j} = \begin{cases} 0 & \text{If component } x_i \text{ is working in phase } j \\ 1 & \text{If component } x_i \text{ fails in phase } j \end{cases} \qquad \text{for } j = 1,2,....,m$$

The phase j binary function, ϕ_j, is then,

$$\phi_j = \begin{cases} 0 & \text{If phase } j \text{ works} \\ 1 & \text{If phase } j \text{ fails} \end{cases} \qquad \text{for } j = 1,2,....,m$$

and $\phi_j = \phi_j(\mathbf{x})$, where $\mathbf{x}$ is the vector of all component states through phases $1..j$

$\phi_j(\mathbf{x})$ is the system structure function in phase j and can be found using equation (4.10).

$$\phi_j(\mathbf{x}) = x_{i_j}\phi(1_{i_j}, x) + (1 - x_{i_j})\phi(0_{i_j}, x) \qquad \text{for } j = 1,2,\ldots.,m \tag{4.10}$$

The probability of the top event (i.e. phase failure probability) can be found by taking the expectation of each term of equation (4.10) as shown in equation (4.11).

$$E[\phi_j(\mathbf{x})] = q_{i_j} \cdot E[\phi(1_{i_j}, x)] + (1 - q_{i_j}) \cdot E[\phi(0_{i_j}, x)] \qquad \text{for } j = 1,2,\ldots.,m \tag{4.11}$$

where $q_{i_j} = E[x_{i_j}]$ is the probability that x_i fails in phase j

The phase j failure probability can be calculated by summing the probabilities of the disjoint (mutually exclusive) paths through the unminimised BDD from the root vertex to each terminal 1 vertex (equation (4.12)). Each disjoint path represents a combination of working and failed components in any phase up to and including phase j that lead to phase j failure, and so events lying on both one and zero branches are included in the probability calculation.

$$Q_j = \sum_{i=1}^{n_{dj}} p(r_i) \tag{4.12}$$

where $p(r_i)$ is the probability of the ith disjoint path to a terminal 1 node

n_{dj} is the number of disjoint paths to a terminal 1 node

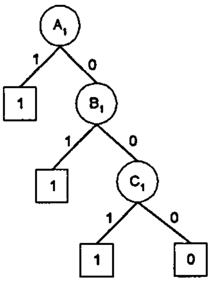
4.3.4 Example

Application of this method may be demonstrated using the fault tree technique in Section 4.2 on the three-phased mission given in Figures 4.4, 4.5 and 4.6. Each success or failure basic event is assigned an **ite** structure according to equations (4.8) or (4.9), and the phases may be constructed using the logical combination rules as follows:

Phase 1

Phase 1 failure $\quad \mathrm{F1} = ite(A_1,1,0) + ite(B_1,1,0) + ite(C_1,1,0)$

$$= ite(A_1,1,ite(B_1,1,ite(C_1,1,0))) \qquad (4.13)$$



Minimal Cut Sets: A_1
 B_1
 C_1

Figure 4.10 Failure in Phase 1 BDD

The disjoint paths to the terminal 1 node are: A_1, $\overline{A_1}\,B_1$, $\overline{A_1}\,\overline{B_1}\,C_1$

Phase 1 failure probability: $Q_1 = q_{A_1} + (1-q_{A_1})q_{B_1} + (1-q_{A_1})(1-q_{B_1})q_{C_1}$

$$= 1-(1-q_{A_1})(1-q_{B_1})(1-q_{C_1}) \qquad (4.14)$$

Phase 2

The failure in phase 2 is found by the AND combination of phase 1 success and phase 2 failure. The success of phase 1 is obtained by the dual of the BDD in equation (4.13), where the terminal nodes are changed from '1' to '0' and '0' to '1' in equation (4.15).

Success through phase 1: $\quad \mathrm{S1} = ite(A_1,0,ite(B_1,0,ite(C_1,0,1))) \qquad (4.15)$

The **ite** expression for phase 2 failure is obtained by the phase 2 fault tree with top event defined as 'failure conditions met in phase 2' in Figure 4.5, and is given in equation (4.16).

Phase 2 failure:

$$\mathrm{F2} = ite(A_1,1,ite(A_2,1,ite(B_1,ite(C_1,1,ite(C_2,1,0)),ite(B_2,ite(C_1,1,ite(C_2,1,0)),0)))) \qquad (4.16)$$

The BDD for this phase 2 failure is given in Figure 4.11.

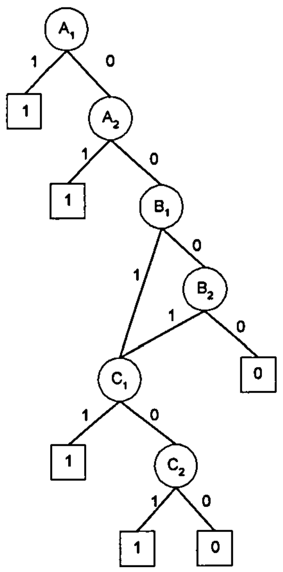


Figure 4.11 Phase 2 Failure BDD (not including phase 1 success)

The BDD for phase 2 failure in Figure 4.11 does not take into account the requirements for system success through phase 1. Using the proposed method to combine the BDDs of success through phase 1 (equation (4.15)) and phase 2 failure (equation (4.16)), the failure in phase 2 (SF2) BDD is as given in equation (4.17).

$$
\begin{aligned}
\mathrm{SF2} &= \mathrm{S1}\cdot\mathrm{F2} \\
&= ite(A_1,0,ite(B_1,0,ite(C_1,0,1)))\cdot \\
&\quad ite(A_1,1,ite(A_2,1,ite(B_1,ite(C_1,1,ite(C_2,1,0)),ite(B_2,ite(C_1,1,ite(C_2,1,0)),0))) \\
&= ite(A_1,0,ite(A_2,ite(B_1,0,ite(C_1,0,1)),ite(B_1,0,ite(B_2,ite(C_1,0,ite(C_2,1,0)),0))))
\end{aligned}
\tag{4.17}
$$

The BDD for failure in phase 2 is given in Figure 4.12.

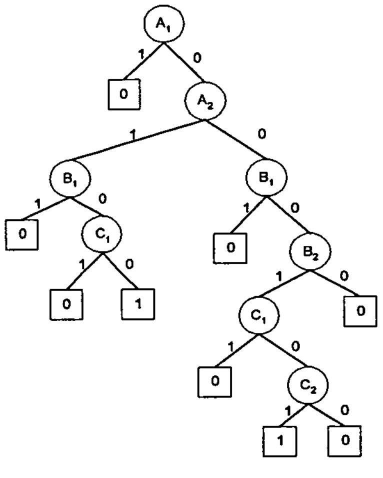


Figure 4.12 Failure in Phase 2 BDD

The implicant sets are found by the disjoint paths to a terminal 1 node and are simplified using the Boolean laws for phased mission systems in Section 4.2.2:

$$\begin{array}{lcl} \overline{A_1}A_2\overline{B_1C_1} & \longrightarrow & A_2\overline{B_1C_1} \\ \overline{A_1A_2B_1}B_2\overline{C_1}C_2 & & \overline{A_{12}}B_2C_2 \end{array}$$

The failure probability in phase 2 is then given in equation (4.18).

$$Q_2 = q_{A_2}(1-q_{B_1})(1-q_{C_1}) + (1-q_{A_1}-q_{A_2})q_{B_2}q_{C_2} \qquad (4.18)$$

Phase 3

The failure in phase 3 is found by the AND combination of phase 1 and 2 successes and phase 3 failure. The success of phase 1 is given in equation (4.15), and the success of phase 2 is obtained by the dual of the phase 2 failure BDD in equation (4.16), where the terminal nodes are changed from '1' to '0' and '0' to '1' in equation (4.19).

Phase 2 success:

$$S2 = ite(A_1,0,ite(A_2,0,ite(B_1,ite(C_1,0,ite(C_2,0,1)),ite(B_2,ite(C_1,0,ite(C_2,0,1)),1)))) \qquad (4.19)$$

The **ite** expression for phase 3 failure is obtained by the phase 3 fault tree with top event defined as 'failure conditions met in phase 3' in Figure 4.6:

Phase 3 failure:

$$F3 = ite(A_1,K_1ite(A_2,K_1,ite(A_3,K_1,0))) \qquad (4.20)$$

$$K_1 = ite(B_1,K_2,ite(B_2,K_2,ite(B_3,K_2,0)))$$

$$K_2 = ite(C_1,1,ite(C_2,1,ite(C_3,1,0)))$$

The BDD for this phase 3 failure is given in Figure 4.13.

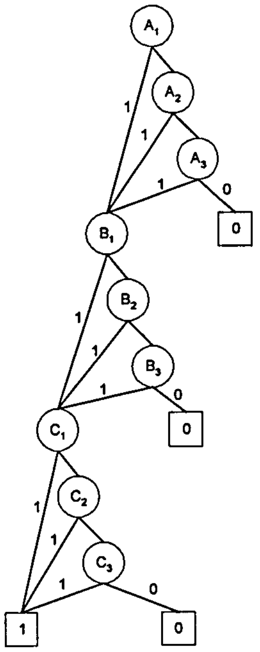


Figure 4.13 Phase 3 Failure BDD (not including phases 1 and 2 successes)

The BDD for phase 3 failure in Figure 4.13 does not take into account the requirements for system success through phases 1 and 2. Using the proposed method to combine the BDD of phase 1 success (equation (4.15)), phase 2 success (equation (4.19)) and phase 3 failure (equation (4.20)), the failure in phase 3 (SF3) becomes as given in equation (4.21).

$$\begin{aligned}\text{SF3} &= \text{S1}\cdot\text{S2}\cdot\text{F3}\\ &= ite(A_1,0,ite(B_1,0,ite(C_1,0,1)))\cdot\\ &\quad ite(A_1,0,ite(A_2,0,ite(B_1,ite(C_1,0,ite(C_2,0,1)),ite(B_2,ite(C_1,0,ite(C_2,0,1)),1)))\cdot\\ &\quad ite(A_1,K_1,ite(A_2,K_1,ite(A_3,K_1,0)))\end{aligned}$$

where:
$$K_1 = ite(B_1,K_2,ite(B_2,K_2,ite(B_3,K_2,0)))$$
$$K_2 = ite(C_1,1,ite(C_2,1,ite(C_3,1,0)))$$

$$\text{SF3} = ite(A_1,0,ite(A_2,0,ite(A_3,ite(B_1,0,ite(B_2,L_1,L_2)),0))) \qquad (4.21)$$

where:
$$L_1 = ite(C_1,0,ite(C_2,0,ite(C_3,1,0)))$$
$$L_2 = ite(B_3,ite(C_1,0,ite(C_2,1,ite(C_3,1,0)),0))$$

The new BDD for failure in phase 3 becomes as shown in Figure 4.14.

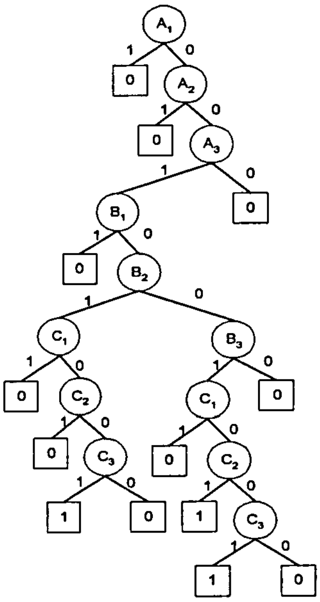


Figure 4.14 Failure in Phase 3 BDD

The implicant sets are found by the disjoint paths leading to a terminal 1 node, and reduced to minimal form using the Boolean laws in Section 4.2.2.

$$\begin{array}{lcl} \overline{A_1 A_2} A_3 \overline{B_1 B_2} B_3 \overline{C_1 C_2} C_3 & & A_3 B_3 C_3 \\ \overline{A_1 A_2} A_3 \overline{B_1 B_2} B_3 \overline{C_1} C_2 & \longrightarrow & A_3 B_3 C_2 \\ \overline{A_1 A_2} A_3 \overline{B_1} B_2 \overline{C_1 C_2} C_3 & & A_3 B_2 C_3 \end{array}$$

The quantification for phase 3 is then given in equation (4.22).

$$Q_3 = q_{A_3} q_{B_3} q_{C_3} + q_{A_3} q_{B_3} q_{C_2} + q_{A_3} q_{B_2} q_{C_3} \tag{4.22}$$

It can be seen that the unreliability of each of the phases found by the BDD method in equations (4.14), (4.18), and (4.22) are identical to that obtained using fault tree analysis in equations (4.6).

4.3.5 Ordering

A binary decision diagram structure is dependent on the ordering in which the events are considered during construction. A simple single phased mission consists of only the events of component failure or success, and each variable in the scheme relates to a different component. However, a multi-phased mission involves component failure or success with a time factor involved to identify the phase. This leads to an interesting comparison of different ordering schemes in the aim of reducing the size and thus the number of nodes in the BDD to make a quicker and more efficient computational process.

Application of the Boolean laws for phased mission analysis presented in Section 4.2.2 allow any ordering of variables to be implemented when constructing each phase BDD. The events are initially assigned an optimal ordering sequence in each phase j, and then can be expanded into sub-events to represent the failure of the component through phases 1..j. The most general sequences are discussed below, with example of an event order $A < B < C$ in phase j:

Component Forwards Ordering (CFO)

Each event is expanded into its series of sub-events in the order of first phase to current phase, *1..j*.

$$A_1 < A_2 < \cdots < A_j < B_1 < B_2 < \cdots < B_j < C_1 < C_2 < \cdots < C_j$$

Component Backwards Ordering (CBO)

Each event is expanded into its series of sub-events in the order of current phase to first phase, *j..1*.

$$A_j < \cdots A_2 < A_1 < B_j < \cdots < B_2 < B_1 < C_j < \cdots < C_2 < C_1$$

Phase Forwards Ordering (PFO)

Each event is expanded into its series of sub-events in the order of first phase to current phase, *1..j*. The sub-events are then considered in the ordering sequence $A < B < C$ for each consecutive phase *1..j*.

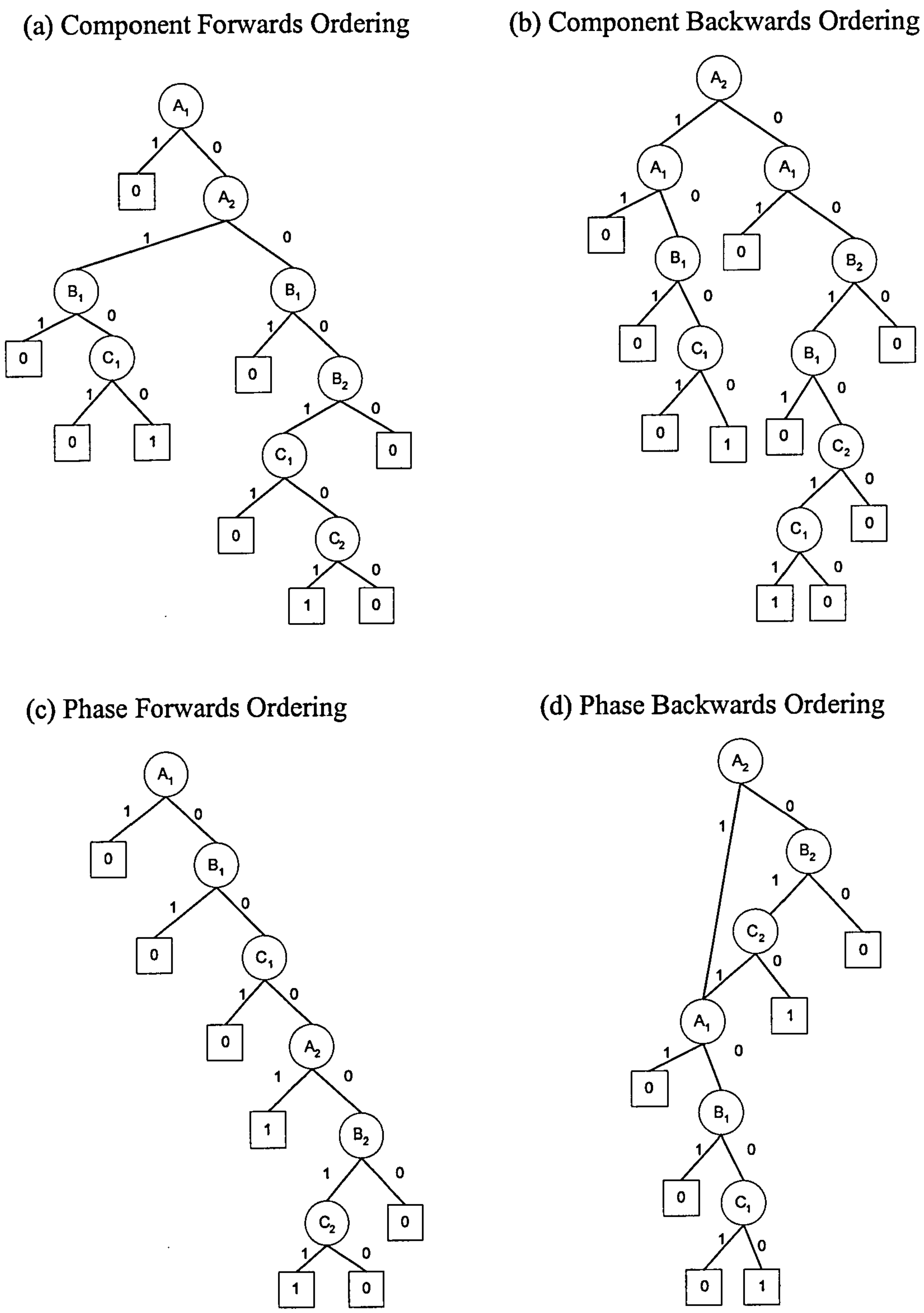
$$A_1 < B_1 < C_1 < A_2 < B_2 < C_2 < \cdots < A_j < B_j < C_j$$

Phase Backwards Ordering (PFO)

Each event is expanded into its series of sub-events in the order of current phase to first phase, *j..1*. The sub-events are then considered in the ordering sequence $A < B < C$ for each consecutive phase *j..1*.

$$A_j < B_j < C_j < \cdots < A_2 < B_2 < C_2 < A_1 < B_1 < C_1$$

The four ordering schemes are applied to the second phase of the example in Figure 4.4 using the method of combining phase 1 success with phase 2 failure. The resulting phase BDDs are given in Figures 4.15(a), 4.15(b), and 4.15(c) and 4.15(d).



(a) Component Forwards Ordering

(b) Component Backwards Ordering

(c) Phase Forwards Ordering

(d) Phase Backwards Ordering

Figure 4.15 Comparison of BDD Variable Ordering Schemes

It can be seen from Figure 4.15 that the ordering scheme of even a simple 2-phased mission can make a difference in the size of the BDD. The largest BDD represents the component backwards ordering scheme with 9 non-terminal nodes, and the smallest BDDs represent the phase backwards and forwards ordering schemes with 6 non-terminal nodes. All four BDD ordering patterns produce the correct prime implicant sets, however the complexity of the BDD will influence the ease of obtaining and simplifying the implicant sets.

To construct the most minimal phased mission BDD, the optimal ordering of components in a phase is obtained and then expanded using an optimal expansion of the sub-components. This particular feature is not considered further in this thesis but is a topic for further research.

4.4 Test Cases

The methods described have been applied to some simple systems in order to quantify both phase and mission failure probabilities. Comparisons may also be made to results obtained by a simple Monte Carlo simulation program operating the system over 1000000 simulations.

Four simple systems are given in Figures 4.16 - 4.19.

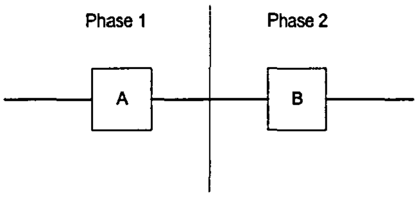


Figure 4.16 Example 1

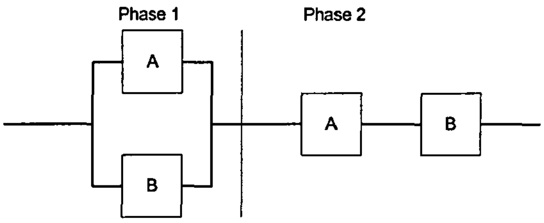


Figure 4.17 Example 2

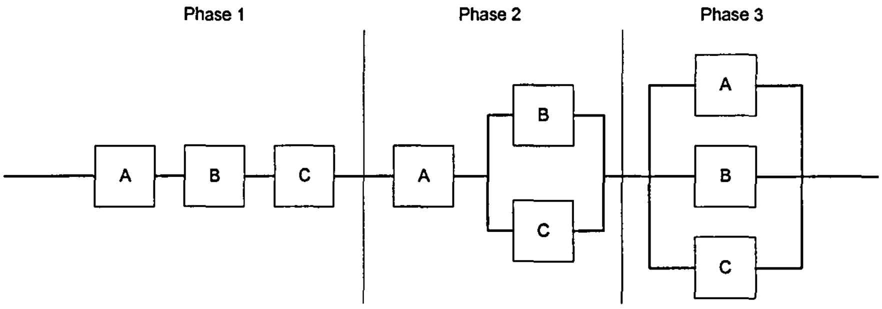


Figure 4.18 Example 3

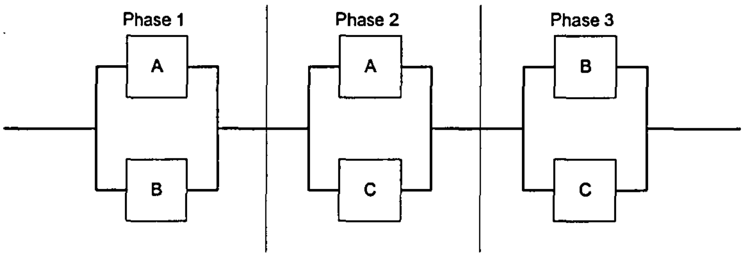


Figure 4.19 Example 4

The quantification of the fault tree and BDD approaches when each component is given a failure rate of 0.001 per hour and all phases are run for the duration of 100 hours (Table 4.1) show that the results obtained by each of the methods are identical.

	FT	BDD	MC
Example 1			
Phase 1 Failure Probability	9.5163x10^{-2}	9.5163x10^{-2}	9.5162x10^{-2}
Phase 2 Failure Probability	1.6402x10^{-1}	1.6402x10^{-1}	1.6405x10^{-1}
MISSION FAILURE PROBABILITY	2.5918x10^{-1}	2.5918x10^{-1}	2.5921x10^{-1}
Example 2			
Phase 1 Failure Probability	9.0559x10^{-3}	9.0559x10^{-3}	9.0561x10^{-3}
Phase 2 Failure Probability	3.2062x10^{-1}	3.2062x10^{-1}	3.2064x10^{-1}
MISSION FAILURE PROBABILITY	3.2968x10^{-1}	3.2968x10^{-1}	3.2970x10^{-1}
Example 3			
Phase 1 Failure Probability	2.5918x10^{-1}	2.5918x10^{-1}	2.5921x10^{-1}
Phase 2 Failure Probability	7.6569x10^{-2}	7.6569x10^{-2}	7.6568x10^{-2}
Phase 3 Failure Probability	1.5184x10^{-3}	1.5184x10^{-3}	1.5187x10^{-3}
MISSION FAILURE PROBABILITY	3.3727x10^{-1}	3.3727x10^{-1}	3.3730x10^{-1}
Example 4			
Phase 1 Failure Probability	9.0559x10^{-3}	9.0559x10^{-3}	9.0560x10^{-3}
Phase 2 Failure Probability	3.1217x10^{-2}	3.1217x10^{-2}	3.1215x10^{-2}
Phase 3 Failure Probability	5.7953x10^{-2}	5.7953x10^{-2}	5.7954x10^{-2}
MISSION FAILURE PROBABILITY	9.8226x10^{-2}	9.8226x10^{-2}	9.8225x10^{-2}

Table 4.1 Test Case Quantifications

where FT - Fault Tree Approach

BDD – Binary Decision Diagram Approach

MC – Mean Failure Probability by Monte-Carlo Approach

4.5 Unconditional Phase Failure Intensity

The rate of phase j failure, w_j, is the probability that phase j failure occurs per unit time during $[t_{j-1}, t_j)$. Considering the method presented for single phase systems in Section 2.2.3.2, the unconditional failure intensity of phase j could be represented by equation (4.23).

$$w_j\ dt = P\left[\bigcup_{l=1}^{N_{pi_j}} \varepsilon_{l_j}\right] - P\left[\overline{A}\bigcup_{l=1}^{N_{pi_j}} \varepsilon_{l_j}\right]$$

where $\overline{A}$ is the event that at least one phase j prime implicant set exists at time t

ε_{l_j} is the event that prime implicant set ε_l occurs in phase j

or $$w_j\ dt = w_j^{(1)}\ dt - w_j^{(2)} dt \qquad (4.23)$$

The first term on the right hand side of equation (4.23) represents the contribution from the occurrence of at least one implicant set during phase j. The second term represents the contribution of prime implicant sets occurring while other prime implicant sets already exist in phase j (i.e. phase j has already failed). This method can be applied to the simple 2-phased mission in Figure 4.20, and the unconditional failure intensity of both phases is derived in Appendix A.

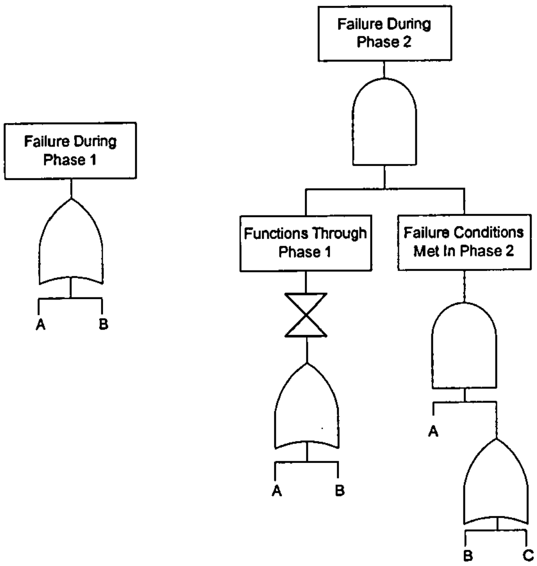


Figure 4.20 Example 2-Phase System

The approach presented in equation (4.23) is seen to be very computationally intensive when applied to the simple example in Figure 4.20. It would be useful if the unconditional phase failure intensity could be derived using a more direct method.

The rate of failure of a phase j, w_j, can also be defined as the probability of phase j failure per unit time given that a mission is taking place. An alternative method to calculate this parameter is presented using the probability of phase failure, Q_j, and the mission frequency, λ_{MISS}, in equation (4.24).

$$w_j = Q_j \, \lambda_{MISS} \tag{4.24}$$

This can be applied to the example in Figure 4.20 as follows:

Phase 1

Top event: $T_1 = A_1 + B_1$

Phase failure probability:
$$\begin{aligned} Q_1 &= q_{A_1} + q_{B_1} - q_{A_1} q_{B_1} \\ &= (1 - e^{-\lambda_A t_1}) + (1 - e^{-\lambda_B t_1}) - (1 - e^{-\lambda_A t_1})(1 - e^{-\lambda_B t_1}) \\ &= 1 - e^{-(\lambda_A + \lambda_B) t_1} \end{aligned}$$

Unconditional failure intensity:
$$\begin{aligned} w_1 &= Q_1 \, \lambda_{MISS} \\ &= \lambda_{MISS} (1 - e^{-(\lambda_A + \lambda_B) t_1}) \end{aligned} \tag{4.25}$$

Phase 2

Top event:
$$\begin{aligned} T_2 &= \overline{A_1} \, \overline{B_1} (A_{12} B_{12} + A_{12} C_{12}) \\ &= A_2 B_2 + A_2 \overline{B_1} C_{12} \end{aligned}$$

Phase failure probability:

$$\begin{aligned} Q_2 &= q_{A_2} q_{B_2} + q_{A_2}(1 - q_{B_1}) q_{C_1} + q_{A_2}(1 - q_{B_1}) q_{C_2} - q_{A_2} q_{B_2} q_{C_1} - q_{A_2} q_{B_2} q_{C_2} \\ &= q_{A_2} q_{B_2} + q_{A_2}(1 - q_{B_1}) q_{C_{12}} - q_{A_2} q_{B_2} q_{C_{12}} \\ &= (e^{-\lambda_A t_1} - e^{-\lambda_A t_2})(e^{-\lambda_B t_1} - e^{-\lambda_B t_2}) + (e^{-\lambda_A t_1} - e^{-\lambda_A t_2}) e^{-\lambda_B t_1} (1 - e^{-\lambda_C t_2}) - (e^{-\lambda_A t_1} - e^{-\lambda_A t_2})(e^{-\lambda_B t_1} - e^{-\lambda_B t_2})(1 - e^{-\lambda_C t_2}) \\ &= e^{-(\lambda_A + \lambda_B) t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-\lambda_A t_1 - \lambda_B t_2} + e^{-(\lambda_A + \lambda_B) t_2} \\ &\quad + e^{-(\lambda_A + \lambda_B) t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-(\lambda_A + \lambda_B) t_1 - \lambda_C t_2} + e^{-(\lambda_A + \lambda_C) t_2 - \lambda_B t_1} \\ &\quad - e^{-(\lambda_A + \lambda_B) t_1} + e^{-\lambda_A t_2 - \lambda_B t_1} + e^{-\lambda_A t_1 - \lambda_B t_2} - e^{-(\lambda_A + \lambda_B) t_2} + e^{-(\lambda_A + \lambda_B) t_1 - \lambda_C t_2} - e^{-(\lambda_A + \lambda_C) t_2 - \lambda_B t_1} - e^{-\lambda_A t_1 - (\lambda_B + \lambda_C) t_2} + e^{-(\lambda_A + \lambda_C + \lambda_B) t_2} \\ &= e^{-(\lambda_A + \lambda_B) t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-\lambda_A t_1 - (\lambda_B + \lambda_C) t_2} + e^{-(\lambda_A + \lambda_C + \lambda_B) t_2} \end{aligned}$$

Unconditional failure intensity: $w_2 = Q_2\,\lambda_{MISS}$

$$= \lambda_{MISS}(e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-\lambda_A t_1 - (\lambda_B+\lambda_C)t_2} + e^{-(\lambda_A+\lambda_C+\lambda_B)t_2}) \tag{4.26}$$

The unconditional failure intensity for the phases of the example in Figure 4.20 (equations (4.25) and (4.26)) are found to be consistent with the expressions obtained in Appendix A (equations (A.9) and (A.30)). The relationship presented in equation (4.24) is therefore seen to be correct, and provides a straightforward method to obtain the unconditional failure intensity of a phase or mission. The fault tree method (Section 4.2) or the BDD method (Section 4.3) allow the failure probability of each individual phase to be calculated. The simple substitution of this parameter into equation (4.24) allows the frequency of phase failure to be obtained.

Similarly, the unconditional failure intensity of a component c in phase j, w_{c_j}, can be defined as the probability that the component fails per unit time during phase j given that it is in a mission. The unconditional failure intensity of component c in phase j may be obtained directly from the component c failure probability in phase j, q_{c_j}, using equation (4.27).

$$w_{c_j} = q_{c_j}\lambda_{MISS} \tag{4.27}$$

where $q_{c_j} = e^{-\lambda_c t_{j-1}} - e^{-\lambda_c t_j}$

λ_{MISS} = Mission frequency

4.6 Summary

The four simple systems described in Section 4.4 are useful to make a suitable quantification for three different methods and allow comparisons between the techniques. In reality a practical system would consist of many more basic events, and operate over additional phases, however the principles of the method are the same.

The techniques described in this chapter are found to be suitable for the solution of systems comprising of non-repairable components operating over a small number of phases. The fault tree method that has been developed for this analysis suffers an explosion in the number of phase failure modes and complexity as the number of phases increases. This leads to computationally intensive calculation procedures.

The binary decision diagram approach is found to provide an efficient alternative to the fault tree technique. The combination of phase failure with previous phase successes can be very simple with an optimal ordering scheme as the events of components failing through sequential phases are considered only once. The quantification of the binary decision diagram approach leads to an exact answer rather than the approximation calculated by the fault tree method. The frequency of phase and component failure is easily obtained using the phase or component failure probability.

There are however certain limitations of this method in terms of its general applicability due to the assumption of non-repairable components. Whilst many systems such as aircraft and spacecraft missions are non-repairable, others will be repairable. In such circumstances the failure probability calculations would need to take account of components repaired upon failure and an alternative approach needs to be developed to account for this.

Chapter 5 Systems with Repairable Components

5.1 Introduction

In many systems, the option of component maintenance will be available. The ability to transform a component from a failed state into a working state is known as *repair*, and the components are described as repairable. For modelling purposes, revealed failures are detected instantly and upon repair a component is considered to be as good as new.

A system is required to work continuously over each of the phases in order to achieve mission success, therefore the parameter of interest is the *reliability* of the system. Fault trees can be used to express the failure logic of a repairable system, but cannot be analysed for an accurate solution. The consideration of repairable components means that the phase algebra in Section 4.2.2 is no longer appropriate, and so other techniques must be employed. Simulation offers a flexible alternative analysis method, however it may be a very computationally time consuming option.

The Markov approach is an appropriate analytical method for the prediction of system reliability (Section 2.4). Conversely this approach is also known to be susceptible to explosions in the number of state equations for even moderate sized problems. Previous research on Markov methods for the solution to phased mission problems by Clarotti et al [30] and Alam and Al-Saggaf [33] have provided a means of calculating the reliability of both individual phases and the entire mission. However these approaches have implemented a full component state transition table comprising of every possible combination of states for all components required in the entire mission. Little investigation appears to have been made into the possibility of reducing the size of the Markov model by considering phase by phase models.

A mission may comprise of both discrete and continuous phases. A discrete phase is a phase which requires the relevant system function to work at an instant in time, thus no state transitions may occur during the phase, and any component failures which exist would have occurred prior to this phase. Component states will be determined by failures and repairs that have taken place in previous phases. A fault tree approach could be applied to model such a phase. A continuous phase requires the appropriate system configuration to be reliable for the specified phase duration and the possibility of component repair requires a Markov approach.

To illustrate the distinction between discrete and continuous phases consider a ship in a battle group in action. An example of the discrete phase would be for the ship to launch a missile at a point in time during a manoeuvre. The ship would need the propulsion and steering system to work over a period of time (reliability) whilst getting to the correct location. To defend itself by launching a missile it would need the missile launch system to function at the instant required. In this case, for efficiency, it may be possible to combine fault tree and reduced Markov methods to produce an accurate and efficient calculation of phase and mission reliability whilst reducing the complexity of the model and computational time.

The methods developed to analyse a phased mission where the components are repairable are reviewed in the remainder of this chapter. Since not all components will be required in every phase of the mission, an *irrelevant* component is defined:

> An irrelevant component in phase j is not required for the successful operation of phase j but may contribute to previous or subsequent phases of the mission.

5.1.1 Markov Model Explosion Problem

The Markov model for a system is susceptible to an explosion in the number of state equations as the number of components in the model increases. If n components are required in a phase and each can work or fail (i.e. 2-state), there will be 2^n system states. To implement this model, the 2^n state equations are formed using a 2^n x 2^n transition matrix.

As the mathematical treatment of the model assumes that only one event (usually corresponding to a single component failure or repair) can occur in a small period of time dt, the possible state changes are very limited. This leads to a very sparse transition matrix as the number of components increases. Most matrix entries are 0, indicating that states cannot communicate with each other. To store every element of such a large matrix would require the use of substantial amounts of unnecessary computer memory. This severely limits the size of the analysis which can be performed. It is possible to do this more efficiently by creating a *linked list*. Such a list would allocate space only to store transitions that can occur, thus freeing memory for other purposes.

To demonstrate the construction of a linked list, an example system consisting of components A, B and C can be used, shown in Figure 5.1.

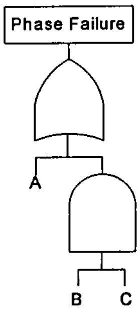


Figure 5.1 Example 3-Component System

There are eight possible system states, denoted by $S_1^{(ABC)} - S_8^{(ABC)}$. A full listing of the system states is given in Figure 5.2.

	A	B	C
$S_1^{(ABC)}$	0	0	0
$S_2^{(ABC)}$	0	0	1
$S_3^{(ABC)}$	0	1	0
$S_4^{(ABC)}$	0	1	1
$S_5^{(ABC)}$	1	0	0
$S_6^{(ABC)}$	1	0	1
$S_7^{(ABC)}$	1	1	0
$S_8^{(ABC)}$	1	1	1

where 1 Failed
0 Working

Figure 5.2 System states for 3-Component Model

The failed states of this system are $S_4^{(ABC)} - S_8^{(ABC)}$. If the failed states of the system are known to be absorbing so that no transitions may be made out of them, the state transition matrix is found to be very sparse in equation (5.1).

$$[A]=\begin{bmatrix} -(\lambda_A+\lambda_B+\lambda_C) & \lambda_C & \lambda_B & 0 & \lambda_A & 0 & 0 & 0 \\ \upsilon_C & -(\lambda_A+\lambda_B+\upsilon_C) & 0 & \lambda_B & 0 & \lambda_A & 0 & 0 \\ \upsilon_B & 0 & -(\lambda_A+\upsilon_B+\lambda_C) & \lambda_C & 0 & 0 & \lambda_A & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5.1)$$

There are 64 possible system state transitions, but only 12 have non-zero values. To store all 64 entries in a data array would use unnecessary memory, thus only the non-zero entries are allocated space. This dynamic memory allocation is only limited by the size of available memory.

A linked list is a collection of structures, each containing a set of member variables. In this example, the member variables will contain data for each non-zero state transition – the departure state, the destination state, and the rate of transition. Each structure will also have a member that references the next structure in the list. By defining a head structure as the first entry of the list, subsequent non-zero transitions are referenced by sequential structures. The final entry in the list is defined as the tail structure, and is terminated by a NULL pointer reference. In this way it is possible to store only the 12 non-zero transition rate values, and access to each is obtained by traversing the list.

This dynamic memory allocation with structures and pointer references is demonstrated in Figure 5.3.

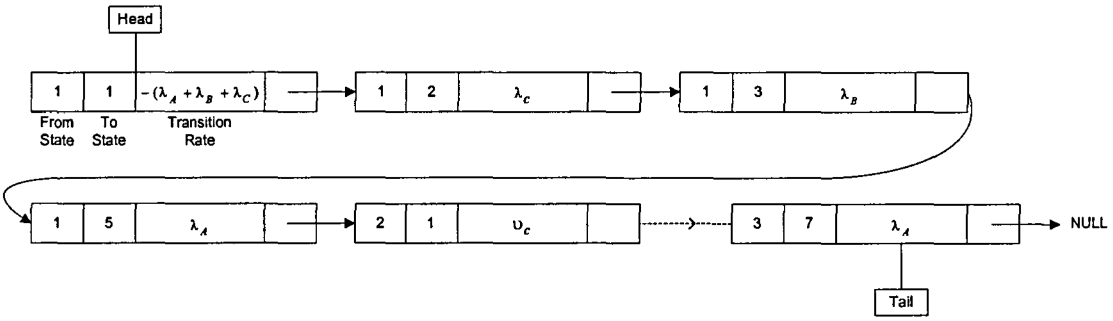


Figure 5.3 Dynamic Memory Allocation – Linked Lists

This process has been implemented in all three modelling scenarios presented in the following sections.

5.2 Reliability of a Phased Mission with Discrete and Continuous Phases

The method for solution to a repairable phased mission system using a full Markov model is presented in Section 5.2.1. The possibility of reducing the size of the Markov model by considering phase by phase models is discussed in sections 5.2.2 and 5.2.3.

5.2.1 Full Markov Method

A full Markov model is generated by using a single model which works over all phases of the mission. This model will have a single vector **[P]** of system state probabilities for every phase of the mission. **[P]** is constructed including all components featured in every stage. The model is then formed by considering the different requirements for each phase success and mission success. The state transition matrix is used to obtain the probability of the system residing in each of the total possible system states (N_S). The matrix equations used to model this are represented by equation (5.2).

$$[\dot{\mathbf{P}}] = [\mathbf{P}][\mathbf{A}] \tag{5.2}$$

where **[A]** is the state transition matrix

At the start of a mission, it is assumed that all components are in the working state, S_1. The initial N_S state vector would be given as equation (5.3).

$$\mathbf{P}(0) = [1\ 0\ 0 \cdots\cdots 0] \tag{5.3}$$

Since all components are initially in the working state, if the first phase is discrete then phase success is guaranteed and the original state vector is passed straight to phase 2. If the first phase is continuous, the N_S x N_S state transition matrix must be created. All possible component state transitions are entered into the transition matrix **[A]**. The identification of states that cause system failure determines absorbing states, and thus no transitions out of them are possible. All entries in the row of an absorbing state become zero.

The set of differential equations are evaluated over the duration of the phase. The reliability of the phase is calculated by the sum of the probabilities of the system residing in a successful state at the end of phase 1 at $t{=}t_1$.

The system can begin a new (next) phase if and only if it is in a successful state for both the new phase and the preceeding phase, thus the failed and success states of the new phase must be identified. If a successful state of the preceeding phase becomes a failed state in the new phase, it is known as a *transition failure* and causes termination of the system. The total transition failure probability on commencing a new phase is calculated by the sum of the probability of all such cases at the phase boundary.

The successful entry into a phase i produces a new set of initial conditions, equation (5.4)

$$\mathbf{P}(t_{i-1}) = [P_1(t_{i-1})\,,\, P_2(t_{i-1})\,,\, P_3(t_{i-1})\,,\ \cdots\ P_{N_S}(t_{i-1})] \tag{5.4}$$

This set of initial state probabilities is derived from the final state probabilities of the previous phase. Since the system cannot reside in a failed state for either phase at the transition point all states representative of this are assigned an initial probability of 0:

For all states j that result in system success for both phases, $P_j(t_{i-1}) = P_j(t_{i-1})$

(i.e. remain unchanged)

For all states k that cause failure in either or both phases, $P_k(t_{i-1}) = 0$

If the new phase is of a discrete nature, the phase solution is obtained directly from the previous phase. If the new phase is continuous, all possible component state transitions are again entered into the transition matrix. The new set of differential equations are then solved over the time duration of phase i.

This process is repeated until the end of the mission is reached. The final mission reliability is obtained by the sum of the probabilities that the system is in a successful state at the end of the final phase. The algorithm for this method is given in Figure 5.4.

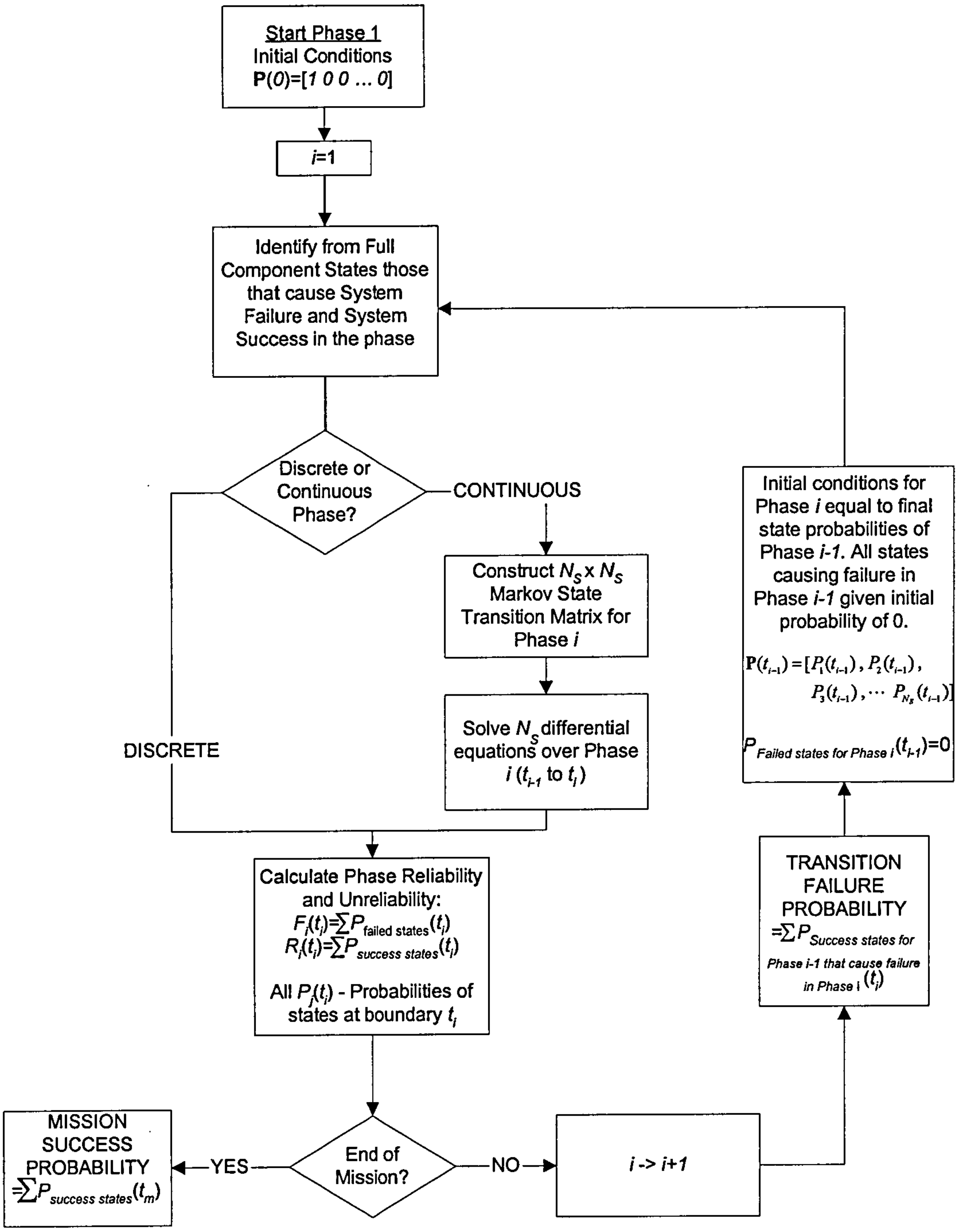

Start Phase 1
Initial Conditions
P(0)=[1 0 0 ... 0]
i=1
Identify from Full Component States those that cause System Failure and System Success in the phase
Discrete or Continuous Phase?
CONTINUOUS
Construct N_S x N_S Markov State Transition Matrix for Phase i
Solve N_S differential equations over Phase i (t_{i-1} to t_i)
DISCRETE
Calculate Phase Reliability and Unreliability:
F_i(t_i)=∑P_failed states(t_i)
R_i(t_i)=∑P_success states(t_i)
All P_j(t_i) - Probabilities of states at boundary t_i
End of Mission?
YES
MISSION SUCCESS PROBABILITY =∑P_success states(t_m)
NO
i -> i+1
TRANSITION FAILURE PROBABILITY =∑P_Success states for Phase i-1 that cause failure in Phase i(t_i)
Initial conditions for Phase i equal to final state probabilities of Phase i-1. All states causing failure in Phase i-1 given initial probability of 0.
P(t_{i-1})=[P_1(t_{i-1}), P_2(t_{i-1}), P_3(t_{i-1}), ··· P_{N_s}(t_{i-1})]
P_Failed states for Phase i(t_{i-1})=0

Figure 5.4 Algorithm to Demonstrate Full Markov Method

An example of a simple 3-phased mission illustrated in Figure 5.5 may be used to demonstrate this method. In this example there are a total of four components in the system, A, B, C, and D. Each component k has an associated failure and repair rate denoted by λ_k and v_k respectively. The total number of component states, 2^4, means that continuous phases require the construction of a 16 x 16 state transition matrix. The components may be required in some or all of the phases.

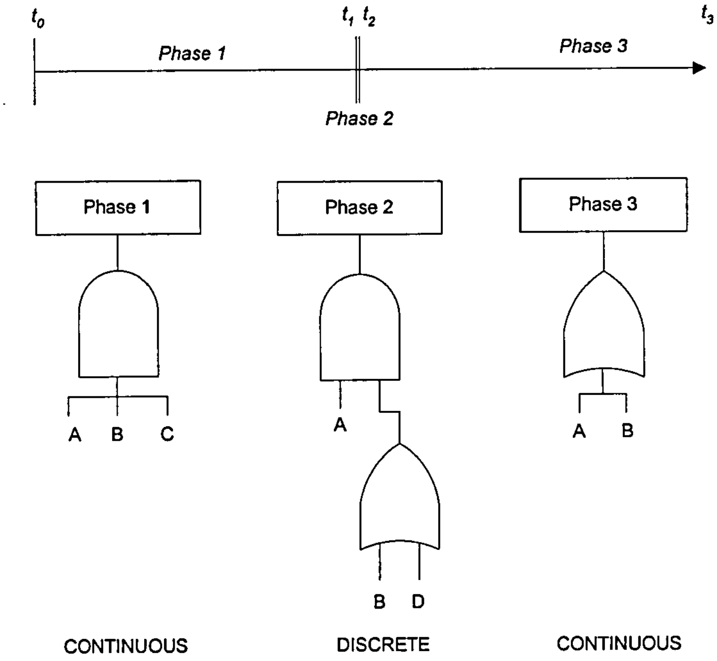


Figure 5.5 Discrete and Continuous Phased Mission

The first phase is of a continuous nature, commencing at $t=0$ and finishing at $t=t_1$. The second phase is instantaneous and thus $t_1=t_2$. The third and final phase is again continuous and runs from to $t=t_2$ to $t=t_3$. Fault trees represent the failure conditions for the system in each phase.

There are 16 possible combinations of component conditions shown in Figure 5.6. The possible state transitions have a rate which corresponds to either the failure or repair of a single component. These rates are assumed to be constant for each component, and repair is revealed and initialised as soon as component failure occurs.

The full state transition matrix for all possible *16* x *16* component state transitions, not accounting for any particular phase, is represented in equation (5.5).

	A	*B*	*C*	*D*
$S_1^{(ABCD)}$	0	0	0	0
$S_2^{(ABCD)}$	0	0	0	1
$S_3^{(ABCD)}$	0	0	1	0
$S_4^{(ABCD)}$	0	0	1	1
$S_5^{(ABCD)}$	0	1	0	0
$S_6^{(ABCD)}$	0	1	0	1
$S_7^{(ABCD)}$	0	1	1	0
$S_8^{(ABCD)}$	0	1	1	1
$S_9^{(ABCD)}$	1	0	0	0
$S_{10}^{(ABCD)}$	1	0	0	1
$S_{11}^{(ABCD)}$	1	0	1	0
$S_{12}^{(ABCD)}$	1	0	1	1
$S_{13}^{(ABCD)}$	1	1	0	0
$S_{14}^{(ABCD)}$	1	1	0	1
$S_{15}^{(ABCD)}$	1	1	1	0
$S_{16}^{(ABCD)}$	1	1	1	1

Where *1* Failed
0 Working

Figure 5.6 Four Component State Table

$$[A]=\begin{bmatrix}
-\Sigma_1 & \lambda_D & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\upsilon_D & -\Sigma_2 & 0 & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 & 0 \\
\upsilon_C & 0 & -\Sigma_3 & \lambda_D & 0 & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 \\
0 & \upsilon_C & \upsilon_D & -\Sigma_4 & 0 & 0 & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 \\
\upsilon_B & 0 & 0 & 0 & -\Sigma_5 & \lambda_D & \lambda_C & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 \\
0 & \upsilon_B & 0 & 0 & \upsilon_D & -\Sigma_6 & 0 & \lambda_C & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 & 0 \\
0 & 0 & \upsilon_B & 0 & \upsilon_C & 0 & -\Sigma_7 & \lambda_D & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 \\
0 & 0 & 0 & \upsilon_B & 0 & \upsilon_C & \upsilon_D & -\Sigma_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_A \\
\upsilon_A & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_9 & \lambda_D & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 \\
0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & 0 & \upsilon_D & -\Sigma_{10} & 0 & \lambda_C & 0 & \lambda_B & 0 & 0 \\
0 & 0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & \upsilon_C & 0 & -\Sigma_{11} & \lambda_D & 0 & 0 & \lambda_B & 0 \\
0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & \upsilon_C & \upsilon_D & -\Sigma_{12} & 0 & 0 & 0 & \lambda_B \\
0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & 0 & 0 & -\Sigma_{13} & \lambda_D & \lambda_C & 0 \\
0 & 0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & 0 & \upsilon_D & -\Sigma_{14} & 0 & \lambda_C \\
0 & 0 & 0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & \upsilon_C & 0 & -\Sigma_{15} & \lambda_D \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & \upsilon_C & \upsilon_D & -\Sigma_{16}
\end{bmatrix} \quad (5.5)$$

where element in row *j* and column *k* represents the transition from state $S_j^{(ABCD)}$ to $S_k^{(ABCD)}$

and $\sum_j$ = sum of elements in row *j* (except element *jj*)

Phase 1

All components are considered to be in the working state at the start of a mission and so the initial state probabilities are defined in equation (5.6).

$$\mathbf{P}(0) = [1 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0] \tag{5.6}$$

Phase 1 will complete successfully as long as components A, B, and C do not reside in the failed state at the same point in time, i.e. states $S_{15}^{(ABCD)}$ and $S_{16}^{(ABCD)}$ are not reached. As these states cause system failure, they are defined as *absorbing* states. Once an absorbing state is entered, no transitions may be made into other states and the system will remain failed. All matrix entries on the row of an absorbing state are assigned to 0 in [**A**] to represent this. The transition matrix becomes as shown in equation (5.7).

$$[\mathbf{A}] = \begin{bmatrix}
-\Sigma_1 & \lambda_D & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\upsilon_D & -\Sigma_2 & 0 & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 & 0 \\
\upsilon_C & 0 & -\Sigma_3 & \lambda_D & 0 & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 & 0 \\
0 & \upsilon_C & \upsilon_D & -\Sigma_4 & 0 & 0 & 0 & \lambda_B & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 & 0 \\
\upsilon_B & 0 & 0 & 0 & -\Sigma_5 & \lambda_D & \lambda_C & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 & 0 & 0 \\
0 & \upsilon_B & 0 & 0 & \upsilon_D & -\Sigma_6 & 0 & \lambda_C & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 & 0 \\
0 & 0 & \upsilon_B & 0 & \upsilon_C & 0 & -\Sigma_7 & \lambda_D & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_A & 0 \\
0 & 0 & 0 & \upsilon_B & 0 & \upsilon_C & \upsilon_D & -\Sigma_8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_A \\
\upsilon_A & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\Sigma_9 & \lambda_D & \lambda_C & 0 & \lambda_B & 0 & 0 & 0 \\
0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & 0 & \upsilon_D & -\Sigma_{10} & 0 & \lambda_C & 0 & \lambda_B & 0 & 0 \\
0 & 0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & \upsilon_C & 0 & -\Sigma_{11} & \lambda_D & 0 & 0 & \lambda_B & 0 \\
0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & 0 & 0 & \upsilon_C & \upsilon_D & -\Sigma_{12} & 0 & 0 & 0 & \lambda_B \\
0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & 0 & 0 & -\Sigma_{13} & \lambda_D & \lambda_C & 0 \\
0 & 0 & 0 & 0 & 0 & \upsilon_A & 0 & 0 & 0 & \upsilon_B & 0 & 0 & \upsilon_D & -\Sigma_{14} & 0 & \lambda_C \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \tag{5.7}$$

The evaluation of the state probabilities over the period from the start of phase 1 (*t*=0) to the end of phase 1 (*t*=*t*$_1$) allows the continuous model to be solved by the set of differential equations as represented in equation (5.2). This will lead to a set of values representing the probability that the system is in each of the 16 states at the end of phase 1. Phase success is achieved if the system is found to reside in any of the working states ($S_1^{(ABCD)}$ - $S_{14}^{(ABCD)}$) at the end of phase 1. As the states are mutually exclusive, state probabilities can be added and the reliability at the end of phase 1 may be represented by equation (5.8).

$$R(t_1) = \sum_{j=1}^{14} P_j^{(ABCD)}(t_1) \tag{5.8}$$

Phase 2

To successfully begin phase 2, the system must reside in a state that produces a working system for both phases 1 and 2. For phase 2 to be in a successful state, component A must be working OR B and D are both working, i.e. the system must be in one of states $S_1^{(ABCD)} - S_9^{(ABCD)}$and $S_{11}^{(ABCD)}$. Transition failure will occur if the system is in a working state for the first phase, but a failed state for the second phase, in this case $S_{10}^{(ABCD)}$ and $S_{12}^{(ABCD)}$ - $S_{14}^{(ABCD)}$. Since phase 2 is a discrete phase, the phase unreliability is equal to the transition failure probability in equation (5.9).

$$Tr(t_1) = P_{10}^{(ABCD)}(t_1) + \sum_{j=12}^{14} P_j^{(ABCD)}(t_1) \tag{5.9}$$

where *Tr(t)* is the probability of transition failure at time *t*

The conditions to represent successful entry to phase 2 are found by the state probabilities at the end of phase 1. All states that result in either phase 1 failure or phase 2 failure are assigned a final probability of 0 at $t{=}t_1$.

As this second phase is a discrete phase, $t_1{=}t_2$, and no state transitions may be made during the phase. Phase success is achieved if the system resides in a successful state upon transition from phase 1. The probability that the system successfully completes phase 2 is the probability that the system resides in a state which is successful for both phases 1 and 2, $S_1^{(ABCD)}$ - $S_9^{(ABCD)}$ and $S_{11}^{(ABCD)}$, and is found by equation (5.10).

$$R(t_2) = \sum_{j=1}^{9} P_j^{(ABCD)}(t_2) + P_{11}^{(ABCD)}(t_2) \tag{5.10}$$

Phase 3

To successfully begin phase 3, the system must reside in a state that produces a working system for both phases 2 and 3. Transition failure will occur if the system is in a working state for phase 2 and a failed state for phase 3, $S_5^{(ABCD)}$-$S_9^{(ABCD)}$ and $S_{11}^{(ABCD)}$, and is found by equation (5.11).

$$Tr(t_2) = \sum_{j=5}^{9} P_j^{(ABCD)}(t_2) + P_{11}^{(ABCD)}(t_2) \qquad (5.11)$$

Phase 3 will be in the working state as long as *A* or *B* do not fail, thus the success states for phase 3 are $S_1^{(ABCD)}$-$S_4^{(ABCD)}$. All other states are assigned an initial probability of 0.

The state probabilities are again evaluated over phase 3 [t_2, t_3) by the solution of the set of differential equations as represented in equation (5.2). The state transition matrix will resemble that of equation (5.5), however since states $S_5^{(ABCD)}$-$S_{16}^{(ABCD)}$ are failed and thus absorbing states, all transition rate entries along rows 5-16 become *0*. This will again lead to a set of values representing the probability that the system is in each of the 16 states at the end of phase 3. Phase and mission success is achieved if the system is found to reside in any of the phase 3 working states ($S_1^{(ABCD)}$-$S_4^{(ABCD)}$) at time $t=t_3$. Reliability at the end of phase 3 may be represented by equation (5.12)

$$R(t_3) = \sum_{j=1}^{4} P_j^{(ABCD)}(t_3) \qquad (5.12)$$

And thus the probability of mission success is given by equation (5.13)

$$R_{MISS} = \sum_{j=1}^{4} P_j^{(ABCD)}(t_3) \qquad (5.13)$$

5.2.2 Combined Reduced Markov and Fault Tree Method

Full Markov models can get very large and in some cases become too large to generate and solve. More efficient ways need to be found which will reduce the size of the Markov model generated. It is only the continuous phases where the reliability calculations necessitate the use of Markov methods. As such it may be possible to develop a method which simplifies the Markov model, to some extent, by removing components which only contribute to the failure of discrete phases.

In segregating components that only feature in discrete phases from those which contribute to the failure of continuous phases, it may be possible to analyse discrete and continuous phases using different methods. A full Markov model for all components featured in only continuous phases ($N_{S_{cont}}$ x $N_{S_{cont}}$) may be determined to identify the requirements for phase success using the set of differential equations given in equation (5.2). The elimination of components used in only discrete phases reduces the size of the full Markov model. Fault trees may then be used to obtain the minimal cut sets of a discrete phase to recognise working and failed phase states of the Markov model combined with discrete phase component states to evaluate phase success.

At the start of a mission, it is assumed that all components are in the working state. Therefore considering continuous phases, the initial $N_{S_{cont}}$ state probability matrix would be given as in equation (5.14).

$$\mathbf{P}(0) = [1\ 0\ 0 \cdots\cdots 0] \tag{5.14}$$

As the first phase will be continuous it is required to identify, from amongst the $N_{S_{cont}}$ system states of the reduced Markov model, those that cause system failure and those that cause system success for phase 1. The $N_{S_{cont}}$ x $N_{S_{cont}}$ transition matrix [**A**] is created. All entries in the row of an absorbing failed state become zero, and the set of $N_{S_{cont}}$ differential equations are evaluated over the duration of the phase. The reliability of the phase is calculated by the sum of the probabilities of the system residing in a successful state at the end of phase 1, at time $t= t_1$.

If the proceeding phase is continuous, the final state probabilities with failed states set to zero may be directly passed to the next phase to give a set of initial state probabilities. All states that cause failure in the proceeding phase contribute to the phase transition failure and are also assigned a probability of 0. The following phase would then be solved in the same way.

If the proceeding phase is discrete, it may feature components that were not considered in the model for the previous phase. The probability of a component c that is not required for the Markov model of continuous phase i being in the failed and success state at the end of the phase is easily evaluated by equations (5.15) as derived in Section 2.4.2.2.

$$q_c(t_i) = \frac{\lambda_c}{\lambda_c + \upsilon_c}[1 - e^{-(\lambda_c+\upsilon_c)t_i}] \qquad a_c(t_i) = 1 - q_c(t_i) \qquad (5.15)$$

The states of the continuous phase Markov model are expanded to give the full system states for the proceeding discrete phase, and their likelihood determined at the end of the continuous phase. By the multiplication of the reduced state probabilities with the availability or unavailability (as appropriate) of the excluded components, it is possible to achieve each of the desired expanded state probabilities.

The failure and success states of the discrete phase may be identified using minimal cut sets determined from the fault tree analysis. All states causing an instant failure in the phase contribute to the phase transition failure and are assigned probability 0 for input into the following phase.

When entering a continuous phase from a discrete phase, the expanded discrete states must be reduced. This is achieved by the summation of the probabilities of all expanded states that contribute to each of the continuous Markov model states to produce a reduced list of initial state probabilities (equation (5.16)) for input to the next phase *i*.

$$\mathbf{P}(t_{i-1}) = [P_1(t_{i-1}),\, P_2(t_{i-1}),\, P_3(t_{i-1}),\ \cdots\ P_{NS_{cont}}(t_{i-1})] \qquad (5.16)$$

All states that cause failure in either the current or previous phase, and also those that cause transition failure are assigned an initial probability of 0.

The algorithm to accomplish this method is given in Figure 5.7. The application of this algorithm may be demonstrated using the 3-phased mission in Figure 5.5.

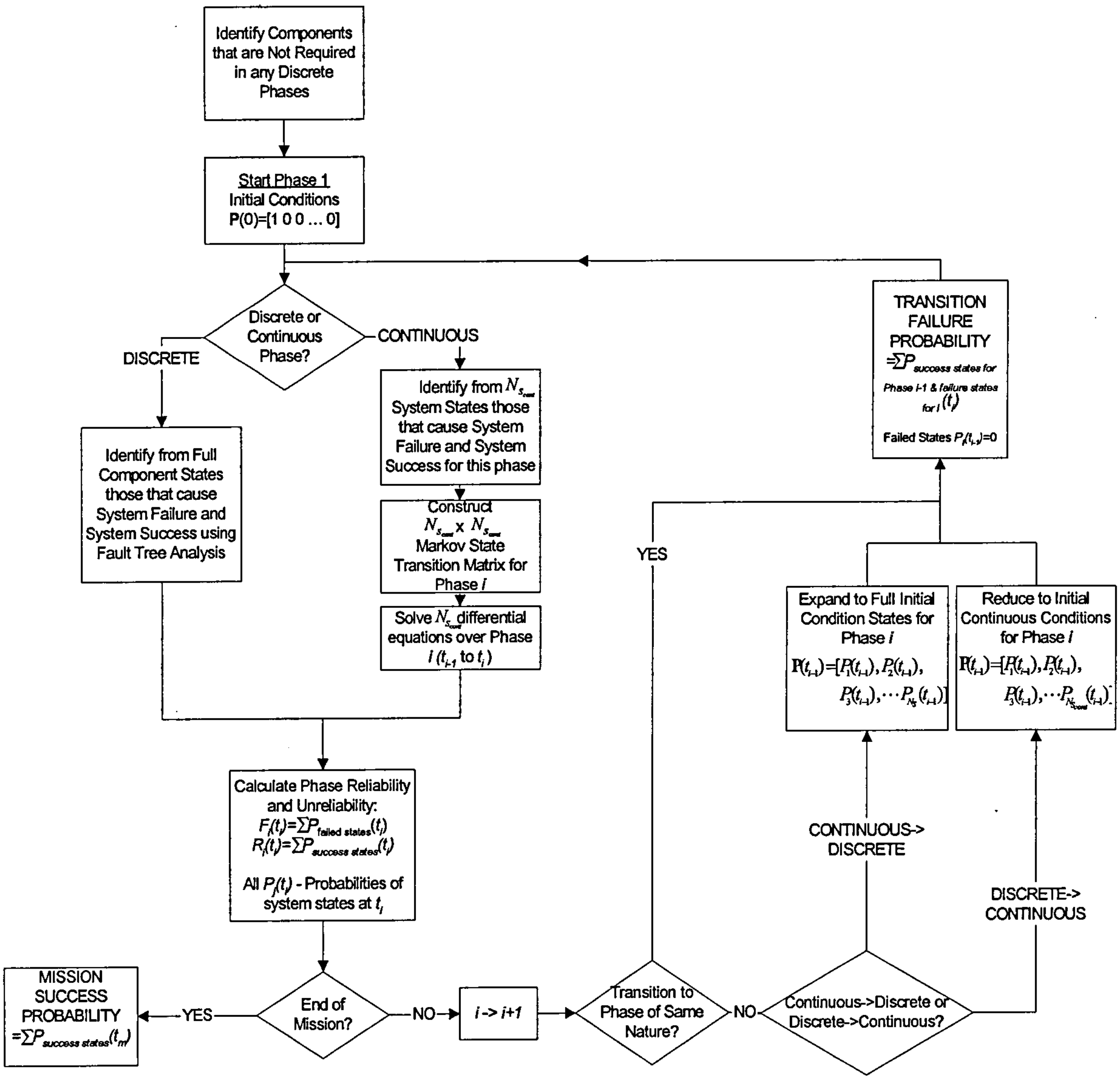

Identify Components that are Not Required in any Discrete Phases
Start Phase 1
Initial Conditions
P(0)=[1 0 0 ... 0]
Discrete or Continuous Phase?
DISCRETE
CONTINUOUS
Identify from Full Component States those that cause System Failure and System Success using Fault Tree Analysis
Identify from $N_{s_{red}}$ System States those that cause System Failure and System Success for this phase
Construct $N_{s_{red}}$ x $N_{s_{red}}$ Markov State Transition Matrix for Phase i
Solve $N_{s_{red}}$ differential equations over Phase i (t_{i-1} to t_i)
Calculate Phase Reliability and Unreliability:
$F_i(t_i)=\sum P_{\text{failed states}}(t_i)$
$R_i(t_i)=\sum P_{\text{success states}}(t_i)$
All $P_j(t_i)$ - Probabilities of system states at t_i
End of Mission?
YES
MISSION SUCCESS PROBABILITY $=\sum P_{\text{success states}}(t_m)$
NO
i-> i+1
Transition to Phase of Same Nature?
YES
NO
Continuous->Discrete or Discrete->Continuous?
CONTINUOUS-> DISCRETE
DISCRETE-> CONTINUOUS
Expand to Full Initial Condition States for Phase i
$\mathbf{P}(t_{i-1})=[P_1(t_{i-1}),P_2(t_{i-1}), P_3(t_{i-1}),\cdots P_{N_s}(t_{i-1})]$
Reduce to Initial Continuous Conditions for Phase i
$\mathbf{P}(t_{i-1})=[P_1(t_{i-1}),P_2(t_{i-1}), P_3(t_{i-1}),\cdots P_{N_{s_{red}}}(t_{i-1})]$
TRANSITION FAILURE PROBABILITY
$=\sum P_{\text{success states for Phase i-1 \& failure states for i}}(t_i)$
Failed States $P_j(t_{i-1})$=0

Figure 5.7 Algorithm to Demonstrate Combined Markov and Fault Tree Methods

Prior To Analysis

It can be noted that component D is only required in the discrete phase 2. Therefore the reduced continuous phase Markov model is formed by considering the states of only components A, B and C as shown in Figure 5.8. The reduced state transition matrix, not accounting for any particular phase, is given in equation (5.17).

	A	B	C
$S_1^{(ABC)}$	0	0	0
$S_2^{(ABC)}$	0	0	1
$S_3^{(ABC)}$	0	1	0
$S_4^{(ABC)}$	0	1	1
$S_5^{(ABC)}$	1	0	0
$S_6^{(ABC)}$	1	0	1
$S_7^{(ABC)}$	1	1	0
$S_8^{(ABC)}$	1	1	1

Figure 5.8 Three Component State Table

$$[\mathrm{A}]=\begin{bmatrix} -\Sigma_1 & \lambda_C & \lambda_B & 0 & \lambda_A & 0 & 0 & 0 \\ \upsilon_C & -\Sigma_2 & 0 & \lambda_B & 0 & \lambda_A & 0 & 0 \\ \upsilon_B & 0 & -\Sigma_3 & \lambda_C & 0 & 0 & \lambda_A & 0 \\ 0 & \upsilon_B & \upsilon_C & -\Sigma_4 & 0 & 0 & 0 & \lambda_A \\ \upsilon_A & 0 & 0 & 0 & -\Sigma_5 & \lambda_C & \lambda_B & 0 \\ 0 & \upsilon_A & 0 & 0 & \upsilon_C & -\Sigma_6 & 0 & \lambda_B \\ 0 & 0 & \upsilon_A & 0 & \upsilon_B & 0 & -\Sigma_7 & \lambda_C \\ 0 & 0 & 0 & \upsilon_A & 0 & \upsilon_B & \upsilon_C & -\Sigma_8 \end{bmatrix} \tag{5.17}$$

Phase 1

The analysis for phase 1 is performed in the same way as that of the full Markov method. However in this case there is only one failed state, $S_8^{(ABC)}$. As this failed state is absorbing, the transition rate entries along row 8 become 0 and the transition state matrix is as shown in equation (5.18).

$$[\mathrm{A}]=\begin{bmatrix} -\Sigma_1 & \lambda_C & \lambda_B & 0 & \lambda_A & 0 & 0 & 0 \\ \upsilon_C & -\Sigma_2 & 0 & \lambda_B & 0 & \lambda_A & 0 & 0 \\ \upsilon_B & 0 & -\Sigma_3 & \lambda_C & 0 & 0 & \lambda_A & 0 \\ 0 & \upsilon_B & \upsilon_C & -\Sigma_4 & 0 & 0 & 0 & \lambda_A \\ \upsilon_A & 0 & 0 & 0 & -\Sigma_5 & \lambda_C & \lambda_B & 0 \\ 0 & \upsilon_A & 0 & 0 & \upsilon_C & -\Sigma_6 & 0 & \lambda_B \\ 0 & 0 & \upsilon_A & 0 & \upsilon_B & 0 & -\Sigma_7 & \lambda_C \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.18}$$

The initial conditions for the probability of each of the states are given by equation (5.19).

$$P(0) = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \tag{5.19}$$

The solution of the set of differential equations (5.2) produces the final state probabilities at t_1 for each of the 8 states in Figure 5.8. The success probability for phase 1 is found by the probability that the system resides in any of the phase 1 success states, $S_1^{(ABC)}$ - $S_7^{(ABC)}$, in equation (5.20).

$$R(t_1) = \sum_{j=1}^{7} P_j^{(ABC)}(t_1) \tag{5.20}$$

Phase 2

Until now, the state of component D has not been considered. It is assumed that component D could have failed during phase 1 with failure rate λ_D, and been repaired in phase 1 with repair rate υ_D. To begin phase 2, the probability of this component being in the failed and working state at the end of phase 1 must be calculated. As a discrete phase occurs at an instant of time, these probabilities are easily found by the unavailability and availability of the component at $t=t_1$. Since component D is repairable up to this point, this would be calculated using equations (5.15) where i=1.

The state probabilities for the end of phase 1 may be multiplied by the availability and unavailability of component D at the phase change time to produce the probabilities of the full listing of all 16 possible phase states as shown in Table 5.1.

Phase 2 transition failure will occur if the system resides in a state representative of success in phase 1 but failure in phase 2 at the phase boundary, and would have a probability associated with it found by summing the likelihoods of all such states.

Discrete Phase 2 State Probability (Figure 5.6)	Component				Calculation from Phase 1 Continuous State Probabilities (Figure 5.8)
	A	B	C	D	
$P_1^{(ABCD)}$	0	0	0	0	$P_1^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_2^{(ABCD)}$	0	0	0	1	$P_1^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_3^{(ABCD)}$	0	0	1	0	$P_2^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_4^{(ABCD)}$	0	0	1	1	$P_2^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_5^{(ABCD)}$	0	1	0	0	$P_3^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_6^{(ABCD)}$	0	1	0	1	$P_3^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_7^{(ABCD)}$	0	1	1	0	$P_4^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_8^{(ABCD)}$	0	1	1	1	$P_4^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_9^{(ABCD)}$	1	0	0	0	$P_5^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_{10}^{(ABCD)}$	1	0	0	1	$P_5^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_{11}^{(ABCD)}$	1	0	1	0	$P_6^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_{12}^{(ABCD)}$	1	0	1	1	$P_6^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_{13}^{(ABCD)}$	1	1	0	0	$P_7^{(ABC)}(t_1)\cdot a_D(t_1)$
$P_{14}^{(ABCD)}$	1	1	0	1	$P_7^{(ABC)}(t_1)\cdot q_D(t_1)$
$P_{15}^{(ABCD)}$	1	1	1	0	0
$P_{16}^{(ABCD)}$	1	1	1	1	0

Table 5.1 Obtaining Discrete Phase 2 State Probabilities from Reduced Continuous Phase 1 State Probabilities

It is possible to evaluate the failed states of phase 2 using fault tree analysis. By obtaining the minimal cut sets for this phase it enables identification of all states that would cause the phase transition to result in failure of the system. In this case the minimal cut sets are:

$$AB$$

$$AD$$

From the full component state list (Figure 5.6) it can be seen that the failed states for this phase are $S_{10}^{(ABCD)}$ and $S_{12}^{(ABCD)}$ - $S_{16}^{(ABCD)}$. However, since states $S_{15}^{(ABCD)}$ - $S_{16}^{(ABCD)}$ represent failure in phase 1, the transition failure is found by the sum of the probabilities that the system is in states $S_{10}^{(ABCD)}$ and $S_{12}^{(ABCD)}$ - $S_{14}^{(ABCD)}$ at the transition point between the first and second phases in equation (5.9). So, using the extended (full) state listing, the success of this phase is again found using equation (5.10).

Phase 3

All states that cause failure in phase 2 ($S_{10}^{(ABCD)}$ and $S_{12}^{(ABCD)}$ - $S_{16}^{(ABCD)}$) are assigned a final probability of 0 for entry to phase 3. The expanded discrete phase 2 states must be reduced to give the initial continuous Markov model states for phase 3 (Figure 5.8). This is achieved by the summation of the probabilities of all expanded states that contribute to each of the continuous Markov model states to produce a reduced list of initial state probabilities for input to phase 3 and is summarised in Table 5.2.

Continuous State Ref (Listed in Figure 5.8)	Component States			State Probability from Phase 2 Discrete State Probabilities (Figure 5.6)
	A	B	C	
$S_1^{(ABC)}$	0	0	0	$P_1^{(ABCD)}(t_2)+P_2^{(ABCD)}(t_2)$
$S_2^{(ABC)}$	0	0	1	$P_3^{(ABCD)}(t_2)+P_4^{(ABCD)}(t_2)$
$S_3^{(ABC)}$	0	1	0	$P_5^{(ABCD)}(t_2)+P_6^{(ABCD)}(t_2)$
$S_4^{(ABC)}$	0	1	1	$P_7^{(ABCD)}(t_2)+P_8^{(ABCD)}(t_2)$
$S_5^{(ABC)}$	1	0	0	$P_9^{(ABCD)}(t_2)$
$S_6^{(ABC)}$	1	0	1	$P_{11}^{(ABCD)}(t_2)$
$S_7^{(ABC)}$	1	1	0	0
$S_8^{(ABC)}$	1	1	1	0

Table 5.2 Obtaining Continuous Phase 3 Initial State Probabilities from Expanded Discrete Phase 2 State Probabilities

To successfully begin phase 3, the system must reside in a state that produces a working system for both phases 2 and 3. From the simplified component state list (Table 5.2) it may be identified that the states to successfully complete phase 2 are those where either A or B are working, $S_1^{(ABC)}$ - $S_6^{(ABC)}$. The success states for phase 3 are $S_1^{(ABC)}$ - $S_2^{(ABC)}$. Therefore phase 3 transition failure will occur if the system is in states $S_3^{(ABC)}$ - $S_6^{(ABC)}$ and is given in equation (5.21).

$$Tr(t_2)=\sum_{j=3}^{6}P_j^{(ABC)}(t_2) \qquad (5.21)$$

Since the success states for phase 3 are $S_1^{(ABC)}$-$S_2^{(ABC)}$, all other states are assigned an initial probability of 0 on entering the phase.

The state probabilities are again evaluated over the time between the start of phase 3 ($t=t_2$) and the end of phase 3 ($t=t_3$) by the solution of the set of differential equations as represented in equation (5.2). The state transition matrix will resemble that of equation (5.17), however since states $S_3^{(ABC)}$-$S_8^{(ABC)}$ are failed and thus absorbing states, all entries along rows 3-8 will be 0. This will again lead to a set of values representing the probability that the system is in each of the 8 states at the end of phase 3. Phase and mission success is achieved if the system is found to reside in either of the working states ($S_1^{(ABC)}$-$S_2^{(ABC)}$) at the end of phase 3. Reliability at the end of phase 3 is represented by equation (5.22).

$$R(t_3) = \sum_{j=1}^{2} P_j^{(ABC)}(t_3) \qquad (5.22)$$

And thus mission success is denoted by equation (5.23).

$$R_{MISS} = \sum_{j=1}^{2} P_j^{(ABC)}(t_3) \qquad (5.23)$$

It can be seen that by identifying components that are only present in discrete phases, they can be eliminated from the Markov model which then only considers components featuring in continuous phases. This can result in a much smaller set of system states and therefore equations. The model formulation is such that every component which is removed from the Markov model will halve its size. The state of all components used in only discrete phases is easily calculated at any point to allow accurate calculation of phase success.

5.2.3 Combined Minimal Markov and Fault Tree Method

The elimination of components used in only discrete phases from the full Markov Model results in a reduction in the number of system states and thus the number of differential equations to be solved over the phase duration. However, the solution of all continuous phases still requires a transition matrix defined by the number of possible states of all remaining components i.e. components which appear in any of the continuous phases. The Markov models can still be large and so there is still room for improvement.

The smallest possible Markov models that could be formed are those used to model each individual continuous phase. Analysis over a continuous phase duration is performed by application of a minimal Markov model (N_{S_i} x N_{S_i}) using only the components required in the particular phase *i*. The full set of states for the total mission is reduced to evaluate initial conditions for each phase, and expanded out again at the end of a phase to enable calculation of successful entry to the immediately succeeding phase. Discrete phase success may again be calculated using fault tree analysis.

At the start of a mission, it is again assumed that all components are in the working state, which is labelled state S_1. Since the first phase will be a continuous phase, the initial N_{S_i} state probability matrix is given by:

$$\mathbf{P}(0) = [1\ 0\ 0 \cdots\cdots 0] \tag{5.24}$$

Identification of the success and failure states out of the minimal N_{S_i} states allows the N_{S_i} x N_{S_i} transition matrix [**A**] to be created. All entries in the row of an absorbing failed state become zero, and the set of N_{S_i} differential equations are evaluated over the duration of the phase. The reliability of the phase is calculated by the sum of the probabilities of the system residing in a successful state at the end of phase 1 ($t=t_1$).

As proceeding continuous phases may not require the same components, it is necessary to expand the reduced continuous phase component state probabilities into the full N_S state probabilities regardless of whether the next phase is discrete or continuous. By the multiplication of the reduced state probabilities with other excluded component availabilities and unavailabilities at the end of the phase, it is possible to achieve each of the desired full state probabilities.

The failure and success states of a discrete phase may be identified using fault tree analysis. All states causing an instant failure in the phase contribute to the phase transition failure and are assigned a probability 0 for input into the following phase.

To begin a later continuous phase it is necessary to identify the initial state probabilities. The full N_S states are minimised to states that account for only those components contributing to the phase. This is achieved by the summation of the probabilities of all full states that contribute to each of the reduced states to produce a minimal list of initial state probabilities for input to the next phase *i*, given in equation (5.25).

$$\mathbf{P}(t_{i-1}) = [P_1(t_{i-1})\,,\, P_2(t_{i-1})\,,\, P_3(t_{i-1})\,,\; \cdots\; P_{N_{S_i}}(t_{i-1})] \qquad (5.25)$$

All states that cause failure in either the current or the previous phase, and also those that cause transition failure are assigned an initial probability of 0.

This method leads to a sequence whereby the reduction of component states during a phase is expanded to give a full set of N_S state probabilities at all phase boundaries. The probability of each component *c* that is not required for a particular continuous phase Markov model being in the failed or success state at the end of the phase is evaluated using equations (5.15).

The minimal Markov model state probabilities at the end of phase *i* are multiplied with the unavailability or availability of all components not required in the phase to evaluate the full N_S state probabilities. These full state probabilities are then easily combined to provide reduced state probabilities for input into further minimal Markov models. The algorithm for this method is given in Figure 5.9.

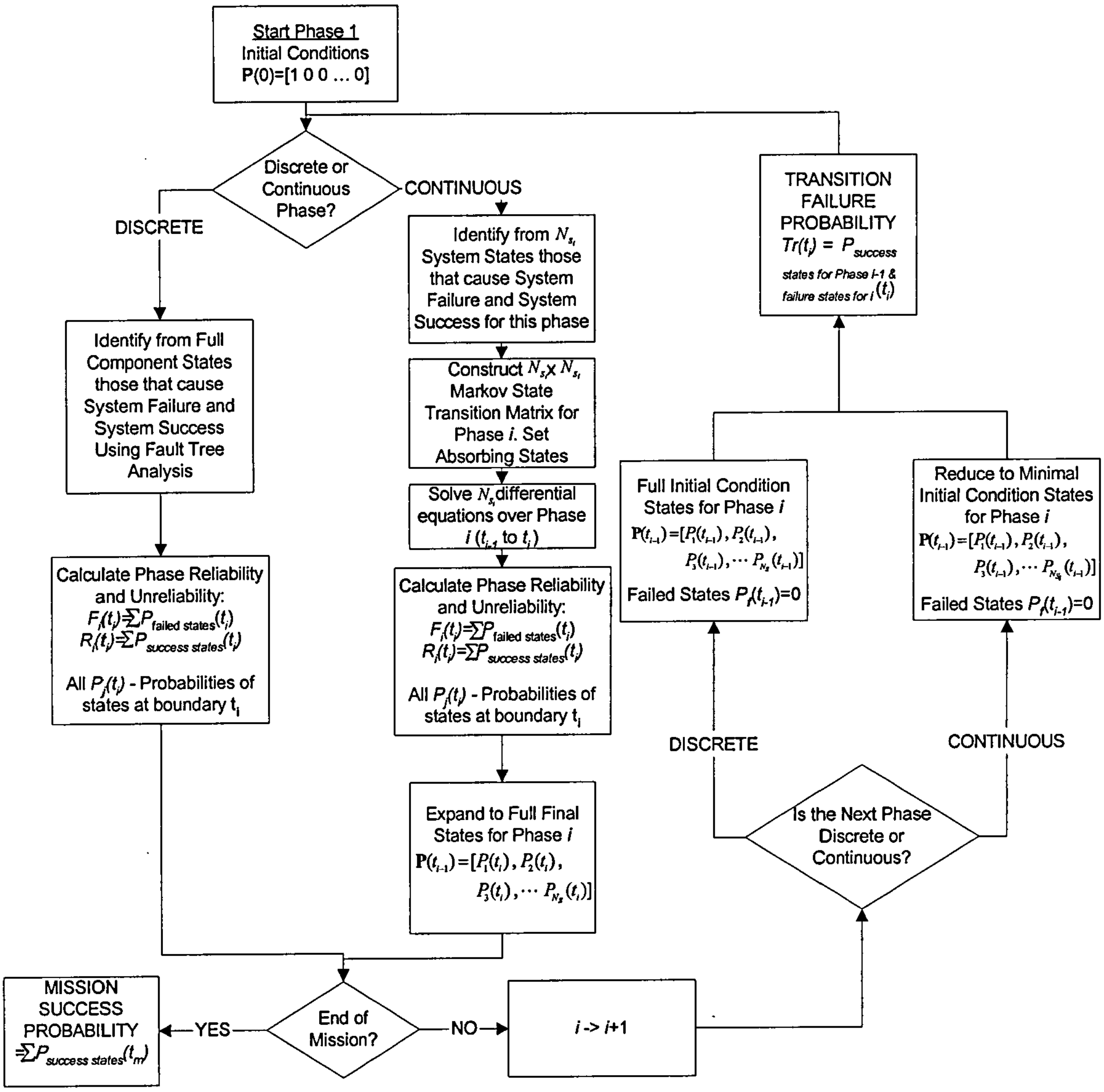

Start Phase 1
Initial Conditions
P(0)=[1 0 0 ... 0]
Discrete or Continuous Phase?
DISCRETE
CONTINUOUS
Identify from Full Component States those that cause System Failure and System Success Using Fault Tree Analysis
Identify from N_{s_i} System States those that cause System Failure and System Success for this phase
Construct N_sx N_{s_i} Markov State Transition Matrix for Phase i. Set Absorbing States
Solve N_{s_i} differential equations over Phase i (t_{i-1} to t_i)
Calculate Phase Reliability and Unreliability:
$F_i(t_i)=\sum P_{\text{failed states}}(t_i)$
$R_i(t_i)=\sum P_{success\ states}(t_i)$
All $P_j(t_i)$ - Probabilities of states at boundary t_i
Calculate Phase Reliability and Unreliability:
$F_i(t_i)=\sum P_{\text{failed states}}(t_i)$
$R_i(t_i)=\sum P_{success\ states}(t_i)$
All $P_j(t_i)$ - Probabilities of states at boundary t_i
Expand to Full Final States for Phase i
$\mathbf{P}(t_{i-1})=[P_1(t_i), P_2(t_i), P_3(t_i), \cdots P_{N_s}(t_i)]$
TRANSITION FAILURE PROBABILITY
$Tr(t_i) = P_{success}$ states for Phase I-1 & failure states for i (t_i)
Full Initial Condition States for Phase i
$\mathbf{P}(t_{i-1})=[P_1(t_{i-1}), P_2(t_{i-1}), P_3(t_{i-1}), \cdots P_{N_s}(t_{i-1})]$
Failed States $P_f(t_{i-1})$=0
Reduce to Minimal Initial Condition States for Phase i
$\mathbf{P}(t_{i-1})=[P_1(t_{i-1}), P_2(t_{i-1}), P_3(t_{i-1}), \cdots P_{N_{s_i}}(t_{i-1})]$
Failed States $P_f(t_{i-1})$=0
DISCRETE
CONTINUOUS
Is the Next Phase Discrete or Continuous?
MISSION SUCCESS PROBABILITY
$=\sum P_{success\ states}(t_m)$
YES
End of Mission?
NO
i -> i+1

Figure 5.9 Algorithm to Demonstrate Minimal Markov and Fault Tree Method

Demonstrating the Minimal Markov model approach, the simple 3-phased mission example defined earlier (Figure 5.5) is again used.

Phase 1

The first phase requires all components that are not discrete phase components and therefore the analysis is the same as in Section 5.2.2. The success probability of phase 1 is evaluated by equation (5.20).

Phase 2

This discrete phase is solved in the same way as Section 5.2.2 to obtain a full solution of all N_S state probabilities (Table 5.1), and calculations of phase (transition) failure (equation (5.9)), and phase success (equation (5.10)). All phase 2 failure states are assigned a final probability of zero for entry to phase 3.

Phase 3

The final phase requires only 2 out of the 4 possible components, A and B. Therefore the full 16 states representing all component combinations can be reduced to a 4 state list shown in Table 5.3.

Full states from Figure 5.6			A	B
$S_1^{(ABCD)}, S_2^{(ABCD)}, S_3^{(ABCD)}, S_4^{(ABCD)}$	$\longrightarrow$	$S_1^{(AB)}$	0	0
$S_5^{(ABCD)}, S_6^{(ABCD)}, S_7^{(ABCD)}, S_8^{(ABCD)}$	$\longrightarrow$	$S_2^{(AB)}$	0	1
$S_9^{(ABCD)}, S_{10}^{(ABCD)}, S_{11}^{(ABCD)}, S_{12}^{(ABCD)}$	$\longrightarrow$	$S_3^{(AB)}$	1	0
$S_{13}^{(ABCD)}, S_{14}^{(ABCD)}, S_{15}^{(ABCD)}, S_{16}^{(ABCD)}$	$\longrightarrow$	$S_4^{(AB)}$	1	1

Table 5.3 Two Component State Table

The full possible 2-component state transition matrix **A** is given by equation (5.26).

$$[\mathrm{A}]=\begin{bmatrix} -\Sigma_1 & \lambda_B & \lambda_A & 0 \\ \upsilon_B & -\Sigma_2 & 0 & \lambda_A \\ \upsilon_A & 0 & -\Sigma_3 & \lambda_B \\ 0 & \upsilon_A & \upsilon_B & -\Sigma_4 \end{bmatrix} \qquad (5.26)$$

Since $S_2^{(AB)}$ - $S_4^{(AB)}$ are failed and thus absorbing states, the state transition matrix for this phase becomes as shown in equation (5.27).

$$[\mathrm{A}]=\begin{bmatrix} -\Sigma_1 & \lambda_A & \lambda_B & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad (5.27)$$

The initial probabilities are calculated by the reduction of the full set of system states to those states required for phase 3. For this phase, the four minimal states $S_1^{(AB)}$ - $S_4^{(AB)}$ would have initial probabilities found by the full N_S state list (Table 5.3) as shown in equations (5.28).

$$P_1^{(AB)}(t_2) = \sum_{j=1}^{\overset{Full\ States}{4}} P_j^{(ABCD)}(t_2) \qquad P_2^{(AB)}(t_2) = \sum_{j=5}^{\overset{Full\ States}{8}} P_j^{(ABCD)}(t_2)$$

$$P_3^{(AB)}(t_2) = \sum_{j=9}^{\overset{Full\ States}{12}} P_j^{(ABCD)}(t_2) \qquad P_4^{(AB)}(t_2) = \sum_{j=13}^{\overset{Full\ States}{16}} P_j^{(ABCD)}(t_2) \tag{5.28}$$

From the simplified component state list (Table 5.3) it may be identified that the states to successfully complete phase 2 are those where either A or B are working, $S_1^{(AB)}$ - $S_3^{(AB)}$. The success state for phase 3 is $S_1^{(AB)}$. Therefore phase 3 transition failure will occur if the system is in states $S_2^{(AB)}$ - $S_3^{(AB)}$, and is given in equation (5.29).

$$Tr(t_2) = \sum_{j=2}^{3} P_j^{(AB)}(t_2) \tag{5.29}$$

Since the success state for phase 3 is $S_1^{(AB)}$, all other states are assigned an initial probability of 0 on entering the phase.

The initial minimal phase state probabilities may be entered into the system of state differential equations (5.2) with transition matrix (5.27) and solved over the duration of phase 3 to calculate the probability of the system residing in each of the 4 possible states at the end of the phase. Phase success would only be found if the system was in state $S_1^{(AB)}$ of Table 5.3 with both components working at the end of the phase in equation (5.30).

$$R(t_3) = P_1^{(AB)}(t_3) \tag{5.30}$$

And thus mission success may be found by equation (5.31).

$$R_{MISS} = P_1^{(AB)}(t_3) \tag{5.31}$$

If subsequent phases were present in the mission, these 4 minimal phase 3 state probabilities would again be expanded to produce a full set of system state probabilities. It is possible to calculate the availability and unavailability of all components not required in the phase using equations (5.15). The probability of the system residing in each of the 4 minimal system states would be multiplied by every possible failure and success combination of all other components at the end of the phase. This produces a full set of system state probabilities at the phase boundary for input to the next phase.

The extra computational effort required in the expansion and reduction of system states between phases is insignificant compared with the considerable reduction of intensive effort required to solve the reduced system state differential equations over a long time period.

5.2.4 Comparison of Results

A general computer program has been developed using C to implement the three methodologies for the phased mission analysis of repairable systems. The problem defined in Figure 5.5 has been analysed by this software.

The components A, B, C and D are each given a failure and repair rate (per hour) as follows:

$$\begin{array}{ll}
\lambda_A = 0.001 & \upsilon_A = 0.02 \\
\lambda_B = 0.0005 & \upsilon_B = 0.001 \\
\lambda_C = 0.0008 & \upsilon_C = 0.04 \\
\lambda_D = 0.002 & \upsilon_D = 0.002
\end{array}$$

The phases are defined to be:

Phase 1	Continuous	100 hour
Phase 2	Discrete	
Phase 3	Continuous	200 hours

The comparison of outputs for phase failure, transition failure and mission success by each of the three methods is given in Table 5.4.

	Full Markov Method	Reduced Markov and FT Method	Minimal Markov and FT Method
Mission Reliability	$6.7709\text{x}10^{-1}$	$6.7707\text{x}10^{-1}$	$6.7705\text{x}10^{-1}$
Phase 1 Unreliability	$1.2523\text{x}10^{-4}$	$1.2522\text{x}10^{-4}$	$1.2521\text{x}10^{-4}$
Phase 2 Unavailability	$8.4371\text{x}10^{-3}$	$8.4353\text{x}10^{-3}$	$8.4353\text{x}10^{-3}$
Phase 3 Unreliability	$2.3668\text{x}10^{-1}$	$2.3666\text{x}10^{-1}$	$2.3666\text{x}10^{-1}$
Phase 2 Transition Failure	$8.4371\text{x}10^{-3}$	$8.4353\text{x}10^{-3}$	$8.4353\text{x}10^{-3}$
Phase 3 Transition Failure	$7.7732\text{x}10^{-2}$	$7.7725\text{x}10^{-2}$	$7.7725\text{x}10^{-2}$

Table 5.4 Comparison of Mission Reliability Data for Three Methods

It can be seen that all methods produce consistent results for the test problem. The differences in part will be due to the errors in the numerical solution routine for the differential equation using time increments of Δt=0.05s. In this small problem, the gains in efficiency cannot be demonstrated. However for large, real systems, problems this can reasonably be expected to be significant.

5.2.4.1 Further Example

To test this method more fully and justify the generality of the methods, a mission consisting of an increased number of phases and components may be considered in Figure 5.10.

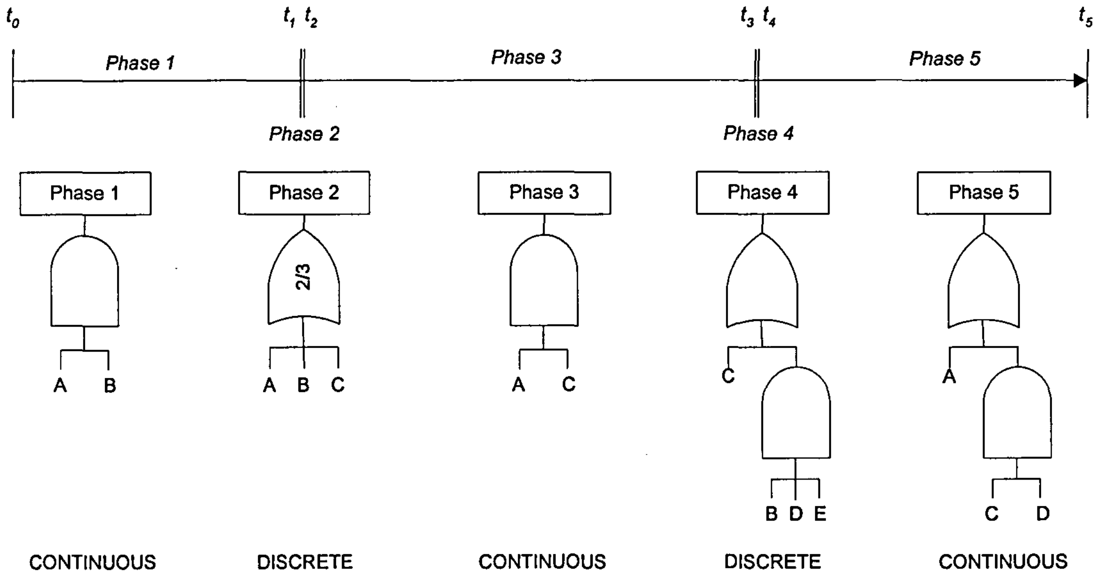


Figure 5.10 Further Example

The component usage may be summarised as follows:

Component	Phases Required	Failure Rate (per hour)	Repair Rate (per hour)
A	1, 2, 3, 5	0.0001	0.02
B	1, 2, 4	0.00005	0.001
C	2, 3, 4, 5	0.00008	0.04
D	4, 5	0.0002	0.002
E	4	0.0005	0.005

Phase 1 :	Continuous	100.0 Hour
Phase 2 :	Discrete	
Phase 3 :	Continuous	200.0 Hours
Phase 4:	Discrete	
Phase 5:	Continuous	100.0 Hour

The phase results by each method are given in Table 5.5.

	Full Markov Method	Reduced Markov and FT Method	Minimal Markov and FT Method
Mission Reliability	9.8201x10^{-1}	9.8194x10^{-1}	9.8283x10^{-1}
Phase 1 Unreliability	3.8140x10^{-5}	3.8135x10^{-5}	3.8132x10^{-5}
Phase 2 Unavailability	1.7633x10^{-5}	1.7631x10^{-5}	1.7629x10^{-5}
Phase 3 Unreliability	1.1591x10^{-4}	1.1590x10^{-4}	1.1596x10^{-4}
Phase 4 Unavailability	2.0213x10^{-3}	2.0213x10^{-3}	2.0223x10^{-3}
Phase 5 Unreliability	1.0274x10^{-2}	1.0272x10^{-2}	1.0282x10^{-2}
Phase 2 Transition Failure	1.7633x10^{-5}	1.7631x10^{-5}	1.7629x10^{-5}
Phase 3 Transition Failure	0	0	0
Phase 4 Transition Failure	2.0213x10^{-3}	2.0213x10^{-3}	2.0223x10^{-3}
Phase 5 Transition Failure	4.9308x10^{-3}	4.9311x10^{-3}	4.9340x10^{-3}
Time Taken to Process Results (*s*)	45.0	6.0	4.0

Table 5.5 Comparison of Mission Reliability Data for Three Methods

The minimal method is found to vastly reduce computational time whilst producing consistent results to the other methods using time increments of Δt=0.05s in the numerical solution routine for the differential equations. This minimal method greatly reduces the time required to perform reliability calculations on a phased mission compared to the full Markov solution implemented in the past.

5.3 Reliability of a Mission with Non-Repairable Continuous Phases

So far only missions comprising of repairable continuous phases and instantaneous discrete phases have been considered. Another possibility is that maintenance may not be allowed for certain periods of time throughout a mission. For such a continuous phase the components would be classed as non-repairable.

The proposed methods in the previous sections allowed the application of fault tree methods to discrete phases to obtain the minimal cut sets for the phase and thus establish working and failed phase states. However, as no state changes were possible at this discrete phase, state probabilities remained the same once transition from the previous phase had been completed.

The introduction of missions that comprise of both non-repairable and repairable continuous phases means that the methods presented in Sections 4.2.3 and 5.2.3 to model the failure of a component over a continuous phase cannot be implemented. Component failure probability distributions are not consistent throughout the duration of the mission, and must be modelled separately for each phase. Methods are presented to calculate the probability that a component resides in a working or failed state at the end of a repairable or non-repairable continuous phase in Sections 5.3.1 and 5.3.2. A technique is presented for solution of missions comprising of both non-repairable and repairable continuous phases in Section 5.3.3.

5.3.1 Component Failure Probability Over a Non-Repairable Phase

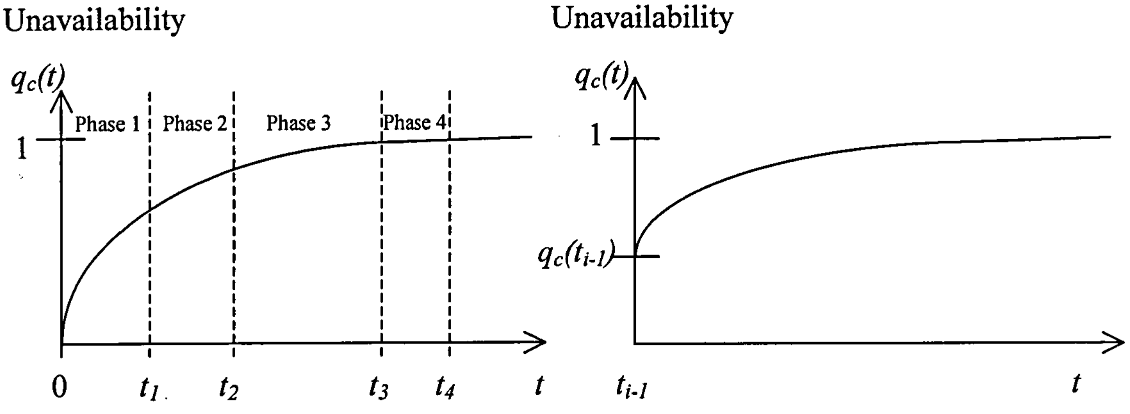
The probability density function of a component *c* in a non-repairable mission is found by the negative exponential distribution given in equation (5.32).

$$f(t) = \lambda_c e^{-\lambda_c t} \qquad \text{for } t>0 \qquad (5.32)$$

The unavailability of the component, $q_c(t)$, with time over the mission duration is modelled by the cumulative probability function $F_c\ (t)$ in equation (5.33).

$$q_c(t) = F_c(t) = \int_0^t f_c(t)\,dt = \left[-e^{-\lambda_c t}\right]_0^t = 1 - e^{-\lambda_c t} \qquad (5.33)$$

In the case of a completely non-repairable mission (Chapter 4), the failure distribution of all components remains constant throughout the mission. The unavailability of a component c over the duration of the mission would be modelled as shown in Figure 5.11(a), and for each separate phase in 5.11(b).



(a) Over the Mission

(b) During Phase *i*

Figure 5.11 Unavailability of a Non-Repairable Component

The unavailability of the component over phase i would be derived in a similar way to equation (5.33) by integration of the probability density function (equation (5.32)). The integration time limits for phase i would be $t=t_{i-1}$ to $t=t_i$ in equation (5.34).

$$q_{c_i} = \int_{t_{i-1}}^{t_i} f_c(t)\,dt = \left[-e^{-\lambda_c t}\right]_{t_{i-1}}^{t_i} = e^{-\lambda_c t_{i-1}} - e^{-\lambda_c t_i} \qquad (5.34)$$

For sequences of repairable and non-repairable phases, the unavailability of a component over a non-repairable phase becomes more complex. The cumulative probability function cannot be represented as in equation (5.33) since this implies that the negative exponential distribution is continuous from $t=0$ to $t=t_m$ and that the initial component c unavailability, $q_c(t_{i-1})$, in any non-repairable phase i of a multi-phased mission is found by equation (5.35).

$$q_c(t_{i-1}) = 1 - e^{-\lambda_c t_{i-1}} \qquad (5.35)$$

Each non-repairable phase following any sequence of repairable and non-repairable phases will have a different negative exponential distribution dependent on the probability of the component being in the failed state at the start of the phase. The distribution of a non-repairable component unavailability can be obtained by Laplace transforms (Section 2.4.2.1). The Laplace transform of a single component unavailability (equation (2.47)) with initial failure probability $q_c(0)$ at t=0 is given in equation (5.36).

$$sq_c(s) - q_c(0) = \frac{\lambda_c}{s} - \lambda_c q_c(s)$$

$$(s+\lambda_c)q_c(s) = \frac{\lambda_c}{s} + q_c(0)$$

$$q_c(s) = \frac{\lambda_c}{s(s+\lambda_c)} + \frac{q_c(0)}{s+\lambda_c}$$

$$q_c(s) = \frac{1}{s} - \frac{(1-q_c(0))}{s+\lambda_c}$$

$$q_c(s) = \frac{1}{s} - \frac{a_c(0)}{s+\lambda_c} \tag{5.36}$$

The inverse of equation (5.36) gives the appropriate exponential distribution with time t in equation (5.37).

$$q_c(t) = 1 - a_c(0)e^{-\lambda_c t} \tag{5.37}$$

where t is measured from the start of the mission

Since we require the unavailability of the component over phase i, the initial failure probability of component c at t=t_{i-1} is $q_c(t_{i-1})$, and t must be replaced by t-t_{i-1} as shown in equation (5.38).

$$q_c(t) = 1 - a_c(t_{i-1})e^{-\lambda_c(t-t_{i-1})} \quad \text{for } t=t_{i-1} \text{ to } t=t_i \tag{5.38}$$

The probability that the component is in the failed state at the end of phase i can be found by solution of equation (5.38) at t=t_i in equation (5.39)

$$q_c(t_i) = 1 - a_c(t_{i-1})e^{-\lambda_c(t_i-t_{i-1})} \tag{5.39}$$

The probability of component *c* failure during this non-repairable phase is then evaluated as the difference in unavailability between the start of the phase ($t=t_{i-1}$) and the end of the phase ($t=t_i$) in equation (5.40).

$$\begin{aligned} q_{c_i} &= \left(1-a_c(t_{i-1})e^{-\lambda_c(t_i-t_{i-1})}\right)-\left(1-a_c(t_{i-1})e^{-\lambda_c(t_{i-1}-t_{i-1})}\right) \\ &= \left(1-a_c(t_{i-1})e^{-\lambda_c(t_i-t_{i-1})}\right)-\left(1-a_c(t_{i-1})\right) \\ &= a_c(t_{i-1})\left(1-e^{-\lambda_c(t_i-t_{i-1})}\right) \end{aligned} \tag{5.40}$$

The initial component *c* availability in phase *i*, $a_c(t_{i-1})$, is obtained directly from the previous phase and will be dependent on the nature of phase *i*-1.

5.3.2 Component Failure Probability Over a Repairable Phase

The solution to a repairable phase is achieved by the Markov method. If a component *c* is required for successful system operation in a repairable phase, the final component availability would be derived from the Markov state model. The probability that the component is in the working or failed state at the end of the phase *i* is found by the sum of all Markov states with contribution from the component working or failed respectively in equations (5.41).

$$a_c(t_i)=\sum_{\substack{j\ \text{states with} \\ c\ \text{working}}} P_j(t_i) \qquad\qquad q_c(t_i)=\sum_{\substack{k\ \text{states with} \\ c\ \text{failed}}} P_k(t_i) \tag{5.41}$$

If the component is not required during the repairable phase, the final component availability must be obtained using alternative methods. The unavailability of a component not required in a repairable single phase mission is given in equation (2.56). For missions of multiple phases, this equation cannot be used since it implies the exponential distribution is continuous from $t=0$ to $t=t_m$ and the initial component *c* unavailability, $q_c(t_{i-1})$, in any phase *i* of a multi-phased mission is found by equation (5.42).

$$q_c(t_{i-1})=\frac{\lambda_c}{\lambda_c+\upsilon_c}\left(1-e^{-(\lambda_c+\upsilon_c)t_{i-1}}\right) \tag{5.42}$$

The probability that a component will fail during a repairable phase given any initial value of unavailability is required. This is modelled in Figure 5.12.

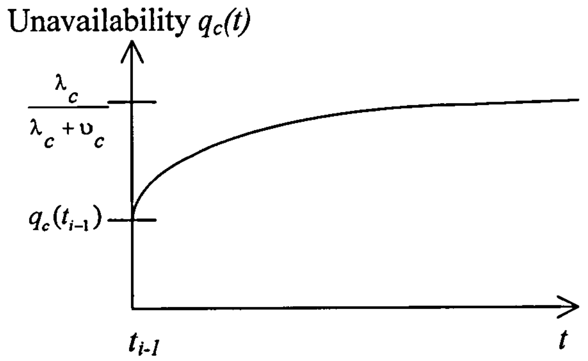


Figure 5.12 Unavailability of a Discrete Phase Component During Continuous Phase *i*

In the same way as for a component over a non-repairable phase, the exponential unavailability model must be derived using Laplace transforms. The Laplace transform for the unavailability of a single repairable component (equation (2.54)) is given in equation (5.43).

$$q_c(s)=\frac{\lambda_c}{\lambda_c+\upsilon_c}\left[\frac{a_c(0)+q_c(0)}{s}\right]+\frac{1}{\lambda_c+\upsilon_c}\cdot\frac{1}{s+\lambda_c+\upsilon_c}\left[\upsilon_c q_c(0)-\lambda_c a_c(0)\right] \quad (5.43)$$

This function is inverted at $t=t_{i-1}$ in equation (5.44).

$$q_c(t)=\frac{\lambda_c}{\lambda_c+\upsilon_c}\left[a_c(t_{i-1})+q_c(t_{i-1})\right]+\frac{e^{-(\lambda_c+\upsilon_c)(t-t_{i-1})}}{\lambda_c+\upsilon_c}\left[\upsilon_c q_c(t_{i-1})-\lambda_c a_c(t_{i-1})\right] \quad (5.44)$$

Since $a_c(t_{i-1})+q_c(t_{i-1})=1$, the distribution of unavailability of the component becomes as given in equation (5.45).

$$q_c(t)=\frac{\lambda_c}{\lambda_c+\upsilon_c}+\frac{e^{-(\lambda_c+\upsilon_c)(t-t_{i-1})}}{\lambda_c+\upsilon_c}\left[\upsilon_c q_c(t_{i-1})-\lambda_c a_c(t_{i-1})\right] \quad \text{for } t=t_{i-1} \text{ to } t=t_i \quad (5.45)$$

The probability that the component is in the failed state and success states at the end of phase *i* is found by equations (5.46) and (5.47) respectively.

$$q_c(t_i)=\frac{\lambda_c}{\lambda_c+\upsilon_c}+\frac{e^{-(\lambda_c+\upsilon_c)(t_i-t_{i-1})}}{\lambda_c+\upsilon_c}\left[\upsilon_c q_c(t_{i-1})-\lambda_c a_c(t_{i-1})\right] \quad (5.46)$$

$$a_c(t_i)=\frac{\upsilon_c}{\lambda_c+\upsilon_c}+\frac{e^{-(\lambda_c+\upsilon_c)(t_i-t_{i-1})}}{\lambda_c+\upsilon_c}\left[\lambda_c a_c(t_{i-1})-\upsilon_c q_c(t_{i-1})\right] \quad (5.47)$$

The initial component availability, $a_c(t_{i-1})$ and unavailability, $q_c(t_{i-1})$, in phase i is obtained directly from the previous phase and will be dependent on the nature of phase i-1.

5.3.3 Combined Minimal Markov and Continuous Phase Fault Tree Method

It may be possible to reduce the Markov models further where non-repairable continuous phases are encountered if the failure of the continuous non-repairable phase can also be modelled using a fault tree. It is possible to use the previously described Markov based methods with repair rates set to zero in non-repairable phases. However there would be processing advantages if the results can be accomplished using smaller models.

To demonstrate a method which can accomplish the analysis of such systems, an adaptation of the example given in Figure 5.5 will be used, shown in Figure 5.13.

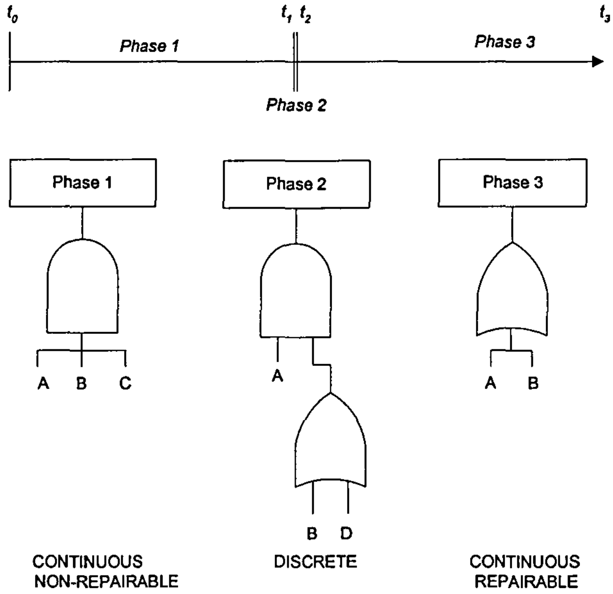


Figure 5.13 Discrete and Continuous Phased Mission with Repairable and Non-Repairable Phases

The probability of a component residing in the working or failed state at the start of a non-repairable phase i is obtained from the solution of the previous phase. If the previous phase was non-repairable, this would be determined using the method presented in Section 5.3.1 (equation (5.39)). If the previous phase was repairable, this would be obtained using either of the techniques demonstrated in Section 5.3.2 (equation (5.41) or (5.46)). In the example given in Figure 5.13, the non-repairable continuous phase is phase 1, and the system will start at t_0 with all components working. If the non-repairable phase were to come later in the mission then failures could exist at the start of the phase.

Qualitative analysis can be implemented to determine the minimal cut sets of a non-repairable continuous phase i. If the initial availability of each component c is known, the probability that component c fails during phase i can be obtained using equation (5.40). The failure probability of phase i, Q_i, can then easily be obtained using a simple inclusion-exclusion expansion of the probability of existence of phase i cut sets in equation (5.48).

$$Q_i = \sum_{j=1}^{N_{mcs_i}} P(C_{j_i}) - \sum_{j=2}^{N_{mcs_i}} \sum_{k=1}^{j-1} P(C_{j_i} \cap C_{k_i}) + \cdots + (-1)^{N_{mcs_i}-1} P(C_{1_i} \cap C_{2_i} \cap \cdots \cap C_{N_{mcs_i}}) \qquad (5.48)$$

where N_{mcs_i} is the number of minimal cut sets in phase i

The probability that each component is in the failed or working state at the end of non-repairable continuous phase i is obtained using equation (5.39). This is passed directly to the next phase which will be solved depending on the type of phase i+1:

- Phase i+1 Continuous and Non-Repairable

  The state probabilities for each component can be passed directly to phase i+1, which will be solved in the same way.

- Phase i+1 Discrete

  The state probabilities for each component can be passed directly to phase i+1. The probability of the discrete phase failure is obtained by the inclusion-exclusion expansion of the existence of phase i+1 cut sets (that did not cause phase i failure) at the end of phase i.

- Phase i+1 Continuous and Repairable

  The component state probabilities must be transformed to the required vector of initial system state probabilities for solution of the phase i+1 Markov model. This is achieved by the combination of the relevant final component state probabilities.

This method can be applied to the example in Figure 5.13 in the following way:

Phase 1

The first phase of the mission is non-repairable and all components are assumed to begin phase 1 in the working state, i.e. $q_c(0)=0$ for all c. There is only one minimal cut set in this initial phase, {A$_1$, B$_1$, C$_1$}, and so the phase 1 failure and success probabilities are obtained using equation (5.48) in equation (5.49).

$$Q_1 = q_{A_1} q_{B_1} q_{C_1} \qquad A_1 = 1 - q_{A_1} q_{B_1} q_{C_1} \tag{5.49}$$

where q_{c_1} for each component c is obtained using equation (5.40)

The final phase 1 component state probabilities are obtained using equation (5.39), and are given in equations (5.50).

$$q_A(t_1) = 1 - e^{-\lambda_A t_1} \qquad q_B(t_1) = 1 - e^{-\lambda_B t_1} \qquad q_C(t_1) = 1 - e^{-\lambda_C t_1} \tag{5.50}$$

Phase 2

The second phase of the mission is of a discrete nature. The minimal cut sets for this phase are C$_1$={A, B} and C$_2$={A, D}. If either minimal cut set exists at the end of phase 1, system failure will occur on transition to phase 2. The probability that a phase 2 minimal cut set exists at the end of phase 1 is obtained using the inclusion-exclusion expansion (equation (5.48)) of the existence of phase 2 cut sets at $t=t_1$ in equation (5.51).

$$Q_2 = q_{C_1}(t_1) + q_{C_2}(t_1) - q_{C_1} q_{C_2}(t_1)$$

$$Q_2 = q_A(t_1)q_B(t_1) + q_A(t_1)q_D(t_1) - q_A(t_1)q_B(t_1)q_D(t_1) \tag{5.54}$$

and $$A_2 = 1 - \left(q_A(t_1)q_B(t_1) + q_A(t_1)q_D(t_1) - q_A(t_1)q_B(t_1)q_D(t_1)\right)$$

The final component state probabilities at the end of phase 2 can then be passed directly to phase 3.

Phase 3

The Markov model for phase 3 requires the initial state probability vector determined by components A and B. This would be obtained by the component state probabilities at the end of the discrete phase 2 as demonstrated in Table 5.6.

State Ref	A	B	Initial Phase 3 State Probability
$S_1^{(AB)}$	0	0	$a_A(t_2)\cdot a_B(t_2)$
$S_2^{(AB)}$	0	1	$a_A(t_2)\cdot q_B(t_2)$
$S_3^{(AB)}$	1	0	$q_A(t_2)\cdot a_B(t_2)$
$S_4^{(AB)}$	1	1	$q_A(t_2)\cdot q_B(t_2)$

Table 5. 6 Initial State Probabilities of Repairable Phase 3 from Discrete Phase 2

However, since the event of components A and B both residing in the failed state at the discrete second phase would have caused phase 2 failure, it is not possible for the system to begin phase 3 in state $S_4^{(AB)}$. This is assigned a state probability of zero at the start of phase 3.

The phase 3 transition failure is determined by the event that either of components A or B are failed at the start of phase 3 using equation (5.29). The phase 3 Markov model is again defined by the transition model given in equation (5.27). Phase 3 success is found by the probability that the system resides in state $S_1^{(AB)}$ at the end of the mission in equation (5.30), and the mission success is obtained using equation (5.31).

Using this method, it is possible for repairable and non-repairable continuous phases to be solved separately. Each non-repairable phase can be solved using standard fault tree techniques, and each repairable phase can be solved by application of a Markov model. The expansion of the state probabilities at the end of each phase allows the unavailability or availability of all components to be calculated for transition to the next phase. The failure probability of an irrelevant component over a non-repairable or repairable phase can easily be obtained using the methods presented in Sections 5.3.1 and 5.3.2.

5.3.4 Comparison of Results

Using the same component and phase data as in Section 5.2.4, the 3-phased mission example given in Figure 5.13 may be solved using a full Markov model, and also using the proposed combined minimal Markov model with continuous phase fault tree method. The phase and transition failure probabilities and mission success probability for each method are compared in Table 5.7 using a time increment value of Δt=0.05s for the minimal solution routine for the differential equation. It can be seen that using the combined minimal Markov and continuous phase fault tree technique produces a very close agreement to that found by the full Markov method.

	Full Markov Method	Combined Minimal Markov and Continuous Phase Fault Tree Method
Mission Reliability	$6.3793\text{x}10^{-1}$	$6.3777\text{x}10^{-1}$
Phase 1 Unreliability	$3.5691\text{x}10^{-4}$	$3.5683\text{x}10^{-4}$
Phase 2 Unreliability	$2.0697\text{x}10^{-2}$	$2.0693\text{x}10^{-2}$
Phase 3 Unreliability	$2.2299\text{x}10^{-1}$	$2.2294\text{x}10^{-1}$
Phase 2 Transition Failure	$2.0697\text{x}10^{-2}$	$2.0693\text{x}10^{-2}$
Phase 3 Transition Failure	$1.1832\text{x}10^{-1}$	$1.1824\text{x}10^{-1}$

Table 5.7 Comparison of Mission Reliability Data for Two Methods

To gain confidence in this methodology and its computer implementation, the method has been applied to the example considered before in Section 5.2.4.1. In this analysis all phases are considered repairable apart from phase 3 and a time step value of Δt=0.05s is used for the minimal solution routine for the differential equation. The results presented in Table 5.8 were obtained. A second model analysis was then performed for the same example with different repairable and non-repairable phases. Results from this further example where phases 1 and 5 were assumed non-repairable with all other phases repairable are given in Table 5.9.

Close agreement between the methods is again evident. The updated method of dealing with non-repairable phases gives faster processing times and offers a significant advantage. It is reasonable to expect that this would be even more dramatic for larger system problems.

Phase 3 Non-Repairable

	Full Markov Method	Combined Minimal Markov and Continuous Phase Fault Tree Method
Mission Reliability	$9.4861\text{x}10^{-1}$	$9.4829\text{x}10^{-1}$
Phase 1 Unreliability	$3.8140\text{x}10^{-5}$	$3.8136\text{x}10^{-5}$
Phase 2 Unreliability	$1.7633\text{x}10^{-5}$	$1.7630\text{x}10^{-5}$
Phase 3 Unreliability	$4.1806\text{x}10^{-4}$	$4.1858\text{x}10^{-4}$
Phase 4 Unreliability	$1.7454\text{x}10^{-2}$	$1.7464\text{x}10^{-2}$
Phase 5 Unreliability	$1.0007\text{x}10^{-2}$	$1.0003\text{x}10^{-2}$
Phase 2 Transition Failure	$1.7633\text{x}10^{-5}$	$1.7630\text{x}10^{-5}$
Phase 3 Transition Failure	0	0
Phase 4 Transition Failure	$1.7454\text{x}10^{-2}$	$1.7464\text{x}10^{-2}$
Phase 5 Transition Failure	$2.3554\text{x}10^{-2}$	$2.3567\text{x}10^{-2}$
Time Taken to Process Results (s)	38.0	1.0

Table 5.8 Comparison of Further Mission Reliability Data for Two Methods

Phase 1,5 Non-Repairable

	Full Markov Method	Combined Minimal Markov and Continuous Phase Fault Tree Method
Mission Reliability	$9.8268\text{x}10^{-1}$	$9.8256\text{x}10^{-1}$
Phase 1 Unreliability	$4.9644\text{x}10^{-5}$	$4.9627\text{x}10^{-5}$
Phase 2 Unreliability	$1.1827\text{x}10^{-4}$	$1.1823\text{x}10^{-4}$
Phase 3 Unreliability	$1.5214\text{x}10^{-4}$	$1.5213\text{x}10^{-4}$
Phase 4 Unreliability	$2.0280\text{x}10^{-3}$	$2.0240\text{x}10^{-3}$
Phase 5 Unreliability	$1.0372\text{x}10^{-2}$	$1.0280\text{x}10^{-2}$
Phase 2 Transition Failure	$1.1827\text{x}10^{-4}$	$1.1823\text{x}10^{-4}$
Phase 3 Transition Failure	0	0
Phase 4 Transition Failure	$2.0280\text{x}10^{-3}$	$2.0240\text{x}10^{-3}$
Phase 5 Transition Failure	$5.0312\text{x}10^{-3}$	$5.0305\text{x}10^{-3}$
Time Taken to Process Results (s)	40.0	1.0

Table 5.9 Comparison of Further Mission Reliability Data for Two Methods

5.4 Summary

The methods presented in this chapter allow solution of a mission that is capable of repair in some or all phases. The inclusion of both discrete and continuous phase models many practical situations where a system is required to work on demand. A non-repairable phase can be solved using standard fault tree techniques, and a repairable phase can be solved by application of a minimal Markov model. The expansion of the state probabilities at the end of each phase allows the unavailability or availability of all components to be calculated for transition to the next phase, and thus any sequence of repairable and non-repairable phases can be modelled.

The main deficiency of this model is that dependencies between components have not been considered. Methods to account for dependencies such as sequential failures and maintenance policies are presented in the following chapters.

Chapter 6 Sequential Failures

6.1 Introduction

In some situations, the top event of a fault tree can only be caused by a sequence of basic event occurrences, thus the order in which components fail will be of importance to the system outcome. This concept of sequential failures was introduced in Section 2.2.3.5.3.

An example of a situation where the system outcome is dependent on the failure ordering of components is a safety protection system designed to protect against a specific hazard (Figure 2.3). If the hazardous event occurs while safety protection devices are functioning, the top event will not occur and a shutdown would be instigated. If the hazardous event occurs while safety protection devices are not working a more catastrophic system level failure will occur. In this type of situation, failed safety features are known as enabling events. The occurrence of the hazardous event is known as an initiator. In a system, an initiator may act as either an enabler or an initiator, whereas an enabler can only act in this capacity. Every minimal cut set of the system requires at least one initiator in order to cause system failure.

A limited ordering requirement is introduced on the basic events. The last event to occur needs to be the hazardous one. If the safety features have failed in any order prior to this then the system failure represented by the fault tree will occur.

6.1.1 Failure Modes

A system may fail through a number of different causes. The order in which components fail in a system may contribute to different outcomes (failed system states), and the outcomes are defined as *failure modes*. The failure modes of the safety system example given in Figure 2.3 could be classified as 'Safe System Shutdown' and 'Catastrophic System Failure'. A safe system shutdown will happen if the initiating event occurs while an enabling event does not exist, whereas a catastrophic failure will be caused if the initiating event occurs when all the enabling events already exist. Both cause the system to cease functioning, however the consequences of catastrophic system failure would be far more serious than a safe system shutdown.

Fault tree representation allows the logical development of each failure mode individually in an inverted tree structure, however this method is not appropriate to accurately account for the dynamic relationship between component failures.

Consider all possible component failure orderings which can be demonstrated using a tree structure. The component failure events are considered in every possible order to determine the maximum number of system states possible and the appropriate system outcome noted. However in a practical situation once a catastrophic system failure state is reached, the system resides in an absorbing failed state and further component failures are irrelevant. Take the example shown in Figure 2.3, considering only two component level events. One is the enabler (E), the second the initiator (I), then all sequences may be represented as given in Figure 6.1:

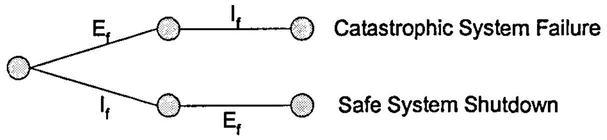


Figure 6.1 Failure Event Tree

Each system outcome may have a different consequence. A safe system shutdown would allow defective items to be repaired to good as new condition and the system would be restored to full working order. In the event of a catastrophic failure maintenance may not be possible, further complications may be caused, and if the reliability of the system is to be modelled it would be considered to reside in an absorbing failed state.

For a system where the order of component failures can result in a different system state outcome, it is important to be able to identify the outcomes to ensure that adequate protection is provided in a system.

6.2 Reliability of a System with Sequential Failures

Two methods are considered by which the reliability of a system involving sequential failures can be calculated:

6.2.1 Fault Tree Method

A logic gate has been developed whereby the gate outcome depends on the order in which the events occur. This gate is defined as a *priority-AND* gate and is represented in Figure 6.2.

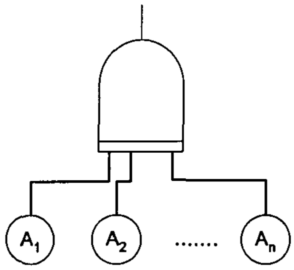


Figure 6.2 Priority-AND gate

The events must occur in the order A_1, $A_2 \ldots A_n$ for the output of the gate to be true. If the events occur in any other sequence to this, the gate output will be false.

Gates such as this where the order of component failure is important are classed as *dynamic* gates. Other non-sequential tree structuring such as AND and OR gates are classed as *static* gates. Methods have been developed to calculate the reliability of static fault tree structures [3], however to perform analysis on a dynamic gate type it is necessary to develop further methods. The Markov method is suitable for dynamic fault tree analysis.

6.2.2 Markov Method

The Markov method models the possible system states and transitions to allow the reliability of a system to be calculated over a duration of time. In order to model the distinction between initiating and enabling events requires the event ordering to be considered and increases the number of possible system states in the model.

In previous Markov models developed, the states in the model took no account of the order of failure. Thus without the distinction between initiating and enabling events, a 2-component parallel system Markov model for system unreliability would be represented by Figure 6.3.

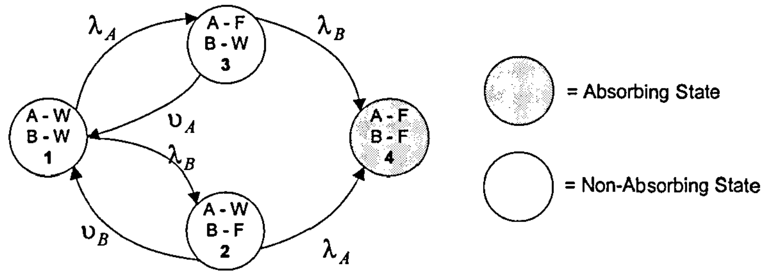


Figure 6.3 2-Component Markov Model

If both components A and B fail, the system will reside in the absorbing state **4**. However this state does not account for the order in which the components have failed. If component B can only cause system failure when component A is down, component A failure is the enabling event and component B failure is the initiating event. The Markov model for this situation would be given in Figure 6.4.

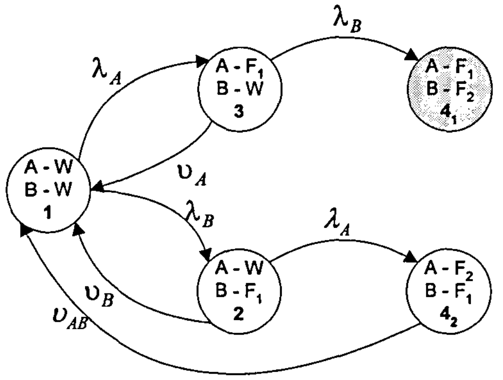
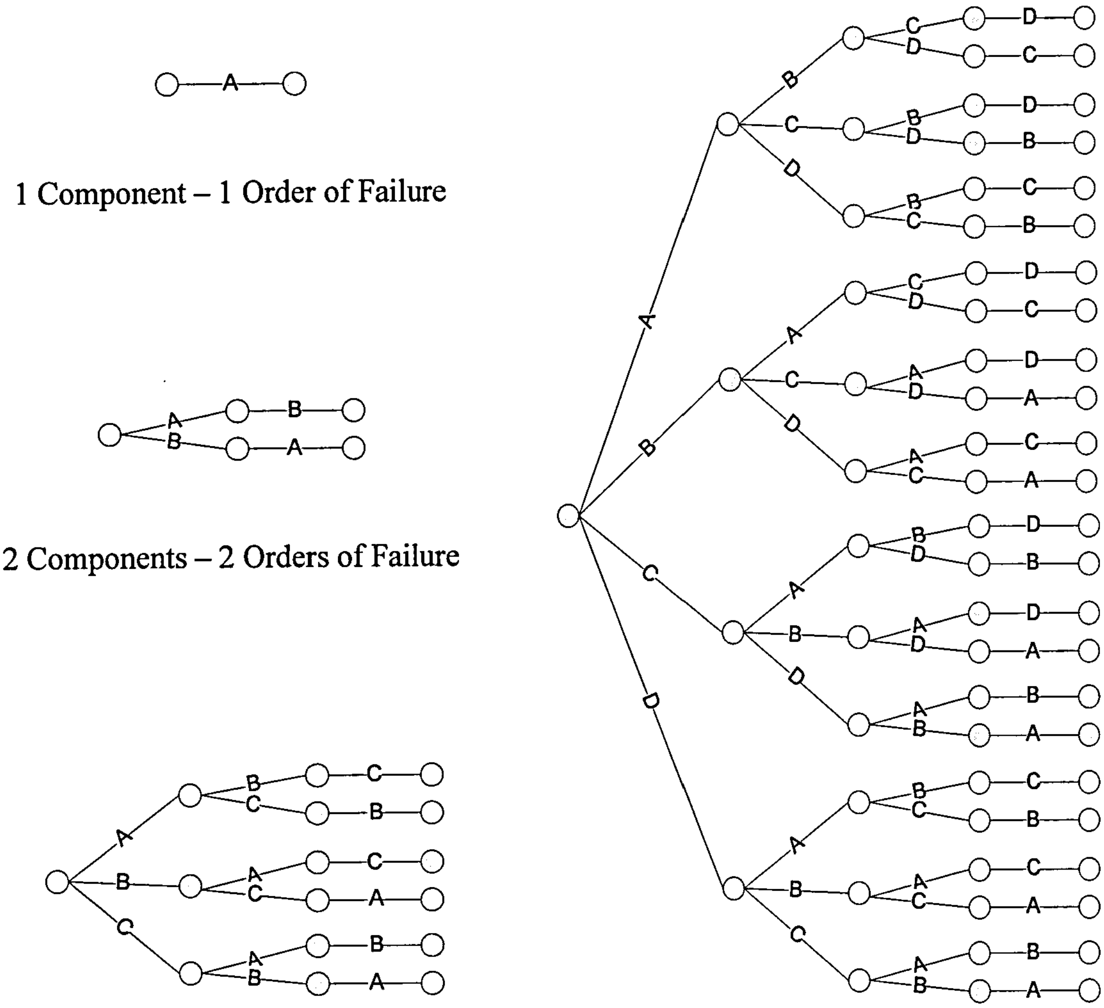


Figure 6.4 2-Component Markov Model with Initiating and Enabling Events

Since the order of component failures is important, states that involve more than one component failure must be expanded to denote the sequence of event occurrence. Where originally state **4** in Figure 6.3 represented both components residing in the failed state, the Markov diagram is now expanded to allow for all possible failure sequences, given by states $\mathbf{4_1}$ and $\mathbf{4_2}$. The two failure sequences result in a different type of system failure. State $\mathbf{4_1}$ leads to catastrophic system failure – failure of component A enables failure of component B to cause system failure. This state is absorbing and thus the system remains in the failed state. State $\mathbf{4_2}$ does not result in a catastrophic system failure. The system would be safely shut down and both the components could be restored to the new condition with repair rate v_{AB}. This would bring the system back into state **1** with all components functioning successfully, and allow the phase to continue.

As the number of components increases, the number of possible orders of component failure increases rapidly. This may be demonstrated in Figure 6.5 for systems comprising of 1, 2, 3 and 4 components using a tree structure.



1 Component – 1 Order of Failure

2 Components – 2 Orders of Failure

3 Components – 6 Orders of Failure

4 Components – 24 Orders of Failure

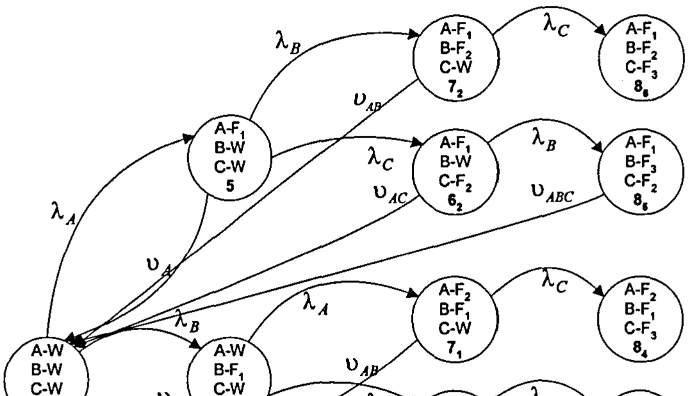
Figure 6.5 Failure Order Combinations for Different Numbers of Components

The development of a Markov model allowing for sequential failures results in an increase of possible system states. For 2 components a full Markov model requires only one extra state, however as the number of components increases the number of possible Markov system states shows a dramatic explosion (Table 6.1).

No. Of Components	Number Of Markov System States	
	Without Sequential Failures	With Sequential Failures
1	2	2
2	4	5
3	8	16
4	16	65
5	32	326

Table 6.1 Number of States in a Markov Model With Sequential Failures

Since the order of occurrence of the enablers does not matter and it is only the initiator that has to be the last to occur it is possible to reduce the number of states. For example in a system comprising of three components in parallel, if the failure of components A and B are enabling events and the failure of component C is an initiating event, a full Markov model would be represented by Figure 6.6.



A-W B-W C-W 1
A-W B-W C-F$_1$ 2
A-W B-F$_1$ C-W 3
A-W B-F$_1$ C-F$_2$ 4$_2$
A-W B-F$_2$ C-F$_1$ 4$_1$
A-F$_1$ B-W C-W 5
A-F$_1$ B-W C-F$_2$ 6$_2$
A-F$_2$ B-W C-F$_1$ 6$_1$
A-F$_1$ B-F$_2$ C-W 7$_2$
A-F$_2$ B-F$_1$ C-W 7$_1$
A-F$_1$ B-F$_2$ C-F$_3$ 8$_6$
A-F$_1$ B-F$_3$ C-F$_2$ 8$_5$
A-F$_2$ B-F$_1$ C-F$_3$ 8$_4$
A-F$_3$ B-F$_1$ C-F$_2$ 8$_3$
A-F$_3$ B-F$_2$ C-F$_1$ 8$_1$
A-F$_2$ B-F$_3$ C-F$_1$ 8$_2$
λ_A
λ_B
λ_C
υ_A
υ_B
υ_C
υ_{AB}
υ_{AC}
υ_{BC}
υ_{ABC}

Figure 6.6 Full Markov Model for Cut Set *ABC*

Catastrophic system failure will occur if the enabling events, components A and B fail, before the failure of component C. A non-catastrophic failure will occur if the components fail in any other order. Therefore the only concern is the order of failure for component C. It is possible to combine the failure states in the model; the absorbing failure states $\mathbf{8}_4$ and $\mathbf{8}_6$ represent a catastrophic failure and are combined to form state $\mathbf{8}_{4,6}$, the non-catastrophic failure states $\mathbf{8}_1$, $\mathbf{8}_2$, $\mathbf{8}_3$, and $\mathbf{8}_5$ can be combined to form state $\mathbf{8}_{1,2,3,5}$. Similarly since catastrophic failure will only occur if components A and B fail first in any order, states $\mathbf{7}_1$, and $\mathbf{7}_2$ can be combined to form state $\mathbf{7}_{1,2}$. Non-catastrophic failure will occur if the initiating event of component C failure occurs before either of the enabling events, and so states $\mathbf{4}_1$ and $\mathbf{4}_2$ can be combined to form state $\mathbf{4}_{1,2}$, and $\mathbf{6}_1$, and $\mathbf{6}_2$ can be combined to form state $\mathbf{6}_{1,2}$. The reduced Markov model is given in Figure 6.7.

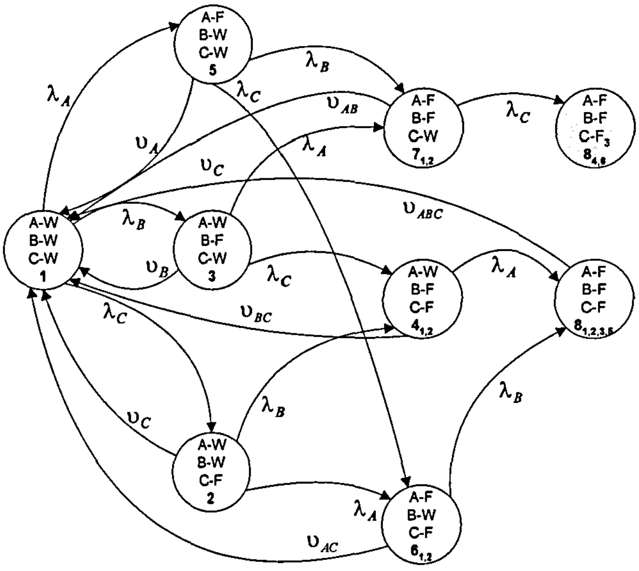


Figure 6.7 Reduced Markov Model for Cut Set *ABC*

This state reduction technique becomes more complex when applied to phased mission systems and will be discussed later.

6.3 Initiating and Enabling Events in Phased Mission Systems

To apply enabler and initiator theory to multi-phased missions there is the possibility that a component is not required during certain phases of the mission. In any phase, the events may be divided into categories:

- Enabler – will only allow initiating events to cause the top event to occur, cannot cause direct phase failure. An enabling event failure may occur in any phase prior to the occurrence of an initiating event.

- Initiator –Upon failure, if enablers are failed then phase failure will occur, otherwise maintenance may be performed to restore all components to full working order. It is also possible for an initiator to act as an enabler for other initiators if they both occur in the same minimal cut set.

- Not Required – The component is not required for the particular phase, but may have been used previously and may be required in future phase configurations. That is to say the system state is not dependent on these component failure modes in this phase.

When considering phased missions it is possible that a component may change function through different phases. A simple example of a road sign illumination system may be used to demonstrate this, shown in Figure 6.8.

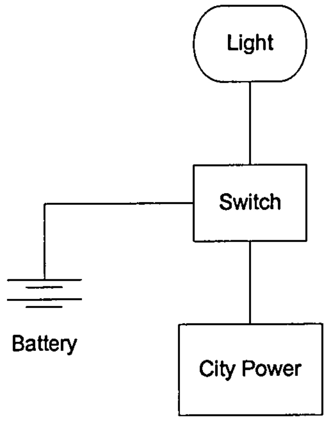


Figure 6.8 Power Source System

In the first phase the light is required to work continuously to illuminate a road sign for motorists. The light is powered by the city power supply, however in the event of a power failure the switch will transfer over to the backup battery. After a specified period of operation the bulb must be replaced and so the second phase requires disconnection of the light from the power supply in order for the bulb to be changed safely. The failure events in this system are given as:

L	-	Bulb Failure
P	-	City Power Supply Failure
B	-	Battery Failure
S_i	-	Switch Control Fails to Isolate Power Source
S_b	-	Switch Control Fails to Transfer to Backup Source

Phase 1 Failure will occur if the light does not work continuously for the specified duration of time as an accident could arise. The city power supply will be used constantly unless failure occurs, at which point the switch control will be activated and the battery is used as a backup source. If the battery is in the working state at the time of the failure of the city power supply, it will be put into operation and used continuously until the city power supply is restored. When the city power supply is restored, the switch control will activate the city power supply as being the primary power source. In the event that the battery fails before the city power supply has been restored, no power will be supplied to the bulb and the light will go out. The road sign will not be illuminated until the city power supply is restored. In such a situation, the failure of the city power supply is the initiating event due to the continuous requirement for successful operation. If this event occurs, the switch control is activated in order for the backup battery to take over. The failure of the switch control is therefore the enabling event. If this event occurs prior to the initiating event, the failure of the city power supply causes the light to go out and a potential dangerous situation to arise. If the enabling event occurs after the initiating event, the light will remain lit since the power supply has already been successfully transferred to the backup battery.

The second phase requires a successful routine bulb change. The continual requirement for the bulb to be lit in the first phase meant that a demand was only placed on the switch control in the event that the city power supply failed. The successful shutdown of the system in the second phase to enable a safe bulb change places a demand on the switch control to cut off both power supplies to the bulb. Since the failure of the switch control on its own can fail the system it becomes an initiating event.

It is possible to construct fault trees to represent Phase 1 failure – Light Does Not Work Continuously and Phase 2 failure – System not Shutdown for Period Routine Maintenance, shown in Figure 6.9.

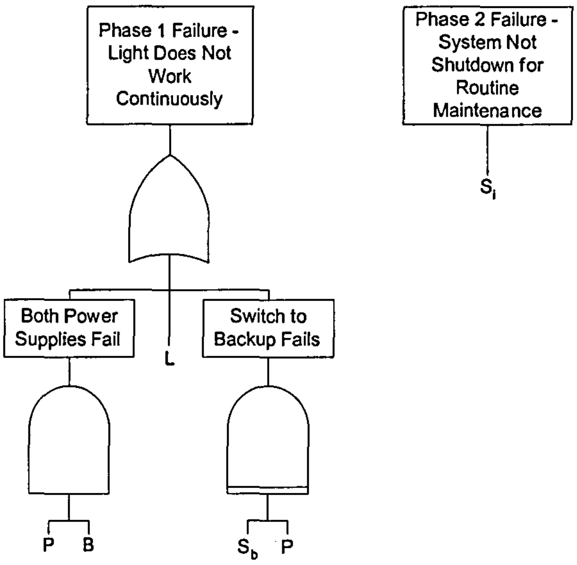

Phase 1 Failure - Light Does Not Work Continuously
Phase 2 Failure - System Not Shutdown for Routine Maintenance
S_i
Both Power Supplies Fail
L
Switch to Backup Fails
P
B
S_b
P

Figure 6.9 Road Sign Illumination System

It can be noted that the switch component failure will contribute differently to the system failure mode in different phases. In this case the failure of the switch control in phase 1 acts as an enabling event. Failure of the switch control in phase 2 acts as an initiating event. Similarly the role of the failure of the city power supply and the battery in phase 1 act as initiating events and change in phase 2 to have no requirement. This demonstrates the possibility for the event of component failure to change contribution through different phases.

6.4 Maintenance Policies

A further consideration is the way in which the components are maintained. So far, it has been assumed that all components begin repair as soon as failure occurs. However as an enabler may not be required continuously, the failure may not be detected unless an inspection takes place or an initiating event occurs and a demand is placed on it to respond. Such a situation can arise in a safety system which is not required until a component fails and places a demand on it to react. As the safety system is dormant and not used continuously, a failure will not be detected. Failures can therefore be categorised as either *revealed* or *unrevealed.*

A revealed failure is detected as soon as a component fails. This generally applies to components that are monitored continually over periods of time, or when they fail cause a noticeable system effect. The repair of such a failure assumes that there is no detection time and that the repair rate will depend only on the time to repair the component.

An unrevealed failure is usually detected by a scheduled maintenance routine. This type of maintenance policy is commonly used in safety and standby systems where components are not continuously operational. Otherwise the failure may not be noticed until a demand is placed on the component to work. The time that the component remains in the failed state depends not only on the component repair time, but also on the time taken to detect the failure. It is commonly assumed that the item is inspected every θ time units.

The failure of a component in a phase may be detected in different ways. The failure of a component causing an initiating event is detected instantly, however a component failure acting only as an enabling event or a component not used in the phase are not monitored continuously and thus failure can occur and remain unrevealed until the next inspection takes place. This is summarised in Table 6.2.

Component Contribution	Type of Failure
Initiator	Revealed
Enabler	Unrevealed
Not Required	Unrevealed

Table 6.2 Component Failure Types

The calculation of phase and mission reliability of a system that contains both initiating and enabling component failure events becomes very complex due to the large number of combinations of revealed and unrevealed failures that can occur.

6.4.1 Markov Model for Revealed and Unrevealed Failures

For an enabler or a component that is not required in a particular phase, it is possible to use a Markov model for the relationship between the revealed and unrevealed failure states as shown in Figure 6.10.

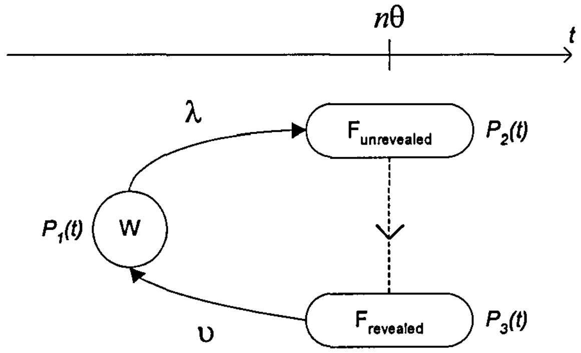
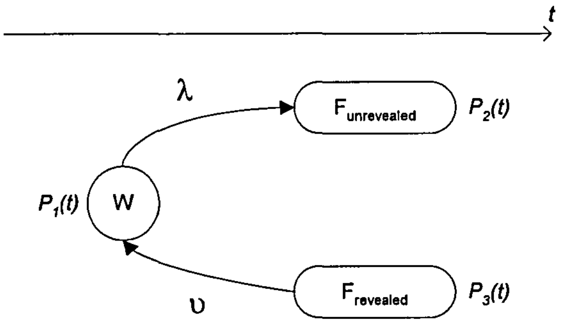


Figure 6.10 Unrevealed Component Failure in Markov Model

If the component begins life in the working state (W) with probability $P_1(t)$ it is possible for a transition to occur to the unrevealed failed state ($F_{\text{unrevealed}}$) at any point in time with failure rate λ.

If a scheduled inspection of the component takes place every $n\theta$ (n=1,2...), an unrevealed failure will not be detected until the next planned maintenance point. The probability of the component residing in this unrevealed failure state is denoted by $P_2(t)$. As soon as the failure is detected at $n\theta$, the component state moves directly from the unrevealed failure state into the revealed failure state (F_{revealed}). The component may then be restored to full working order with repair rate υ. The probability of the component residing in this revealed failure state is denoted by $P_3(t)$.

Transitions linking working and failed states can only occur between inspection points of a phase i. If phase i begins at time $t=t_{i-1}$ and ends at $t=t_i$, the state change model is shown in Figure 6.11.



for $t_{i-1} \leq t \leq t_i$
$t \neq n\theta$

Figure 6.11 Markov Model Between Inspection Points

At every $n\theta$, any unrevealed failures are detected and thus an instant transition between the unrevealed and revealed failure states occurs, shown in Figure 6.12.

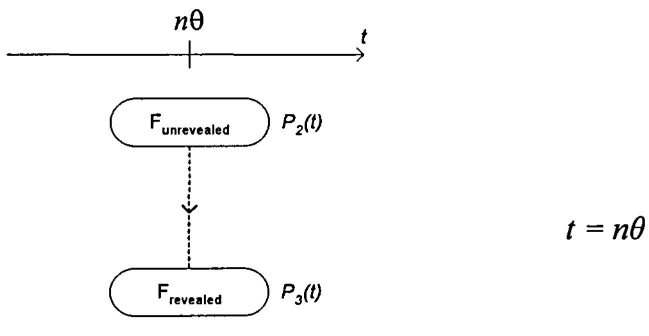


Figure 6.12 Markov Model At Inspection Points

The probability of the component residing in the unrevealed failed state ($P_2^*(n\theta)$) and revealed failed state ($P_3^*(n\theta)$) just after every $n\theta$ is given by equations (6.1)

$$\begin{aligned} P_3^*(n\theta) &= P_2(n\theta) + P_3(n\theta) \\ P_2^*(n\theta) &= 0 \end{aligned} \qquad n = 1,2,.. \qquad (6.1)$$

where $P_n^*(t)$ is the probability of the component residing in state n just after time t.

The concept for a single component Markov model for revealed and unrevealed failures may be extended to represent a system comprising of enablers, initiators, and components that are not required for a particular phase. If a mission is considered in its entirety, a total of N_C components from all phases must be considered throughout the mission duration.

Until now the states in the Markov models used for phased mission analysis have taken no account of scheduled inspection and the distinction between initiating and enabling events has not been made. A 2-component parallel system Markov model to calculate system unreliability was represented by Figure 6.3. Considering the possibility of sequential failures where all component failures are revealed, the 2-component Markov model was expanded to allow for sequential failures with component A failure as an enabling event and component B failure as an initiating event (Figure 6.4).

If a mission is considered in its entirety, a complete set of system states must be developed. As the failure of a component could act as an enabling event or an initiating event and in some phases not be required, there is a possibility that any component could fail unrevealed and thus a full Markov model must be developed to represent this. A new set of notation is introduced,

0	Component in the working state
1_{nU}	Component is the nth to fail. Failure unrevealed.
1_{nR}	Component is the nth to fail. Failure revealed.

For a 2-component system, the full set of system states may be summarised in Table 6.3.

State	A	B
1	0	0
2_1	0	1_{1U}
2_2	0	1_{1R}
3_1	1_{1U}	0
3_2	1_{1R}	0
4_1	1_{2U}	1_{1U}
4_2	1_{1U}	1_{2U}
4_3	1_{2U}	1_{1R}
4_4	1_{1U}	1_{2R}
4_5	1_{2R}	1_{1U}
4_6	1_{1R}	1_{2U}
4_7	1_{2R}	1_{1R}
4_8	1_{1R}	1_{2R}

Table 6.3 Possible States for a Mission Comprising of 2 Components

The Markov model in Figure 6.4 must be further expanded to identify revealed and unrevealed failures as repair of the enabling event cannot be initiated until a failure is identified at an inspection point. The Markov model would become that illustrated in Figure 6.13.

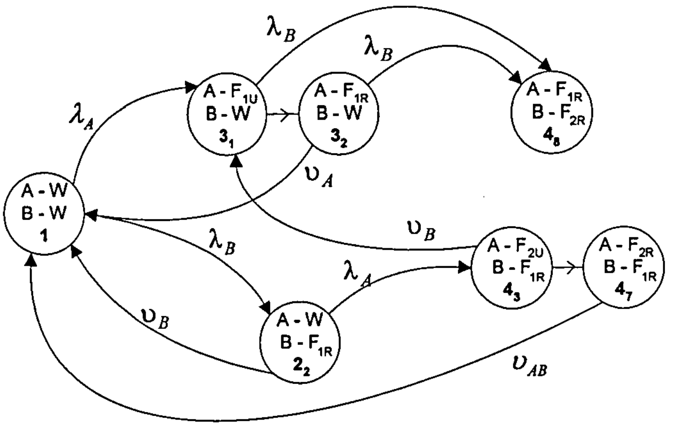


Figure 6.13 2-Component Markov Model with Unrevealed failures

If the system begins with both components working (state **1**), component failure may occur in either order. If the initiating event, component B revealed failure, occurs first with rate λ_B and component A is in the working state, system failure does not occur and the system will reside in state $\mathbf{2_2}$. From state $\mathbf{2_2}$ two transitions may be made. Component B may be restored to the good as new condition with repair rate υ_B and transfer back to state **1**. Alternatively before component B is repaired, component A may fail unrevealed and the system will make a transition to state $\mathbf{4_3}$. As the initiating event occurred prior to the enabling event, the resulting state with both components failed is a non-catastrophic system failure. A non-catastrophic failure occurs if the initiating event puts a demand on the safety system when the enabler allows safe shutdown. The enabler may be restored, therefore either component B is repaired with rate υ_B back to state $\mathbf{3_1}$, or the next scheduled inspection point reveals the failure of A and the system moves directly to state $\mathbf{4_7}$, where both components may be repaired with rate υ_{AB} back to state **1**.

The alternative sequence is that the enabling event, component A failure, occurs first. This failure will be unrevealed and the system will make a transition from state **1** to state $\mathbf{3_1}$. The occurrence of the enabling event first puts the system into a critical state for component B. Two transitions are possible – component A failure is revealed at the next inspection point, or component B fails before the failure of component A is detected. If the failure of component A is revealed at the next inspection point, instant transition to state $\mathbf{3_2}$ will occur where it may be restored to new condition (state **1**) with rate υ_A. State $\mathbf{3_2}$ is also a critical state for component B. If component B fails during the critical time that the system resides in state $\mathbf{3_1}$ or $\mathbf{3_2}$, instant system failure will occur. This will automatically reveal the fact that component A has failed and the system will transfer to state $\mathbf{4_8}$. This catastrophic failure is absorbing and the system will remain in this state.

It is seen that when considering a two-component parallel system with no sequential failures or scheduled inspection (Figure 6.3) there was only 1 state to represent both components in the failed state (4). This represented the only system failure mode. Once initiating and enabling events are taken into consideration with both unrevealed and revealed failures, there becomes a possibility of 8 failure states ($\mathbf{4_{1\text{-}8}}$ in Table 6.3). Now there are two revealed system failure outcomes, states $\mathbf{4_7}$ and $\mathbf{4_8}$. If the enabling event occurs and allows the initiating event to cause system failure, the result is catastrophic. If the initiating event occurs prior to the enabling event, repair is possible and the outcome is non-catastrophic.

For a 2-component system with both unrevealed and revealed component failures there is a possibility of 13 system states (Table 6.3). However, since component B failure is an initiator and thus cannot fail unrevealed, states 2_1,4_1,4_2,4_5, and 4_6 will not be used in the model. As the number of components in a system increases, the consideration of scheduled inspection points and sequential failure relationships results in an explosion of possible system states. Table 6.4 gives a comparison of how the possible number of system states increases as the number of components in the system increases. The elimination of system states that are not required for a particular model due to the function of components is discussed further in Chapter 7.

No. Of Components	Number Of States	
	Revealed Failure Only Model	Revealed and Unrevealed Failure Model
1	2	3
2	4	13
3	8	79
4	16	553

Table 6.4 Number of System States for Revealed and Unrevealed Failures

6.5 Summary

If events are categorised as initiators or enablers which fail revealed or unrevealed respectively, the Markov model gets very large for even small or moderate numbers of components. A method is required to reduce the number of possible system states as far as possible. If components that are not required for a particular phase can be identified, and separated from the components that are required in the phase and the failures that act as initiating or enabling events, a reduced Markov model may be constructed. For a two component system (one initiator), this is shown by comparison of the complete list of 13 system states (Table 6.3) with the reduced 7 state diagram (Figure 6.13). Rules to identify the possible system states in any phase required for a Markov model are presented in the following chapter.

It is also possible that an initiating event may only cause system failure if it occurs during a particular phase. If it occurs prior to the phase in question, the phase failure will not occur. Each type of initiating event must be modelled accordingly. Methods are required to solve such a phased mission system where the function of a component failure and appropriate maintenance policy can change through the phases. This is discussed in the next chapter.

Chapter 7 Phase Specific and Non- Phase Specific Initiating Events

7.1 Introduction

A component failure that acts as an initiating event in a phase may occur either prior to, or during the phase in question. In some cases, the top event of phase failure will only occur if the initiating event fails during a particular phase. If the initiating event occurred prior to the phase, it will not contribute to phase failure. This type of initiating event is defined as *phase specific* (PS) and is denoted by I_p. Other initiating events that can contribute to a phase failure regardless of which phase they occurred in are *non- phase specific* (NPS) and are defined by I.

The general case of non- phase specific initiators will be considered first in Section 7.2, followed by the introduction of phase specific initiators in Section 7.3.

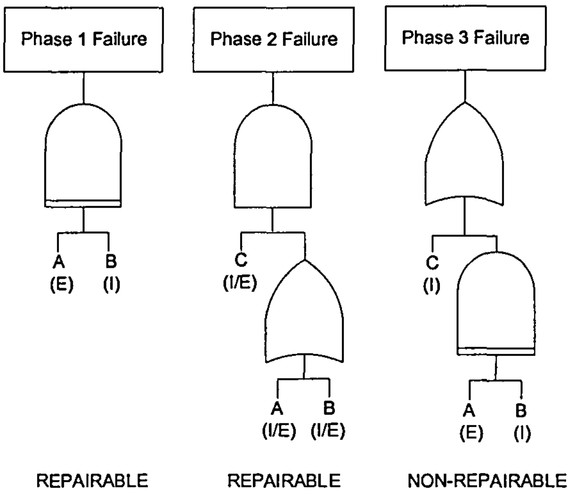
7.2 Non-Phase Specific Initiators

This section considers a phased mission system comprising of only NPS initiating events. Failure of a phase may be caused by the existence of a sequential cut set regardless of whether the events in the cut set occurred prior to or during the phase in question.

When considering a phased mission, it is possible that component failures can act in different capacities through the phases. The analysis of a phased mission involving enabling events and NPS initiating events can be demonstrated using a simple example consisting of three components, A, B and C (Figure 7.1).

The three phases are of a continuous nature. No state transitions can occur during a discrete phase and so a priority-AND gate would not occur in this type of phase. Since the inclusion of discrete phases is accommodated by simply checking for system compliance conditions at the appropriate time point it is not felt necessary to consider this in the demonstration example.

A component failure event can be categorised as a different type in each of the three phases. An event that only acts as an enabler in a phase may result in either an unrevealed or revealed component failure. If an enabling event occurs unrevealed, it will become revealed either by the occurrence of an initiating event from the same sequential cut set or at the next inspection point. The Markov model representing unrevealed enabling events requires states to signify both the unrevealed and revealed failure possibilities. If an enabling event only occurs revealed, it cannot reside in the unrevealed failure state at any point in the phase. The Markov model representing revealed enabling events requires states to signify only the revealed failure. Since considering the worst case scenario (in terms of model development) where enabling events occur unrevealed encompasses the simpler situation where an enabling event can occur revealed, enabling events will be treated as unrevealed.



where	E	Enabling Event
	I	Initiating Event not Specific to Phase
	I/E	Initiating Event Capable of Enabling

Figure 7.1 Mission with Sequential Failures and NPS Initiating Events

The occurrence of an initiating event is a revealed component failure. It is possible that an initiating event can also act as an enabler, for example in a parallel arrangement of 2 components where at least one component is required to work for the system to function successfully. The failure of either component would act as an enabling event for the initiating failure of the other component.

The type of event caused by component failure in each of the phases of Figure 7.1 is summarised in Table 7.1.

Component Failure	Phase 1	Phase 2	Phase 3
A	Enabler	Initiator/ Enabler	Enabler
B	Initiator	Initiator/ Enabler	Initiator
C	Not Required	Initiator/ Enabler	Initiator

Table 7.1 Component Failure Events in 3-Phased Mission

7.2.1 Full Markov Model

Since the phases in the example (Figure 7.1) are either repairable or contain dynamic gates, a suitable method for analysis is the Markov method. Using a full Markov model as described in Section 5.2.1, a complete list of possible system states can be constructed. As component failure may occur revealed or unrevealed and is subject to change through the phases, the full list requires the inclusion of each type of failure for every component. The ordering of failure events is also important, thus for each state involving failures a suitable representation must be given for the sequential failure ordering.

For a system with three components the list is developed and all possible system states with appropriate ordering and failure type are given in Table 7.2.

Using the relevant sub-set of states from the full listing in Table 7.2, a full Markov model comprising of every component and appropriate state transitions can be constructed for each of the three phases, represented by Figures 7.2, 7.3 and 7.4 respectively.

State Ref	Component States		
	A	B	C
$1^{(ABC)}$	0	0	0
$2_1^{(ABC)}$	0	0	1_{1U}
$2_2^{(ABC)}$	0	0	1_{1R}
$3_1^{(ABC)}$	0	1_{1U}	0
$3_2^{(ABC)}$	0	1_{1R}	0
$4_1^{(ABC)}$	0	1_{2U}	1_{1U}
$4_2^{(ABC)}$	0	1_{1U}	1_{2U}
$4_3^{(ABC)}$	0	1_{2U}	1_{1R}
$4_4^{(ABC)}$	0	1_{1U}	1_{2R}
$4_5^{(ABC)}$	0	1_{2R}	1_{1U}
$4_6^{(ABC)}$	0	1_{1R}	1_{2U}
$4_7^{(ABC)}$	0	1_{2R}	1_{1R}
$4_8^{(ABC)}$	0	1_{1R}	1_{2R}
$5_1^{(ABC)}$	1_{1U}	0	0
$5_2^{(ABC)}$	1_{1R}	0	0
$6_1^{(ABC)}$	1_{2U}	0	1_{1U}
$6_2^{(ABC)}$	1_{1U}	0	1_{2U}
$6_3^{(ABC)}$	1_{2U}	0	1_{1R}
$6_4^{(ABC)}$	1_{1U}	0	1_{2R}
$6_5^{(ABC)}$	1_{2R}	0	1_{1U}
$6_6^{(ABC)}$	1_{1R}	0	1_{2U}
$6_7^{(ABC)}$	1_{2R}	0	1_{1R}
$6_8^{(ABC)}$	1_{1R}	0	1_{2R}
$7_1^{(ABC)}$	1_{2U}	1_{1U}	0
$7_2^{(ABC)}$	1_{1U}	1_{2U}	0
$7_3^{(ABC)}$	1_{2U}	1_{1R}	0
$7_4^{(ABC)}$	1_{1U}	1_{2R}	0
$7_5^{(ABC)}$	1_{2R}	1_{1U}	0
$7_6^{(ABC)}$	1_{1R}	1_{2U}	0
$7_7^{(ABC)}$	1_{2R}	1_{1R}	0
$7_8^{(ABC)}$	1_{1R}	1_{2R}	0
$8_1^{(ABC)}$	1_{3U}	1_{2U}	1_{1U}
$8_2^{(ABC)}$	1_{2U}	1_{3U}	1_{1U}
$8_3^{(ABC)}$	1_{3U}	1_{1U}	1_{2U}
$8_4^{(ABC)}$	1_{2U}	1_{1U}	1_{3U}
$8_5^{(ABC)}$	1_{1U}	1_{3U}	1_{2U}
$8_6^{(ABC)}$	1_{1U}	1_{2U}	1_{3U}
$8_7^{(ABC)}$	1_{3U}	1_{2U}	1_{1R}
$8_8^{(ABC)}$	1_{2U}	1_{3U}	1_{1R}
$8_9^{(ABC)}$	1_{3U}	1_{1U}	1_{2R}

State Ref	Component States		
	A	B	C
$8_{10}^{(ABC)}$	1_{2U}	1_{1U}	1_{3R}
$8_{11}^{(ABC)}$	1_{1U}	1_{3U}	1_{2R}
$8_{12}^{(ABC)}$	1_{1U}	1_{2U}	1_{3R}
$8_{13}^{(ABC)}$	1_{3U}	1_{2R}	1_{1U}
$8_{14}^{(ABC)}$	1_{2U}	1_{3R}	1_{1U}
$8_{15}^{(ABC)}$	1_{3U}	1_{1R}	1_{2U}
$8_{16}^{(ABC)}$	1_{2U}	1_{1R}	1_{3U}
$8_{17}^{(ABC)}$	1_{1U}	1_{3R}	1_{2U}
$8_{18}^{(ABC)}$	1_{1U}	1_{2R}	1_{3U}
$8_{19}^{(ABC)}$	1_{3U}	1_{2R}	1_{1R}
$8_{20}^{(ABC)}$	1_{2U}	1_{3R}	1_{1R}
$8_{21}^{(ABC)}$	1_{3U}	1_{1R}	1_{2R}
$8_{22}^{(ABC)}$	1_{2U}	1_{1R}	1_{3R}
$8_{23}^{(ABC)}$	1_{1U}	1_{3R}	1_{2R}
$8_{24}^{(ABC)}$	1_{1U}	1_{2R}	1_{3R}
$8_{25}^{(ABC)}$	1_{3R}	1_{2U}	1_{1U}
$8_{26}^{(ABC)}$	1_{2R}	1_{3U}	1_{1U}
$8_{27}^{(ABC)}$	1_{3R}	1_{1U}	1_{2U}
$8_{28}^{(ABC)}$	1_{2R}	1_{1U}	1_{3U}
$8_{29}^{(ABC)}$	1_{1R}	1_{3U}	1_{2U}
$8_{30}^{(ABC)}$	1_{1R}	1_{2U}	1_{3U}
$8_{31}^{(ABC)}$	1_{3R}	1_{2U}	1_{1R}
$8_{32}^{(ABC)}$	1_{2R}	1_{3U}	1_{1R}
$8_{33}^{(ABC)}$	1_{3R}	1_{1U}	1_{2R}
$8_{34}^{(ABC)}$	1_{2R}	1_{1U}	1_{3R}
$8_{35}^{(ABC)}$	1_{1R}	1_{3U}	1_{2R}
$8_{36}^{(ABC)}$	1_{1R}	1_{2U}	1_{3R}
$8_{37}^{(ABC)}$	1_{3R}	1_{2R}	1_{1U}
$8_{38}^{(ABC)}$	1_{2R}	1_{3R}	1_{1U}
$8_{39}^{(ABC)}$	1_{3R}	1_{1R}	1_{2U}
$8_{40}^{(ABC)}$	1_{2R}	1_{1R}	1_{3U}
$8_{41}^{(ABC)}$	1_{1R}	1_{3R}	1_{2U}
$8_{42}^{(ABC)}$	1_{1R}	1_{2R}	1_{3U}
$8_{43}^{(ABC)}$	1_{3R}	1_{2R}	1_{1R}
$8_{44}^{(ABC)}$	1_{2R}	1_{3R}	1_{1R}
$8_{45}^{(ABC)}$	1_{3R}	1_{1R}	1_{2R}
$8_{46}^{(ABC)}$	1_{2R}	1_{1R}	1_{3R}
$8_{47}^{(ABC)}$	1_{1R}	1_{3R}	1_{2R}
$8_{48}^{(ABC)}$	1_{1R}	1_{2R}	1_{3R}

where 0 Component in the working state
1_{nU} Component is the nth to fail. Failure unrevealed.
1_{nR} Component is the nth to fail. Failure revealed.

Table 7.2 Full State Representation of 3-Component System with Sequential Failures and Scheduled Inspection

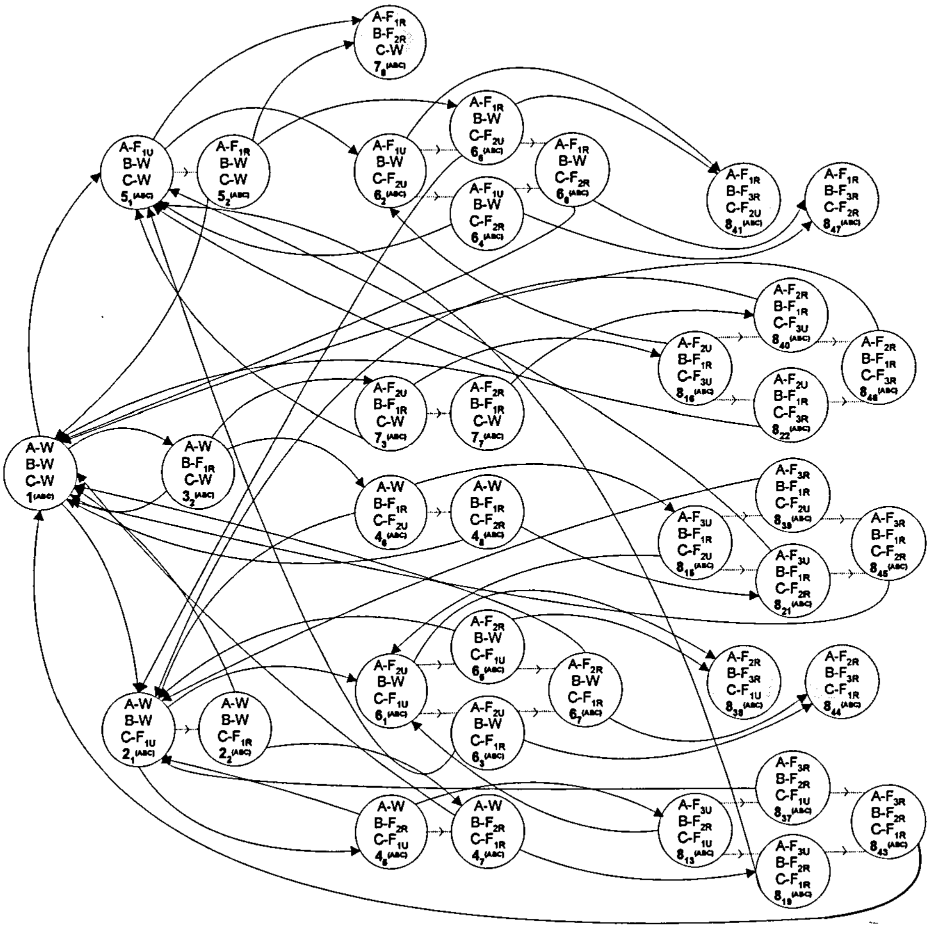

A-F$_{1R}$ B-F$_{2R}$ C-W $7_{8}^{(ABC)}$
A-F$_{1R}$ B-W C-F$_{2U}$ $6_{6}^{(ABC)}$
A-F$_{1U}$ B-W C-W $5_{1}^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_{2}^{(ABC)}$
A-F$_{1U}$ B-W C-F$_{2U}$ $6_{2}^{(ABC)}$
A-F$_{1R}$ B-W C-F$_{2R}$ $6_{8}^{(ABC)}$
A-F$_{1U}$ B-W C-F$_{2R}$ $6_{4}^{(ABC)}$
A-F$_{1R}$ B-F$_{3R}$ C-F$_{2U}$ $8_{41}^{(ABC)}$
A-F$_{1R}$ B-F$_{3R}$ C-F$_{2R}$ $8_{47}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_{3U}$ $8_{40}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_{3U}$ $8_{16}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_{3R}$ $8_{46}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_{3R}$ $8_{22}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-W $7_{3}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_{7}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_{2}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_{2U}$ $4_{6}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_{2R}$ $4_{8}^{(ABC)}$
A-F$_{3R}$ B-F$_{1R}$ C-F$_{2U}$ $8_{39}^{(ABC)}$
A-F$_{3U}$ B-F$_{1R}$ C-F$_{2U}$ $8_{15}^{(ABC)}$
A-F$_{3R}$ B-F$_{1R}$ C-F$_{2R}$ $8_{45}^{(ABC)}$
A-F$_{3U}$ B-F$_{1R}$ C-F$_{2R}$ $8_{21}^{(ABC)}$
A-F$_{2R}$ B-W C-F$_{1U}$ $6_{5}^{(ABC)}$
A-F$_{2U}$ B-W C-F$_{1U}$ $6_{1}^{(ABC)}$
A-F$_{2R}$ B-W C-F$_{1R}$ $6_{7}^{(ABC)}$
A-F$_{2R}$ B-F$_{3R}$ C-F$_{1U}$ $8_{38}^{(ABC)}$
A-F$_{2R}$ B-F$_{3R}$ C-F$_{1R}$ $8_{44}^{(ABC)}$
A-W B-W C-F$_{1U}$ $2_{1}^{(ABC)}$
A-W B-W C-F$_{1R}$ $2_{2}^{(ABC)}$
A-F$_{2U}$ B-W C-F$_{1R}$ $6_{3}^{(ABC)}$
A-F$_{3R}$ B-F$_{2R}$ C-F$_{1U}$ $8_{37}^{(ABC)}$
A-W B-F$_{2R}$ C-F$_{1U}$ $4_{5}^{(ABC)}$
A-W B-F$_{2R}$ C-F$_{1R}$ $4_{7}^{(ABC)}$
A-F$_{3U}$ B-F$_{2R}$ C-F$_{1U}$ $8_{13}^{(ABC)}$
A-F$_{3R}$ B-F$_{2R}$ C-F$_{1R}$ $8_{43}^{(ABC)}$
A-F$_{3U}$ B-F$_{2R}$ C-F$_{1R}$ $8_{19}^{(ABC)}$

Figure 7.2 Full Markov Model for Phase 1

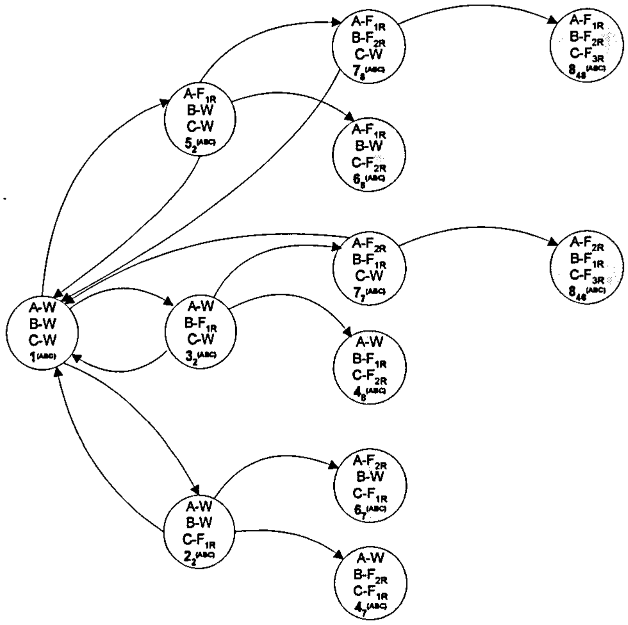

A-F$_{1R}$ B-F$_{2R}$ C-W $7_{8}^{(ABC)}$
A-F$_{1R}$ B-F$_{2R}$ C-F$_{3R}$ $8_{48}^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_{2}^{(ABC)}$
A-F$_{1R}$ B-W C-F$_{2R}$ $6_{8}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_{7}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_{3R}$ $8_{46}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_{2}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_{2R}$ $4_{8}^{(ABC)}$
A-F$_{2R}$ B-W C-F$_{1R}$ $6_{7}^{(ABC)}$
A-W B-W C-F$_{1R}$ $2_{2}^{(ABC)}$
A-W B-F$_{2R}$ C-F$_{1R}$ $4_{7}^{(ABC)}$

Figure 7.3 Full Markov Model for Phase 2

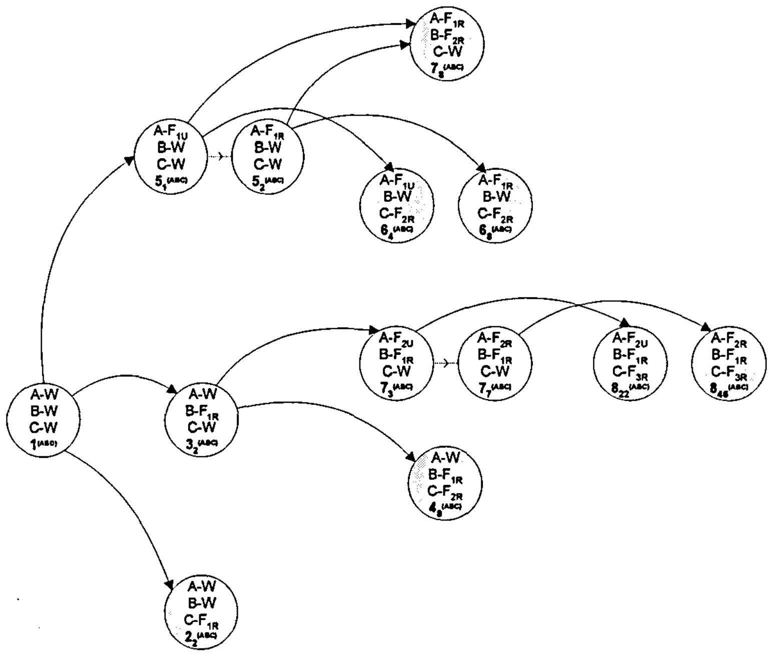

A-F$_{1R}$ B-F$_{2R}$ C-W $7_8^{(ABC)}$
A-F$_{1U}$ B-W C-W $5_1^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_2^{(ABC)}$
A-F$_{1U}$ B-W C-F$_{2R}$ $6_4^{(ABC)}$
A-F$_{1R}$ B-W C-F$_{2R}$ $6_8^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-W $7_3^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_7^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_{3R}$ $8_{22}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_{3R}$ $8_{46}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_2^{(ABC)}$
A-W B-F$_{1R}$ C-F$_{2R}$ $4_8^{(ABC)}$
A-W B-W C-F$_{1R}$ $2_2^{(ABC)}$

Figure 7.4 Full Markov Model for Phase 3

Out of the 79 possible system states, only 38 are used during the three phases of the mission. It must also be noted that from these 38 mission system states, several are not possible within some phases. To analyse the full Markov model using the matrix method would produce a very sparse transition matrix and would require the solution of the full set of 79 differential equations. The full Markov method was investigated in Section 5.2.1 and demonstrated the susceptibility to state space explosion with only revealed failures. In this case components can fail both revealed and unrevealed and ordering is important thus the state space explosion becomes increasingly problematic. As found in Section 5.2.1 it uses unnecessary computer memory resources and extra computational time to develop a full Markov model for every phase in an entire mission. The solution process can be made significantly more efficient if unused states can be eliminated from the model.

7.2.1.1 State Identification

If the mission is taken in its entirety, it is very difficult to identify all states that can be eliminated from the full model listing (Table 7.2) due to the change in sequential failure relationships throughout the mission. Considering each component contribution over the phases of the mission (Table 7.1), there are two impossibilities that allow some states to be removed from the full Markov model. These are summarised in Table 7.3.

Impossibility	
1. Every cut set of a phase must involve an initiating event. is impossible for all components to be in the unrevealed failure state at any point in time.	$8_1^{(ABC)} - 8_6^{(ABC)}$
2. A component that is required in all phases and only ever fails as an initiating event can never fail unrevealed. (component B)	$3_1^{(ABC)}, 4_1^{(ABC)} - 4_4^{(ABC)}, 7_1^{(ABC)} - 7_2^{(ABC)},$ $7_5^{(ABC)} - 7_6^{(ABC)}, 8_1^{(ABC)} - 8_{12}^{(ABC)}, 8_{25}^{(ABC)} - 8_{36}^{(ABC)}$

Table 7.3 Summary of Impossible System States due to Component Contributions

Application of these two rules to the full state listing (Table 7.2) eliminates 33 states from the model. However since these rules apply for the whole mission, the generality of them fails to identify all of the states that are never required and also the states that are not possible within each individual phase. Identification of all states that the system cannot reside in both for the entire mission and also within each phase can only be accomplished by examination of the individual sequential failure relationships and cut sets of the mission. For the example mission shown in Figure 7.1, the cut sets are given by,

Phase 1 $A^E B^I$

Phase 2 $A^{I/E} C^{I/E}$
$B^{I/E} C^{I/E}$

where E = Enabling Event
I = NPS Initiating Event
I/E = Initiating Event Capable of Enabling

Phase 3 C^I
$A^E B^I$

There are certain points to be noticed from the full list of cut sets of this mission that allow further state reduction of the full Markov model, summarised in Table 7.4.

Impossibility	States Removed
1. The system cannot reside in a state where component A has failed unrevealed and component B fails after this revealed. This is justified since in Phases 1 and 3 the failure of component B automatically reveals the failure of component A, and in Phase 2 component A cannot fail unrevealed.	$7_4^{(ABC)}, 8_{14}^{(ABC)}, 8_{17}^{(ABC)} - 8_{18}^{(ABC)}$, $8_{20}^{(ABC)}, 8_{23}^{(ABC)} - 8_{24}^{(ABC)}$
2. The system cannot reside in a state where components A and B fail revealed in the order of A then B, and component C fails last unrevealed. This state is not possible since in phases 1 and 3 system failure will occur after the first two failures and no further state transitions may take place, and in phase 2 component C cannot fail unrevealed.	$8_{42}^{(ABC)}$

Table 7.4 Summary of Impossible System States due to Mission Cut Sets

This state reduction method becomes very complex with increasing numbers of components, making it more difficult to identify all states from the full expansion (Table 7.2) that are not possible at any point during the mission. Since these points identify state impossibilities that are consistent through the entire mission, the generality of them fails to recognise all of the impossible system states in each individual phase.

A general set of rules for any phased mission system is produced to enable the removal of impossible system states from the full Markov model within each phase. Given a full list of system minimal cut sets it is possible to identify the unattainable system states for each phase of the example given in Figure 7.1, shown in Table 7.5.

Impossibility	Impossible States		
	Phase 1	Phase 2	Phase 3
1. An initiating event cannot fail unrevealed	$3_1^{(ABC)}, 4_1^{(ABC)} - 4_4^{(ABC)}, 7_1^{(ABC)} - 7_2^{(ABC)}, 7_5^{(ABC)} - 7_6^{(ABC)}, 8_1^{(ABC)} - 8_{12}^{(ABC)}, 8_{25}^{(ABC)} - 8_{36}^{(ABC)}$	$2_1^{(ABC)}, 3_1^{(ABC)}, 4_1^{(ABC)} - 4_6^{(ABC)}, 5_1^{(ABC)}, 6_1^{(ABC)} - 6_6^{(ABC)}, 7_1^{(ABC)} - 7_6^{(ABC)}, 8_1^{(ABC)} - 8_{42}^{(ABC)}$	$2_1^{(ABC)}, 3_1^{(ABC)}, 4_1^{(ABC)} - 4_6^{(ABC)}$, $6_1^{(ABC)} - 6_2^{(ABC)}, 6_5^{(ABC)} - 6_6^{(ABC)}$, $7_1^{(ABC)} - 7_2^{(ABC)}, 7_5^{(ABC)} - 7_6^{(ABC)}$, $8_1^{(ABC)} - 8_{18}^{(ABC)}, 8_{25}^{(ABC)} - 8_{42}^{(ABC)}$
2. The occurrence of a sequentially ordered cut set reveals failures of all components in the cut set.	$7_4^{(ABC)}, 8_{14}^{(ABC)}, 8_{17}^{(ABC)} - 8_{18}^{(ABC)}$, $8_{20}^{(ABC)}, 8_{23}^{(ABC)} - 8_{24}^{(ABC)}$	-	$7_4^{(ABC)}, 8_{14}^{(ABC)}, 8_{20}^{(ABC)}$, $8_{23}^{(ABC)} - 8_{24}^{(ABC)}$
3. Once a cut set occurs, no further component failures may take place.	$8_{42}^{(ABC)}, 8_{48}^{(ABC)}$	$8_{43}^{(ABC)} - 8_{45}^{(ABC)}, 8_{47}^{(ABC)}$	$4_7^{(ABC)}, 6_3^{(ABC)}, 6_7^{(ABC)}$, $8_{19}^{(ABC)}, 8_{21}^{(ABC)}, 8_{43}^{(ABC)} -$ $8_{45}^{(ABC)}, 8_{47}^{(ABC)} - 8_{48}^{(ABC)}$

Table 7.5 State Removal within Each Individual Phase

If all the possible system states through the duration of the mission are identified, the full Markov model can be implemented. However since this requires the use of identical system states throughout the phases, the full Markov model for each phase must include all of the 38 possible system states listed in Table 7.6.

State Ref	Component States			Phase 1	Phase 2	Phase 3
	A	B	C			
$1^{(ABC)}$	0	0	0	W	W	W
$2_1^{(ABC)}$	0	0	1_{1U}	W	R	R
$2_2^{(ABC)}$	0	0	1_{1R}	W	W	F
$3_2^{(ABC)}$	0	1_{1R}	0	W	W	W
$4_5^{(ABC)}$	0	1_{2R}	1_{1U}	W	R	R
$4_6^{(ABC)}$	0	1_{1R}	1_{2U}	W	R	R
$4_7^{(ABC)}$	0	1_{2R}	1_{1R}	W	F	R
$4_8^{(ABC)}$	0	1_{1R}	1_{2R}	W	F	F
$5_1^{(ABC)}$	1_{1U}	0	0	W	R	W
$5_2^{(ABC)}$	1_{1R}	0	0	W	W	W
$6_1^{(ABC)}$	1_{2U}	0	1_{1U}	W	R	R
$6_2^{(ABC)}$	1_{1U}	0	1_{2U}	W	R	R
$6_3^{(ABC)}$	1_{2U}	0	1_{1R}	W	R	R
$6_4^{(ABC)}$	1_{1U}	0	1_{2R}	W	R	F
$6_5^{(ABC)}$	1_{2R}	0	1_{1U}	W	R	R
$6_6^{(ABC)}$	1_{1R}	0	1_{2U}	W	R	R
$6_7^{(ABC)}$	1_{2R}	0	1_{1R}	W	W	R
$6_8^{(ABC)}$	1_{1R}	0	1_{2R}	W	W	F
$7_3^{(ABC)}$	1_{2U}	1_{1R}	0	W	R	W
$7_7^{(ABC)}$	1_{2R}	1_{1R}	0	W	F	W
$7_8^{(ABC)}$	1_{1R}	1_{2R}	0	F	F	F
$8_{13}^{(ABC)}$	1_{3U}	1_{2R}	1_{1U}	W	R	R
$8_{15}^{(ABC)}$	1_{3U}	1_{1R}	1_{2U}	W	R	R
$8_{16}^{(ABC)}$	1_{2U}	1_{1R}	1_{3U}	W	R	R
$8_{19}^{(ABC)}$	1_{3U}	1_{2R}	1_{1R}	W	R	R
$8_{21}^{(ABC)}$	1_{3U}	1_{1R}	1_{2R}	W	R	R
$8_{22}^{(ABC)}$	1_{2U}	1_{1R}	1_{3R}	W	R	F
$8_{37}^{(ABC)}$	1_{3R}	1_{2R}	1_{1U}	W	R	R
$8_{38}^{(ABC)}$	1_{2R}	1_{3R}	1_{1U}	F	R	R
$8_{39}^{(ABC)}$	1_{3R}	1_{1R}	1_{2U}	W	R	R
$8_{40}^{(ABC)}$	1_{2R}	1_{1R}	1_{3U}	W	R	R
$8_{41}^{(ABC)}$	1_{1R}	1_{3R}	1_{2U}	F	R	R
$8_{43}^{(ABC)}$	1_{3R}	1_{2R}	1_{1R}	W	R	R
$8_{44}^{(ABC)}$	1_{2R}	1_{3R}	1_{1R}	F	R	R
$8_{45}^{(ABC)}$	1_{3R}	1_{1R}	1_{2R}	W	R	R
$8_{46}^{(ABC)}$	1_{2R}	1_{1R}	1_{3R}	W	F	F
$8_{47}^{(ABC)}$	1_{1R}	1_{3R}	1_{2R}	F	R	R
$8_{48}^{(ABC)}$	1_{1R}	1_{2R}	1_{3R}	R	F	R

W – Working State in Phase F – Failed State in Phase R – Unreachable State in Phase

Table 7.6 Possible System States for Full Markov Model of 3-Component System Example with Sequential Failures and Scheduled Inspection

The full Markov model system states may be classed as either *required* or *unreachable* during each phase of the mission. A required system state is achievable during a phase, where as an unreachable system state is not possible during a phase but may be attainable during other phases of the mission. An unreachable state will have no transitions either into or out of it, in which case a series of zero entries will appear in the corresponding row and column of the full 38 x 38 state transition matrix. Since the probability of the system residing in an unreachable state is zero, only the equations to represent the possible system states must be solved in each phase. In the same way as for the full Markov model in Section 5.2.1, the sparse nature of this matrix must be accounted for and memory storage allocated as described in Section 5.1.1.

7.2.1.2 State Combination

It may be possible to combine states with the same failure mode to reduce the Markov model further. If a component is identified that never contributes to a sequential failure cut set during the mission, it is possible to remove that component failure from the ordering scheme. Since the order of failure of the component compared to other components is irrelevant throughout the mission, state combination will be consistent through all phases. At this stage using a full Markov model it is not possible to remove components from the failure ordering scheme during individual phases. Since the initiating events are not phase specific, the ordering of a component failure not contributory to a particular phase sequential cut set may become important in a later phase.

This state combination technique can be applied to the example in Figure 7.1. Component C is not an input to a dynamic gate in any phase of the mission and so it is not necessary to consider the order of failure of component C in relation to the other components. Component C is not required during phase 1 but it is possible that it can fail during this phase. The failure of component C can be classed as either 1_U or 1_R, with no representation of order. All other component failures may then be re-ordered with respect only to each other. The possible mission system states after this re-ordering process are given in Table 7.7.

State Ref	Component States			Phase 1	Phase 2	Phase 3
	A	B	C			
$1^{(ABC)}$	0	0	0	W	W	W
$2_1^{(ABC)}$	0	0	1_U	W	R	R
$2_2^{(ABC)}$	0	0	1_R	W	W	F
$3_2^{(ABC)}$	0	1_{1R}	0	W	W	W
$4_5^{(ABC)}$	0	1_{1R}	1_U	W	R	R
$4_6^{(ABC)}$	0	1_{1R}	1_U	W	R	R
$4_7^{(ABC)}$	0	1_{1R}	1_R	W	F	R
$4_8^{(ABC)}$	0	1_{1R}	1_R	W	F	F
$5_1^{(ABC)}$	1_{1U}	0	0	W	R	W
$5_2^{(ABC)}$	1_{1R}	0	0	W	W	W
$6_1^{(ABC)}$	1_{1U}	0	1_U	W	R	R
$6_2^{(ABC)}$	1_{1U}	0	1_U	W	R	R
$6_3^{(ABC)}$	1_{1U}	0	1_R	W	R	R
$6_4^{(ABC)}$	1_{1U}	0	1_R	W	R	F
$6_5^{(ABC)}$	1_{1R}	0	1_U	W	R	R
$6_6^{(ABC)}$	1_{1R}	0	1_U	W	R	R
$6_7^{(ABC)}$	1_{1R}	0	1_R	W	W	R
$6_8^{(ABC)}$	1_{1R}	0	1_R	W	W	F
$7_3^{(ABC)}$	1_{2U}	1_{1R}	0	W	R	W
$7_7^{(ABC)}$	1_{2R}	1_{1R}	0	W	F	W
$7_8^{(ABC)}$	1_{1R}	1_{2R}	0	F	F	F
$8_{13}^{(ABC)}$	1_{2U}	1_{1R}	1_U	W	R	R
$8_{15}^{(ABC)}$	1_{2U}	1_{1R}	1_U	W	R	R
$8_{16}^{(ABC)}$	1_{2U}	1_{1R}	1_U	W	R	R
$8_{19}^{(ABC)}$	1_{2U}	1_{1R}	1_R	W	R	R
$8_{21}^{(ABC)}$	1_{2U}	1_{1R}	1_R	W	R	R
$8_{22}^{(ABC)}$	1_{2U}	1_{1R}	1_R	W	R	F
$8_{37}^{(ABC)}$	1_{2R}	1_{1R}	1_U	W	R	R
$8_{38}^{(ABC)}$	1_{1R}	1_{2R}	1_U	F	R	R
$8_{39}^{(ABC)}$	1_{2R}	1_{1R}	1_U	W	R	R
$8_{40}^{(ABC)}$	1_{2R}	1_{1R}	1_U	W	R	R
$8_{41}^{(ABC)}$	1_{1R}	1_{2R}	1_U	F	R	R
$8_{43}^{(ABC)}$	1_{2R}	1_{1R}	1_R	W	R	R
$8_{44}^{(ABC)}$	1_{1R}	1_{2R}	1_R	F	R	R
$8_{45}^{(ABC)}$	1_{2R}	1_{1R}	1_R	W	R	R
$8_{46}^{(ABC)}$	1_{2R}	1_{1R}	1_R	W	F	F
$8_{47}^{(ABC)}$	1_{1R}	1_{2R}	1_R	F	R	R
$8_{48}^{(ABC)}$	1_{1R}	1_{2R}	1_R	R	F	R

Where W – Working State in Phase
F – Failed State in Phase
R – Unreachable State in Phase

Table 7.7 Possible System States for Full Markov Model of 3-Component System Example with No Ordering of Component C

The removal of component C from the order of failure has produced multiple states representing the same failure mode in the model. It is possible to combine all states with the same combination of component failures into a single state. For example states $4_5^{(ABC)}$ and $4_6^{(ABC)}$ now represent the situation that component B fails revealed, and component C has failed unrevealed either before or after the failure of component B. The replication of the state means that states $4_5^{(ABC)}$ and $4_6^{(ABC)}$ can be combined to form a single state, and is defined by $4_{5,6}^{(ABC)}$. In general, the combination of replicated states is defined by equation (7.1).

$$\text{Identical States: } S_l, S_m, S_n \quad \text{Combine to: } S_l, S_m, S_n \rightarrow S_{l,m,n} \tag{7.1}$$

All replicated states in Table 7.7 may be combined using this method. However, in some phases an unreachable state will be combined with a required phase state. For example, states $4_7^{(ABC)}$ and $4_8^{(ABC)}$ now represent the same component combination where component B fails revealed, and component C has failed revealed either before or after the failure of component B. In phase 3, state $4_7^{(ABC)}$ was previously an unreachable state since component B cannot fail after component C, and state $4_8^{(ABC)}$ was an achievable phase state. In such a case the new combined state takes the place of the achievable phase state and results in the same success or failure outcome. The final combined states are consistent through all phases of the mission and are given in Table 7.8.

The single states in each of the three phases given by Figures 7.2, 7.3, and 7.4 may be replaced where possible by the new combined states. The full Markov models for phases 1, 2, and 3 become as shown in Figures 7.5, 7.6, and 7.7 respectively.

State Ref	Component States			Phase 1	Phase 2	Phase 3
	A	B	C			
$1^{(ABC)}$	0	0	0	W	W	W
$2_1^{(ABC)}$	0	0	1_U	W	R	R
$2_2^{(ABC)}$	0	0	1_R	W	W	F
$3_2^{(ABC)}$	0	1_{1R}	0	W	W	W
$4_{5,6}^{(ABC)}$	0	1_{1R}	1_U	W	R	R
$4_{7,8}^{(ABC)}$	0	1_{1R}	1_R	W	F	F
$5_1^{(ABC)}$	1_{1U}	0	0	W	R	W
$5_2^{(ABC)}$	1_{1R}	0	0	W	W	W
$6_{1,2}^{(ABC)}$	1_{1U}	0	1_U	W	R	R
$6_{3,4}^{(ABC)}$	1_{1U}	0	1_R	W	R	R
$6_{5,6}^{(ABC)}$	1_{1R}	0	1_U	W	R	R
$6_{7,8}^{(ABC)}$	1_{1R}	0	1_R	W	W	F
$7_3^{(ABC)}$	1_{2U}	1_{1R}	0	W	R	W
$7_7^{(ABC)}$	1_{2R}	1_{1R}	0	W	F	W
$7_8^{(ABC)}$	1_{1R}	1_{2R}	0	F	F	F
$8_{13,15,16}^{(ABC)}$	1_{2U}	1_{1R}	1_U	W	R	R
$8_{19,21,22}^{(ABC)}$	1_{2U}	1_{1R}	1_R	W	R	F
$8_{37,39,40}^{(ABC)}$	1_{2R}	1_{1R}	1_U	W	R	R
$8_{38,41}^{(ABC)}$	1_{1R}	1_{2R}	1_U	F	R	R
$8_{43,45,46}^{(ABC)}$	1_{2R}	1_{1R}	1_R	W	F	F
$8_{44,47,48}^{(ABC)}$	1_{1R}	1_{2R}	1_R	F	F	R

Table 7.8 Possible System States for Full Markov Model of 3-Component System Example with Sequential Failures and Scheduled Inspection

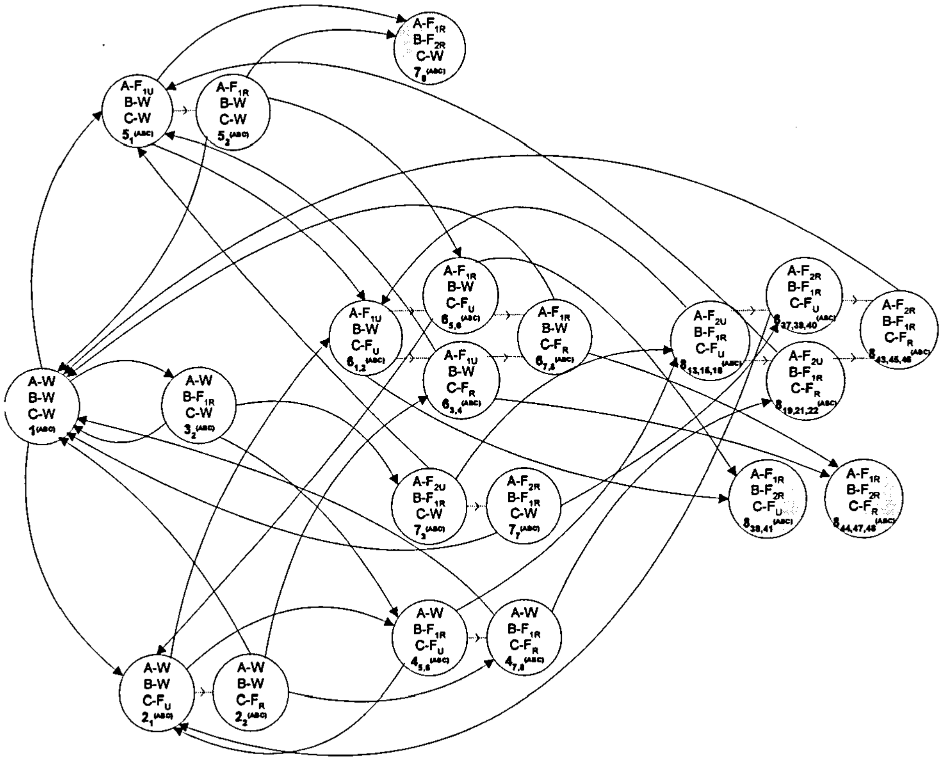
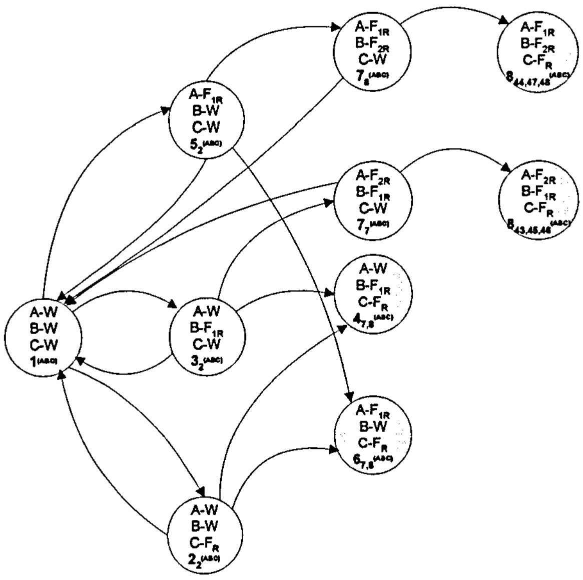
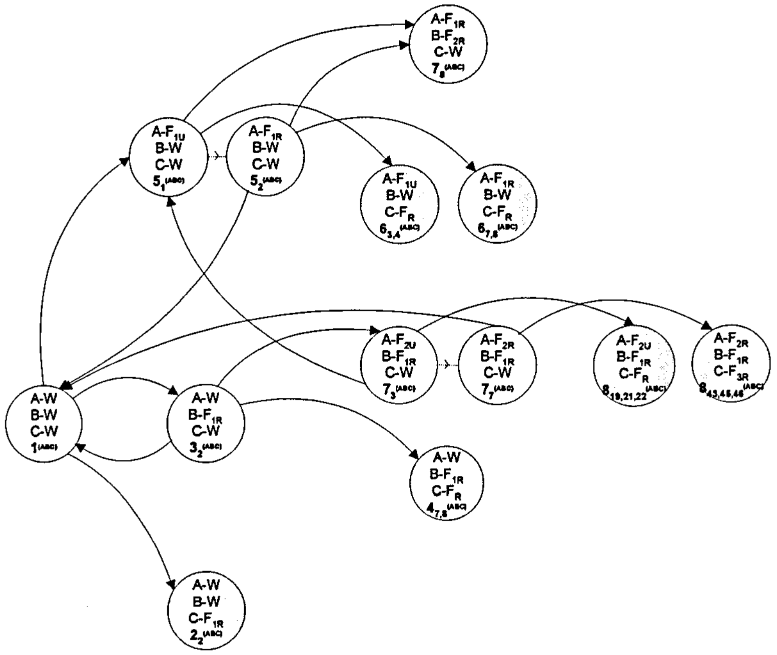

A-F$_{1R}$ B-F$_{2R}$ C-W $7_8^{(ABC)}$
A-F$_{1U}$ B-W C-W $5_1^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_2^{(ABC)}$
A-F$_{1R}$ B-W C-F$_U$ $6_{5,6}^{(ABC)}$
A-F$_{1U}$ B-W C-F$_U$ $6_{1,2}^{(ABC)}$
A-F$_{1R}$ B-W C-F$_R$ $6_{7,8}^{(ABC)}$
A-F$_{1U}$ B-W C-F$_R$ $6_{3,4}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_U$ $8_{37,39,40}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_R$ $8_{43,45,46}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_U$ $8_{13,15,16}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_R$ $8_{19,21,22}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_2^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-W $7_3^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_7^{(ABC)}$
A-F$_{1R}$ B-F$_{2R}$ C-F$_U$ $8_{38,41}^{(ABC)}$
A-F$_{1R}$ B-F$_{2R}$ C-F$_R$ $8_{44,47,48}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_U$ $4_{5,6}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_R$ $4_{7,8}^{(ABC)}$
A-W B-W C-F$_U$ $2_1^{(ABC)}$
A-W B-W C-F$_R$ $2_2^{(ABC)}$

Figure 7.5 Full Markov Model with Combined States for Phase 1



A-F$_{1R}$ B-F$_{2R}$ C-W $7_8^{(ABC)}$
A-F$_{1R}$ B-F$_{2R}$ C-F$_R$ $8_{44,47,48}^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_2^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_7^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_R$ $8_{43,45,46}^{(ABC)}$
A-W B-F$_{1R}$ C-F$_R$ $4_{7,8}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_2^{(ABC)}$
A-F$_{1R}$ B-W C-F$_R$ $6_{7,8}^{(ABC)}$
A-W B-W C-F$_R$ $2_2^{(ABC)}$

Figure 7.6 Full Markov Model with Combined States for Phase 2



A-F$_{1R}$ B-F$_{2R}$ C-W $7_8^{(ABC)}$
A-F$_{1U}$ B-W C-W $5_1^{(ABC)}$
A-F$_{1R}$ B-W C-W $5_2^{(ABC)}$
A-F$_{1U}$ B-W C-F$_R$ $6_{3,4}^{(ABC)}$
A-F$_{1R}$ B-W C-F$_R$ $6_{7,8}^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-W $7_3^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-W $7_7^{(ABC)}$
A-F$_{2U}$ B-F$_{1R}$ C-F$_R$ $8_{19,21,22}^{(ABC)}$
A-F$_{2R}$ B-F$_{1R}$ C-F$_{3R}$ $8_{43,45,46}^{(ABC)}$
A-W B-W C-W $1^{(ABC)}$
A-W B-F$_{1R}$ C-W $3_2^{(ABC)}$
A-W B-F$_{1R}$ C-F$_R$ $4_{7,8}^{(ABC)}$
A-W B-W C-F$_{1R}$ $2_2^{(ABC)}$

Figure 7.7 Full Markov Model with Combined States for Phase 3

It can be seen that combining states in the full Markov diagram produces a more compact model for analysis. For example in Phase 1 (Figure 7.2) there were previously three paths leading to a catastrophic system state. The path to state 7_8 cannot be combined with any others since there are no other states representing the same component failure combination. The two paths originally resulting in a catastrophic state with all three components A, B, and C in the failed state are shown in Figure 7.8.

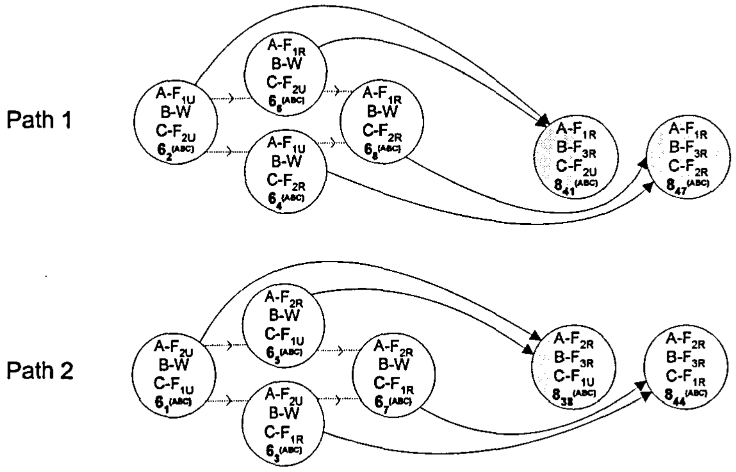

Path 1
A-F_{1U} B-W C-F_{2U} $6_2^{(ABC)}$
A-F_{1R} B-W C-F_{2U} $6_6^{(ABC)}$
A-F_{1U} B-W C-F_{2R} $6_4^{(ABC)}$
A-F_{1R} B-W C-F_{2R} $6_8^{(ABC)}$
A-F_{1R} B-F_{3R} C-F_{2U} $8_{41}^{(ABC)}$
A-F_{1R} B-F_{3R} C-F_{2R} $8_{47}^{(ABC)}$
Path 2
A-F_{2U} B-W C-F_{1U} $6_1^{(ABC)}$
A-F_{2R} B-W C-F_{1U} $6_5^{(ABC)}$
A-F_{2U} B-W C-F_{1R} $6_3^{(ABC)}$
A-F_{2R} B-W C-F_{1R} $6_7^{(ABC)}$
A-F_{2R} B-F_{3R} C-F_{1U} $8_{38}^{(ABC)}$
A-F_{2R} B-F_{3R} C-F_{1R} $8_{44}^{(ABC)}$

Figure 7.8 Original Paths Leading to Catastrophic Failure in Phase 1

The identification of states representing the same system failure mode allows the two paths in Figure 7.8 to be combined into a single path as shown in Figure 7.9.

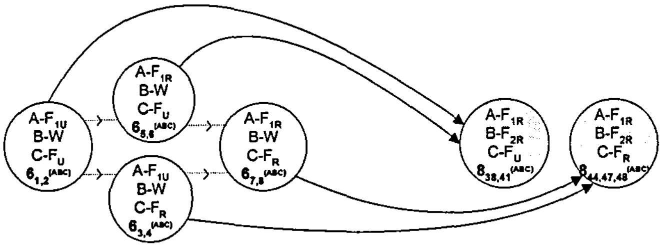

A-F_{1U} B-W C-F_U $6_{1,2}^{(ABC)}$
A-F_{1R} B-W C-F_U $6_{5,6}^{(ABC)}$
A-F_{1U} B-W C-F_R $6_{3,4}^{(ABC)}$
A-F_{1R} B-W C-F_R $6_{7,8}^{(ABC)}$
A-F_{1R} B-F_{2R} C-F_U $8_{38,41}^{(ABC)}$
A-F_{1R} B-F_{2R} C-F_R $8_{44,47,48}^{(ABC)}$

Figure 7.9 Combined Paths Leading to Catastrophic Failure in Phase 1

The combination of states representing this particular catastrophic failure mode has halved the number of possible system states from 12 to 6.

The comparison between the number of states forming the original full Markov model for each phase and the reduced number of states using this combination technique is summarised in Table 7.9.

Phase	Number of States in Original Full Markov Model	Number of States in Combined State Full Markov Model
1	37	21
2	12	10
3	13	13

Table 7.9 Comparison of the Number of States of the Original Full Markov Model and the Combined State Markov Model

This state combination technique is seen to reduce the number of states required for the full Markov model, especially in the first phase. The reduced number of system states results in a much smaller model for analysis, thus reducing the computational time and memory requirements.

Once the achievable system states have been identified and the state combination technique has been applied, the final phase Markov models are defined by Figures 7.5, 7.6, and 7.7 with all possible system states of the full Markov model listed in Table 7.8.

7.2.1.3 Phase Transition Problem

When considering the full Markov model for a system with no sequential failure relationships or scheduled inspection as presented in Section 5.2.1, the states are common from one phase to another. The probability of a system residing in a particular state can be directly passed to the same state in the immediately proceeding phase at any transition point. Since only static fault tree gates are considered, a failure outcome is achieved if the events of a cut set occur in any order. The system will reside in a model state representative of the components that have failed, regardless of how this state was achieved. When considering the possibility of sequential failures, further analysis must be carried out across a phase boundary.

At transition points between phases the situation may arise where a working system state in the previous phase is not an achievable system state in the immediately succeeding phase. The reasons for this are discussed as follows:

- A component failure cannot occur unrevealed in the next phase

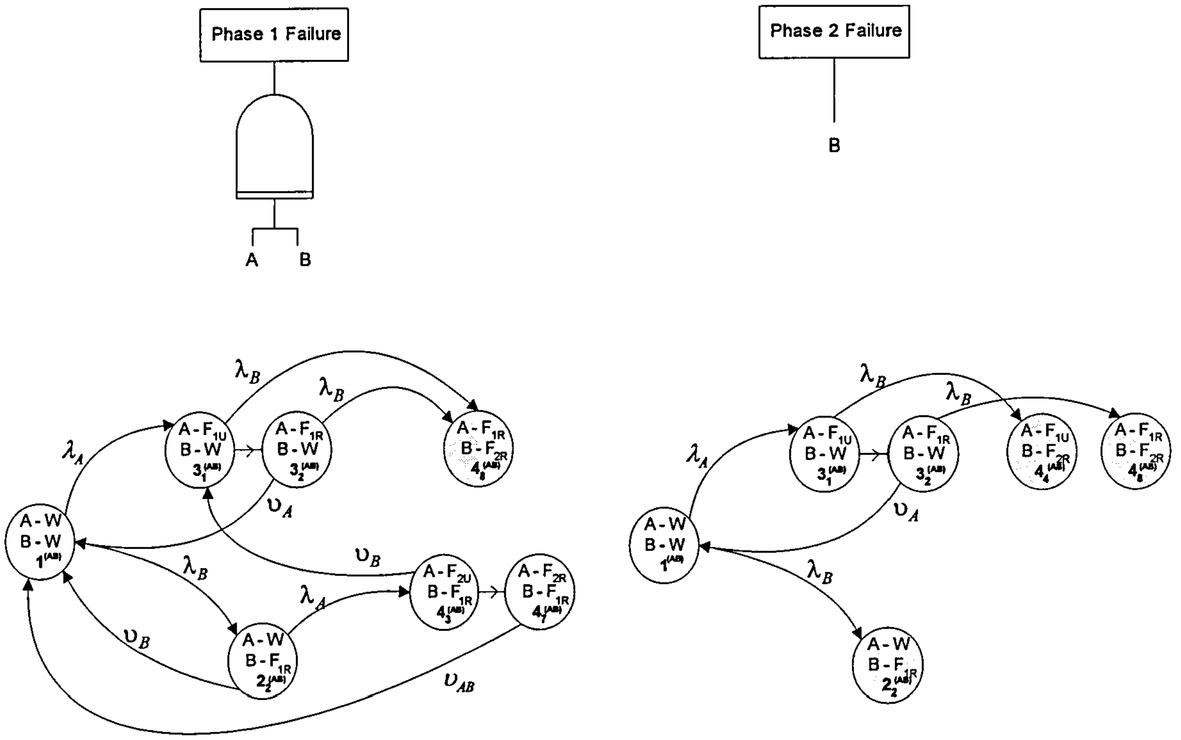
An initiating event will always occur revealed in a phase. In the case that an unrevealed enabling event at the end of one phase assumes the role of an initiating event at the start of the next phase, the component failure will automatically be revealed at the time of transition. A similar situation occurs if a component that does not contribute to the system failure for a particular phase experiences failure, if it acts as an initiating event in the immediately succeeding phase the failure of the component is revealed at the phase transition. States that represent the unrevealed failure of the event become unreachable in the following phase when it begins to act as an initiator.

Application of this rule to the example in Figure 7.1 identifies that enabling event A in phase 1 becomes an initiating event in phase 2. All states representative of an unrevealed component A failure at the end of phase 1 become equivalent to the same state with component A in the revealed failure state on transition to phase 2. Similarly component C does not contribute to the failure conditions in phase 1 and so failure will occur unrevealed. The failure of component C in phase 2 acts as an initiating event and so at the time of transition to phase 2 this failure will also become revealed. The probability of the system residing in a state with the component in the unrevealed failure state at the end of the phase is redistributed to the probability of the system residing in the same state with the component in the revealed failure state, and the unrevealed failure state probability is set to zero. The final re-assigned phase 1 system state probabilities for entry to phase 2 become as shown in equations (7.2).

$$\begin{array}{ll}
P_{2_2}^{(ABC)}(t_1) = P_{2_1}^{(ABC)}(t_1) + P_{2_2}^{(ABC)}(t_1) & P_{2_1}^{(ABC)}(t_1) \rightarrow 0 \\
P_{4_{7,8}}^{(ABC)}(t_1) = P_{4_{5,6}}^{(ABC)}(t_1) + P_{4_{7,8}}^{(ABC)}(t_1) & P_{4_{5,6}}^{(ABC)}(t_1) \rightarrow 0 \\
P_{5_2}^{(ABC)}(t_1) = P_{5_1}^{(ABC)}(t_1) + P_{5_2}^{(ABC)}(t_1) & P_{5_1}^{(ABC)}(t_1) \rightarrow 0 \\
P_{6_{7,8}}^{(ABC)}(t_1) = P_{6_{1,2}}^{(ABC)}(t_1) + P_{6_{3,4}}^{(ABC)}(t_1) + P_{6_{5,6}}^{(ABC)}(t_1) + P_{6_{7,8}}^{(ABC)}(t_1) & P_{6_{1,2}}^{(ABC)}(t_1), P_{6_{3,4}}^{(ABC)}(t_1), P_{6_{5,6}}^{(ABC)}(t_1) \rightarrow 0 \\
P_{7_7}^{(ABC)}(t_1) = P_{7_3}^{(ABC)}(t_1) + P_{7_7}^{(ABC)}(t_1) & P_{7_3}^{(ABC)}(t_1) \rightarrow 0 \\
P_{8_{43,45,46}}^{(ABC)}(t_1) = P_{8_{13,15,16}}^{(ABC)}(t_1) + P_{8_{19,21,22}}^{(ABC)}(t_1) + P_{8_{37,39,40}}^{(ABC)}(t_1) + P_{8_{43,45,46}}^{(ABC)}(t_1) & P_{8_{13,15,16}}^{(ABC)}(t_1), P_{8_{19,21,22}}^{(ABC)}(t_1), P_{8_{37,39,40}}^{(ABC)}(t_1) \rightarrow 0 \\
P_{8_{44,47,48}}^{(ABC)}(t_1) = P_{8_{38,41}}^{(ABC)}(t_1) + P_{8_{44,47,48}}^{(ABC)}(t_1) & P_{8_{38,41}}^{(ABC)}(t_1) \rightarrow 0
\end{array} \tag{7.2}$$

- A particular combination of component failures cannot occur

A phase system state representing a particular combination of component failures can be unreachable if the phase fails prior to the state being reached. Consider the simple 2-phase example in Figure 7.10.



(a) Phase 1 Markov Model

(b) Phase 2 Markov Model

Figure 7.10 Two Phase Example

State $4_7^{(AB)}$ represents the revealed failure of component B followed by the revealed failure of component A. This is a working state in phase 1 since the sequential cut set $\{A^{(E)}\ B^{(I)}\}$ has not occurred. State $4_7^{(AB)}$ becomes unreachable in the second phase since phase 2 failure occurs after the failure of component B (state $2_2^{(AB)}$) and no further component failures can take place. If such a situation occurs across a phase boundary, the working system state probability will directly contribute to the phase transition failure probability into the following phase. In the example in Figure 7.10, transition failure will occur if the system resides in a working phase 1 state that is failed in phase 2 ($2_2^{(AB)}$), or a working phase 1 state that becomes unreachable in phase 2 because the state cannot be reached ($4_3^{(AB)}$ and $4_7^{(AB)}$),

$$Tr(t_1) = P_{2_2}^{(AB)}(t_1) + P_{4_3}^{(AB)}(t_1) + P_{4_7}^{(AB)}(t_1)\,.$$

If the reverse situation occurs whereby an impossible system state becomes possible in a later phase, it will be assigned an initial state probability of zero.

7.2.1.4 Final Full Markov Model Solution Process

The reliability of each phase and the overall mission illustrated in Figure 7.1 would be solved using a full Markov model in the following way:

Phase 1

The full 21 Markov model states are listed in Table 7.8. The system can reside in any of these 21 system states in phase 1, as shown in Figure 7.5. The mission is assumed to commence with all components in the working state **1** and so the initial 21 state probability matrix is given by equation (7.3).

$$\mathbf{P}(0) = [1\ 0\ 0\cdots\cdots 0] \qquad (7.3)$$

The set of differential equations to give transient state probabilities are solved over the duration of phase 1. The reliability of phase 1 is found by the sum of the final probabilities of the system residing in a successful state (Table 7.8), given by equation (7.4).

$$R(t_1) = 1 - \left(P_{7_8}^{(ABC)}(t_1) + P_{8_{38,41}}^{(ABC)}(t_1) + P_{8_{44,47,48}}^{(ABC)}(t_1)\right) \qquad (7.4)$$

Phase 2

All states that cause failure or are not possible in phase 1 are assigned a probability of 0 at the phase termination. The final set of sequential state probabilities at the end of phase 1 must then be combined to form a reduced set of state probabilities representative of the possible phase 2 states.

As described in Section 7.2.1.3, the enabling event of component A failure in phase 1 becomes a NPS initiating event in phase 2. Also, the event of component C failure which does not contribute to system failure in phase 1 becomes an initiating event in phase 2. At the transition point between phases 1 and 2, the failure of components A and C will automatically become revealed. The first step is to re-assign all probabilities for states representative of components A or C in the unrevealed state to contribute to the identical system state with components A or C respectively in the revealed state. The final re-assigned phase 1 system state probabilities are given in equations (7.2).

Transition failure will occur if the system resides in a successful phase 1 state that represents the existence of a phase 2 minimal cut set. In this case, both the phase 2 minimal cut sets are non-sequential, {A,C} and {B,C}. Transition failure will occur if the system resides in any states with components A and C, or B and C failed, irrelevant of failure order at the end of phase 1. Transition failure must account for all successful phase 1 states representative of phase 2 failure including those states that become unreachable and do not contribute to the system states in phase 2 (Section 7.2.1.3). Phase 2 transition failure is found by equation (7.5).

$$Tr(t_1) = P^{(ABC)}_{4_{7,8}}(t_1) + P^{(ABC)}_{6_{7,8}}(t_1) + P^{(ABC)}_{8_{43,45,46}}(t_1) \qquad (7.5)$$

Each possible phase 2 system state is assigned an initial probability equal to the corresponding state probability at the end of phase 1. All states that were not possible in phase 1, or that cause phase 2 transition failure, are assigned an initial probability of zero in phase 2. The initial sequential state probabilities for phase 2 are given in equations (7.6).

$$\begin{array}{ll}
P^{(ABC)}_{1}(t_1) = P^{(ABC)}_{1}(t_1) & P^{(ABC)}_{6_{7,8}}(t_1) = 0 \\
P^{(ABC)}_{2_2}(t_1) = P^{(ABC)}_{2_2}(t_1) & P^{(ABC)}_{7_7}(t_1) = P^{(ABC)}_{7_7}(t_1) \\
P^{(ABC)}_{3_2}(t_1) = P^{(ABC)}_{3_2}(t_1) & P^{(ABC)}_{7_8}(t_1) = 0 \\
P^{(ABC)}_{4_{7,8}}(t_1) = 0 & P^{(ABC)}_{8_{43,45,46}}(t_1) = 0 \\
P^{(ABC)}_{5_2}(t_1) = P^{(ABC)}_{5_2}(t_1) & P^{(ABC)}_{8_{44,47,48}}(t_1) = 0
\end{array} \qquad (7.6)$$

The full Markov model with transitions between states (Figure 7.6) may then be solved over the duration of phase 2 taking into account the sparse nature of the matrix. The reliability of phase 2 is found by the sum of the probabilities that the system resides in a successful state at the end of the phase in equation (7.7).

$$R(t_2) = P^{(ABC)}_{1}(t_2) + P^{(ABC)}_{2_2}(t_2) + P^{(ABC)}_{3_2}(t_2) + P^{(ABC)}_{5_2}(t_2) + P^{(ABC)}_{7_7}(t_2) + P^{(ABC)}_{7_8}(t_2) \qquad (7.7)$$

Phase 3

The final state probabilities at the end of phase 2 are passed directly to phase 3, where all states that cause failure or are not possible in phase 2 are assigned a final probability of zero. Since all events in phase 2 are required and initiating, there will be no unrevealed component failures at the start of phase 3.

The system must reside in a state that is successful for both phases 2 and 3 to complete the transition successfully. In the same way as for the transition to phase 2, transition failure will occur if the system resides in a state representing the existence of a phase 3 minimal cut set. There are two phase 3 minimal cut sets; non-sequential {C}, and sequential $\{A^{(E)},B^{(I)}\}$. Transition failure will occur if the system resides in a successful final phase 2 state with component C in the failed state ($2_2^{(ABC)}$), or in a state representative of the failure sequence of components A then B ($7_8^{(ABC)}$). In this case there are no successful phase 2 states that become unreachable and thus contribute to the transition failure in phase 3. The phase 3 transition failure is given by equation (7.8).

$$Tr(t_2) = P_{2_2}^{(ABC)}(t_2) + P_{7_8}^{(ABC)}(t_2) \tag{7.8}$$

The final phase 2 state probabilities are passed directly to the identical state in phase 3. All states that were unreachable in phase 2 but become possible in phase 3, and also states causing phase 3 transition failure are assigned an initial probability of zero. The initial phase 3 system state probabilities become as given in equations (7.9).

$$\begin{array}{ll}
P_1^{(ABC)}(t_2) = P_1^{(ABC)}(t_2) & P_{6_{7,8}}^{(ABC)}(t_2) = 0 \\
P_{2_2}^{(ABC)}(t_2) = 0 & P_{7_3}^{(ABC)}(t_2) = 0 \\
P_{3_2}^{(ABC)}(t_2) = P_{3_2}^{(ABC)}(t_2) & P_{7_7}^{(ABC)}(t_2) = P_{7_7}^{(ABC)}(t_2) \\
P_{4_{7,8}}^{(ABC)}(t_2) = 0 & P_{7_8}^{(ABC)}(t_2) = 0 \\
P_{5_1}^{(ABC)}(t_2) = 0 & P_{8_{19,21,22}}^{(ABC)}(t_2) = 0 \\
P_{5_2}^{(ABC)}(t_2) = P_{5_2}^{(ABC)}(t_2) & P_{8_{43,45,46}}^{(ABC)}(t_2) = 0 \\
P_{6_{3,4}}^{(ABC)}(t_2) = 0 &
\end{array} \tag{7.9}$$

The full Markov model with transitions shown in Figure 7.7 may then be solved over the duration of the phase. The reliability of phase 3 is found by the sum of the probabilities that the system resides in a successful state at the end of the phase in equation (7.10).

$$R(t_3) = P_1^{(ABC)}(t_3) + P_{3_2}^{(ABC)}(t_3) + \sum_{j=1,2} P_{5_j}^{(ABC)}(t_3) + \sum_{j=3,7} P_{7_j}^{(ABC)}(t_3) \qquad (7.10)$$

The total mission unreliability is the probability that the system failed during the mission, thus does not reside in a successful system state at the end of phase 3. This is given in equation (7.11).

$$Q_{MISS} = 1 - \left(P_1^{(ABC)}(t_3) + P_{3_2}^{(ABC)}(t_3) + \sum_{j=1,2} P_{5_j}^{(ABC)}(t_3) + \sum_{j=3,7} P_{7_j}^{(ABC)}(t_3) \right) \qquad (7.11)$$

7.2.2 Reduced Markov Model

The Markov models can become very large with only a moderate number of components and so this process needs to be made more efficient if at all possible. By considering only the Markov model for each phase it may be possible to further reduce the size and complexity of the problem.

There are two methods by which the Markov model can be reduced further. One is through the elimination of irrelevant component states from the phase Markov model, and the other is the implementation of fault tree analysis for solution to non-repairable phases. At the end of each phase, the reduced models are expanded to represent the required states of all components contributing to later phases in the mission for entry to the next phase.

7.2.2.1 Phase Transition Model

A new model is defined between phases, the *phase transition model*. This is the minimal model required at a particular point in the mission. At the start of the mission, all components that do not contribute to any NPS sequential minimal cut sets in any phase are eliminated from the ordering scheme of the full Markov state model as discussed in Section 7.2.1.2. This defines the initial transition model.

At each following transition point, a new transition model can be defined. If a component is not required in any later phases, it may be removed from the transition model completely. All further components that do not contribute to any NPS sequential minimal cut sets in later phases can be eliminated from the ordering scheme of the most recent transition model.

Minimisation of the Markov model within each individual phase may only be implemented where components do not contribute to any NPS sequential minimal cut sets in later phases. At the end of each phase the minimised model is expanded back to the transition model for input to the next phase.

In the example in Figure 7.1, the initial transition model for components A, B, and C is defined by identifying that component C does not contribute to any NPS sequential cut sets during the mission (Section 7.2.1.2). Since all three components are required in the final phase, it is not possible to remove any components completely from the transition model. Components A and B both contribute to a NPS sequential cut set in phase 3, and so this transition model cannot be further reduced at any phase boundaries through the mission. The transition model is discussed further with inclusion of PS sequential minimal cut sets in Section 7.3.1.

7.2.2.2 Removal of Irrelevant Components

A smaller Markov model in a repairable phase could be formed by including only the components contributing to the phase failure. Analysis over a continuous phase duration is performed by application of a minimal Markov model (N_{S_i} x N_{S_i}) using only the components required in the particular phase *i*. The full set of states for the transition model is reduced to evaluate the N_{S_i} initial conditions for each phase, and expanded out to the transition model at the end of a phase to enable calculation of successful entry to the immediately succeeding phase.

This method may only be implemented for situations where an irrelevant component only contributes to non-sequential cut sets or PS sequential minimal cut sets in later phases. If the component failure is known to contribute to a NPS sequential minimal cut set later in the mission, the order of failure of the component with respect to other components would be required and so cannot be removed from the model.

As described in Section 5.2.3, it is possible to eliminate components that are not required in a phase from the full Markov model. In the example shown in Figure 7.1, state removal due to non-required components is only possible in phase 1. Component C is irrelevant during this phase, and only contributes to static gates in later phases. The phase 1 Markov model can be reduced to 7 system states dependent on only the status of components A and B (Table 7.10 and Figure 7.11).

State	A	B
$1^{(AB)}$	0	0
$2_1^{(AB)}$	0	1_{1U}
$2_2^{(AB)}$	0	1_{1R}
$3_1^{(AB)}$	1_{1U}	0
$3_2^{(AB)}$	1_{1R}	0
$4_1^{(AB)}$	1_{2U}	1_{1U}
$4_2^{(AB)}$	1_{1U}	1_{2U}
$4_3^{(AB)}$	1_{2U}	1_{1R}
$4_4^{(AB)}$	1_{1U}	1_{2R}
$4_5^{(AB)}$	1_{2R}	1_{1U}
$4_6^{(AB)}$	1_{1R}	1_{2U}
$4_7^{(AB)}$	1_{2R}	1_{1R}
$4_8^{(AB)}$	1_{1R}	1_{2R}

Table 7.10 States of A and B

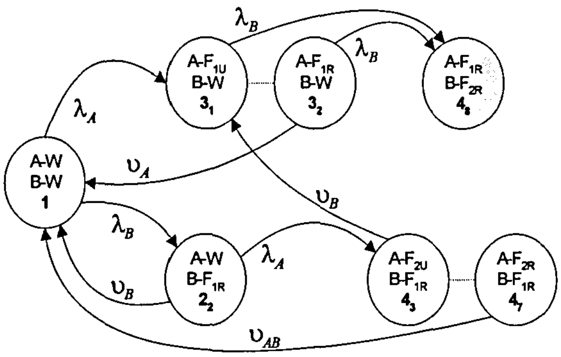


Figure 7.11 Reduced Phase 1 Markov Model

The failure of a component c that is not required in a particular phase is assumed to occur with rate λ_c and is unrevealed since it is not continuously monitored. This failure will be revealed at the next inspection point or where it appears as an initiator in a later phase, and the component may then be restored to new condition at repair rate v_c. The scheduled inspection of a component c takes place every $n\theta_c$ (n=1,2,..), where θ_c remains consistent for each component through the mission and $n_{i\max}\ \theta_c$ is the last inspection point for component c in phase i. The inspection period θ_c is considered to be much larger than the mean repair time.

There are two possibilities of scheduled maintenance in phase i. The first assumes that if the component was monitored continuously in the previous phase, or maintenance is known to begin at the start of a phase, then scheduled inspection points begin at t_{i-1}.

The unavailability of an irrelevant component under scheduled maintenance that begins at t_{i-1} over the duration of phase i can be given as a function of time as shown in Figure 7.12.

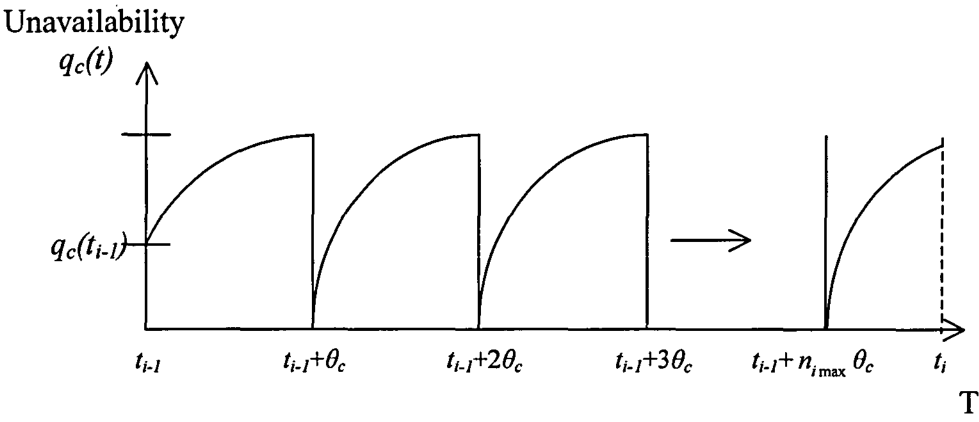
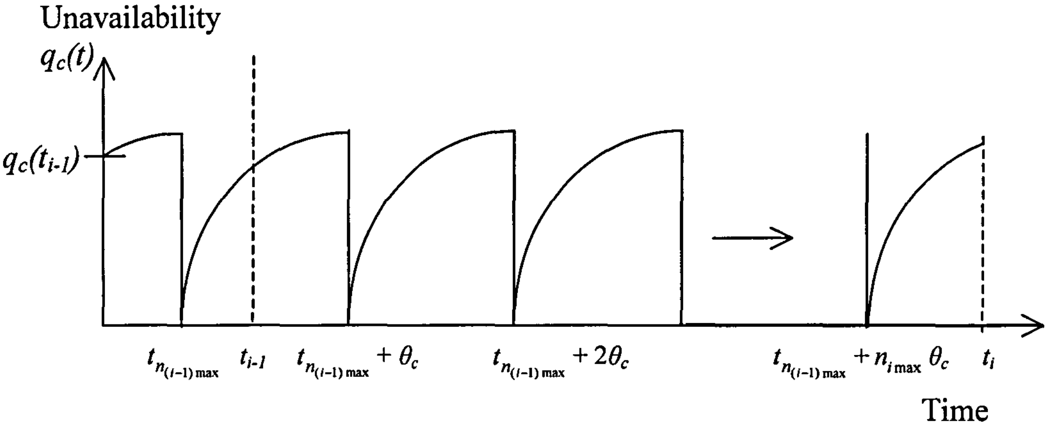


Figure 7.12 Unavailability of an Irrelevant Component Under Scheduled Inspection beginning at t_{i-1}

Alternatively if the scheduled maintenance of the component is continued from the previous phase, the scheduled inspection points depend on the most recent inspection time in the last phase. The last scheduled inspection of component c in phase i is defined as being at $t=t_{n_{i\max}}$. The unavailability of an irrelevant component under scheduled maintenance in phase i that continues from phase i-1 can be given as a function of time as shown in Figure 7.13.



where $t_{n_{(i-1)\max}}$ is the last inspection point in phase i-1

$t_{n_{(i-1)\max}}+n_{i\max}\theta_c$ is the last inspection point in phase i

Figure 7.13 Unavailability of an Irrelevant Component Under Scheduled Inspection Continuing from Phase i-1

Considering the first phase of the mission, all components are known to begin in the working state and so the initial unavailability of an irrelevant component will be zero. As the mission progresses it is possible that the component will not begin a phase in the working state, and the initial component unavailability in a phase i will be greater than zero.

Using the derivations in Section 5.3.1 of component failure probability with time for a component beginning a phase i with initial unavailability greater than zero (equation 5.38), it is possible to obtain the unavailability of the component with time up until the first inspection point in a repairable phase. The unavailability of an irrelevant component c in phase i is given as a function of time from the start of phase i, at $t=t_{i-1}$, to the first inspection point by equation (7.12), and from the first inspection point to the end of the phase, at $t=t_i$, by equation (7.13).

$$q_c(t) = \begin{cases} 1-a_c(t_{i-1})e^{-\lambda_c(t-t_{i-1})} \text{ for } t_{i-1} \leq t \leq (t_{n_{(i-1)\max}} + \theta_c) & (7.12) \\ 1-e^{-\lambda_c[t-(n-1)\theta]} \quad \text{for } (t_{n_{(i-1)\max}} + (n\text{-}1)\theta_c) \leq t \leq (t_{n_{(i-1)\max}} + n\theta_c) \;\; n = 2,3,\ldots,n_{i\max}+1 & (7.13) \end{cases}$$

where $t_{n_{(i-1)\max}} = t_{i-1}$ if the first scheduled inspection point is at $t = t_{i-1}$

Since the component is not required in the phase, the reliability of the component over the phase duration is not important. The only requirement is the probability of the component residing in the working or failed state at the end of the phase for transition into the next phase. If the phase finishes before the first inspection point, the unavailability of the component at the end of the phase i is given by equation (7.14).

$$q_c(t_i) = 1 - a_c(t_{i-1})e^{-\lambda_c(t_i-t_{i-1})} \tag{7.14}$$

If phase i finishes after the first inspection point, the final unavailability of the component is found by equation (7.15).

$$q_c(t_i) = 1 - e^{-\lambda_c[t_i-(t_{n_{(i-1)\max}}+n_{i\max}\theta)]} \tag{7.15}$$

where $t_{n_{(i-1)\max}} = t_{i-1}$ if the first scheduled inspection point in phase i is at $t = t_{i-1}$

The initial component *c* availability in phase *i*, $a_c(t_{i-1})$, is obtained depending on the configuration of the previous phase. If the previous phase *i*-1 was non-repairable and component *c* did NOT contribute to a sequential failure relationship (Section 7.2.2.3), regardless of whether the component was required in the previous phase, the probability that *c* is available at the end of phase *i-1* is obtained from equation (5.39) in equation (7.16).

$$a_c(t_{i-1}) = a_c(t_{i-2})e^{-\lambda_c(t_{i-1}-t_{i-2})} \qquad (7.16)$$

where $a_c(t_{i-2})$ is the initial availability of component *c* in phase *i-1*

In the case that the previous phase *i-1* was non-repairable and component *c* contributed to a sequential failure relationship, or if the previous phase *i-1* was repairable and component *c* was required in the phase configuration, the probability that *c* is in the working state at the end of phase *i-1* is obtained using the previous phase Markov model in equation (7.17).

$$a_c(t_{i-1}) = \sum P_j(t_{i-1}) \qquad (7.17)$$

where *j* are successful phase *i-1* states with contribution of component *c* working

If the previous phase was repairable but component *c* was not required in the phase configuration, the final component availability would be obtained using equation (7.14) or (7.15).

In the same way as presented in Section 5.2.2, the probability of the reduced set of Markov states may be multiplied by the unavailability and availability of irrelevant components at the end of a phase to produce a full set of transition model state probabilities for input to the next phase. If an irrelevant component failure acts as an enabler or is not used in the following phase, the unavailability of the component relates to the initial unrevealed failure state. If an irrelevant component failure acts as an initiating event in the following phase, the unavailability relates to the initial revealed failure state. Since the component does not contribute to any NPS sequential minimal cut sets in later phases, the order of failure of the component in the transition model is not important. The only requirement is the probability that the component is in the working or failed state at the end of the phase.

The failure of a component that is not required during a non-repairable phase and does not contribute to any NPS sequential minimal cut sets in later phases is modelled as described in Section 5.3.1.

Once any irrelevent components are removed from the state model and the required system states for a phase have been identified, the reduced Markov models for each of the individual phases may be solved.

7.2.2.3 Combined Fault Tree and Markov Method

If a phase is non-repairable, other methods may be investigated for solution. Fault tree methods allow the calculation of system unreliability for systems comprising of only non-repairable components. It is possible to combine solutions of event probability for static and dynamic gate types to calculate phase unreliability.

It can be seen that phase 3 in example Figure 7.1 consists of only non-repairable components. However the fault tree representation of the system uses both static and dynamic gate types to show the logic of the top event occurrence of phase 3 failure. A static gate may be solved using simple fault tree analysis. Since a dynamic gate involves sequential failures, treating a priority-AND gate as a normal AND gate would give a pessimistic result. Solution of the top event occurrence probability including a dynamic gate requires a method that allows for dependencies in a system such as a Markov model.

A combination of fault tree and Markov methods may be implemented for situations where components that are input to static gates of a non-repairable phase do not contribute to any NPS sequential minimal cut sets of later phases. If a component is known to contribute to a later NPS sequential minimal cut set, the ordering of the component with respect to the other components would be required later in the mission. The component could not be treated independently from the components input to dynamic gates and eliminated from the Markov model. In this example, component C does not contribute to any later NPS sequential minimal cut sets, and so it is possible to model the component failure probability using fault tree analysis.

Figure 7.14 shows the labelling of the output events for gates in phase 3 of Figure 7.1.

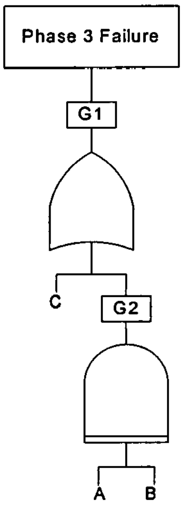


Figure 7.14 Phase 2 Representation

The top event occurrence, phase 3 failure, is the output of gate G1 and can be represented by logic equation (7.18).

$$G1 = C+G2 \tag{7.18}$$

Gate G2 is a dynamic gate which since it is independent of the rest of the fault tree can be considered as a separate subsystem for analysis. The dynamic nature of G2 means that the probability of the system residing in a state that allows occurrence of G2 must be found using a Markov Model. The Markov model would be represented using the state listing in Table 7.10 and is given in Figure 7.15.

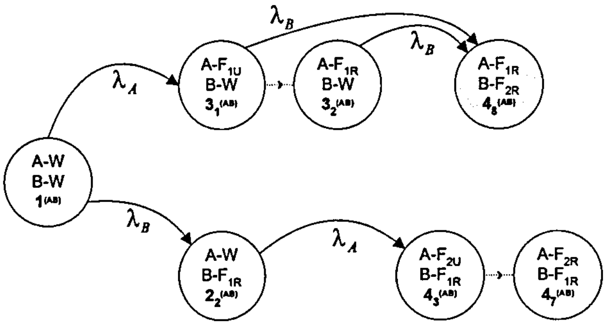

λ_B
λ_B
λ_A
A-F$_{1U}$ B-W $3_1^{(AB)}$
A-F$_{1R}$ B-W $3_2^{(AB)}$
A-F$_{1R}$ B-F$_{2R}$ $4_8^{(AB)}$
A-W B-W $1^{(AB)}$
λ_B
λ_A
A-W B-F$_{1R}$ $2_2^{(AB)}$
A-F$_{2U}$ B-F$_{1R}$ $4_3^{(AB)}$
A-F$_{2R}$ B-F$_{1R}$ $4_7^{(AB)}$

Figure 7.15 Markov Model of Dynamic Gate G2

The final state probabilities from phase 2 may be combined to give a set of initial reduced Markov system state probabilities for phase 3 by removing component C from the transition model. The solution of the set of differential equations for this model over the phase 3 duration results in a final set of system state probabilities at

$t=t_3$. The probability that gate G2 fails and thus contributes to the top event occurrence is found by the probability that the enabling event, component A failure, occurs prior to the initiating event of component B failure. This is represented by the probability that the system resides in state $4_8^{(AB)}$ in Figure 7.15 at the end of the phase. The probability of event G2 is found by equation (7.19).

$$P(G2) = P_{4_8}^{(AB)}(t_3) \tag{7.19}$$

Equation (7.18) demonstrates the relationship between the occurrence of the top event, G1, and the dynamic gate occurrence, G2. Once the probability of occurrence of G2 has been calculated it is possible to incorporate the results into the event of the static gate G1 occurrence.

Since component C failure is an initiating event, it is automatically revealed. The probability that component C fails during phase 3 and thus contributes to the top event occurrence is required. This is found by fault tree analysis as derived in Section 5.3.1 (equation (5.40)), and is given by equations (7.20).

$$\begin{aligned} q_{C_3} &= a_C(t_2)\left(1 - e^{-\lambda_C(t_3-t_2)}\right) \\ a_{C_3} &= 1 - q_{C_3} \end{aligned} \tag{7.20}$$

where $a_C(t_2)$ is found by the contribution of all transition model state probabilities with component C working at the end of the previous phase.

The results can then be combined to allow calculation of the probability of the top event occurrence, G1, in equation (7.21).

$$P(G1) = q_{C_3} + P(G2) - (q_{C_3} \cdot P(G2)) \tag{7.21}$$

7.2.2.4 Final Reduced Markov Model Solution Process

The final solution process for a phased mission system where all sequential cut sets are NPS can be summarised in algorithmic form in Figure 7.16. The proposed method for solution to a mission comprising of both non-repairable and repairable continuous phases with only NPS sequential minimal cut sets and scheduled inspection will be demonstrated in more detail by application to the example given in Figure 7.1.

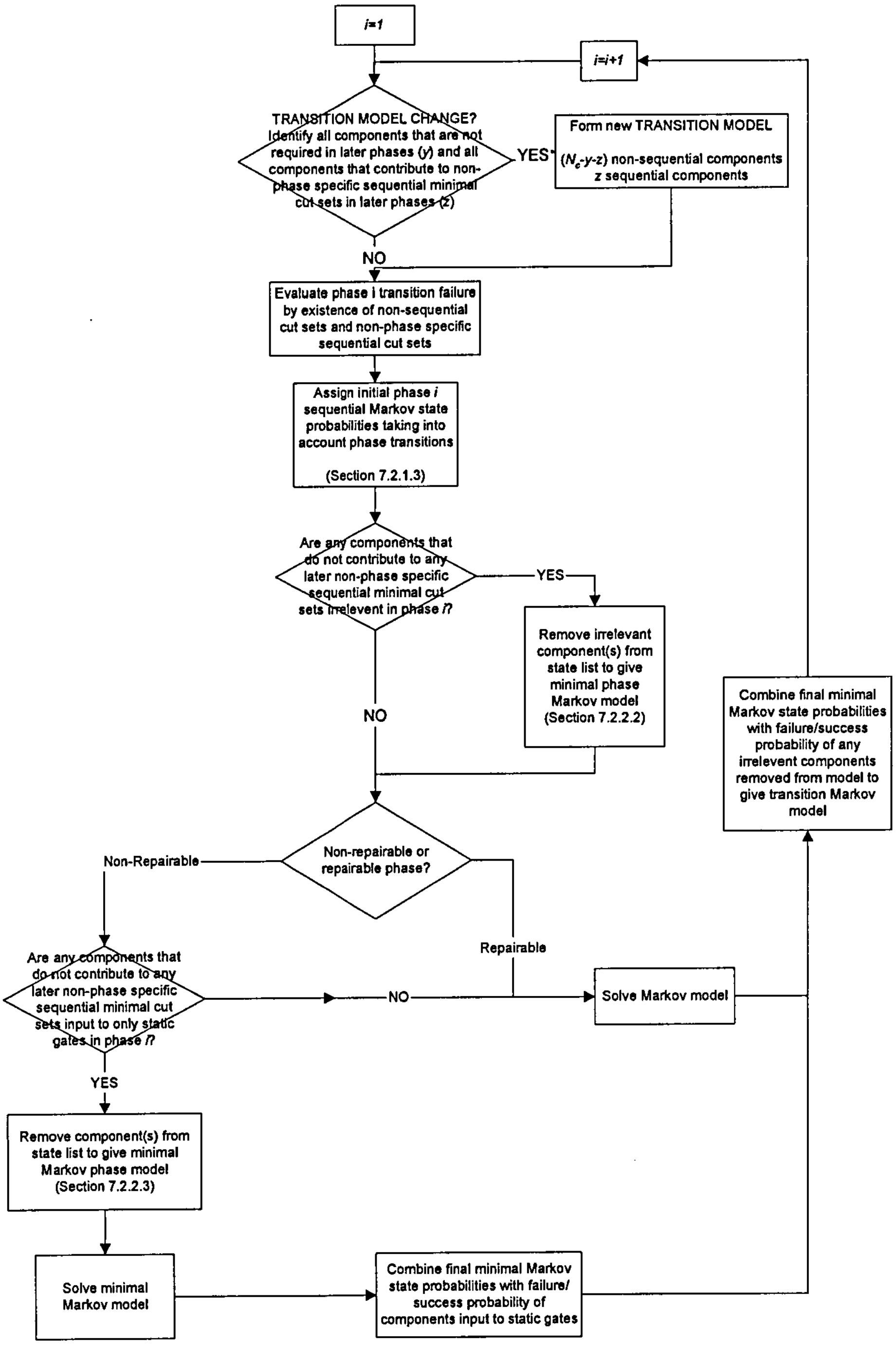

i=1
i=i+1
TRANSITION MODEL CHANGE? Identify all components that are not required in later phases (y) and all components that contribute to non-phase specific sequential minimal cut sets in later phases (z)
YES
Form new TRANSITION MODEL
(N_c-y-z) non-sequential components
z sequential components
NO
Evaluate phase i transition failure by existence of non-sequential cut sets and non-phase specific sequential cut sets
Assign initial phase i sequential Markov state probabilities taking into account phase transitions
(Section 7.2.1.3)
Are any components that do not contribute to any later non-phase specific sequential minimal cut sets irrelevent in phase i?
YES
Remove irrelevant component(s) from state list to give minimal phase Markov model (Section 7.2.2.2)
NO
Combine final minimal Markov state probabilities with failure/success probability of any irrelevent components removed from model to give transition Markov model
Non-Repairable
Non-repairable or repairable phase?
Repairable
Are any components that do not contribute to any later non-phase specific sequential minimal cut sets input to only static gates in phase i?
NO
Solve Markov model
YES
Remove component(s) from state list to give minimal Markov phase model (Section 7.2.2.3)
Solve minimal Markov model
Combine final minimal Markov state probabilities with failure/ success probability of components input to static gates

Figure 7.16 Algorithm to Solve a Phased Mission System with only NPS Sequential Failure Relationships

Phase 1

The important things to notice are that,

- Component C is not required in the phase, but will be used in later phases.
- There is a sequential relationship between components A and B.

Since component C is not required during this phase and does not contribute to any later NPS sequential cut sets, it can be removed from the sequential ordering of the Markov model and the initial transition model is defined by the state listing in Table 7.8. In this first phase, component C can be eliminated from the Markov model completely to reduce computational time and model complexity as discussed in Section 7.2.2.2.

The initial sequential phase 1 states must represent the sequential failure relationship between components A and B, and are listed in Table 7.10. Referring to the rules as given in Sections 7.2.1.1 it is possible to identify all system states that are not required in phase 1. There is only one minimal cut set that contributes to the occurrence of the top event, AB. However in order to cause phase 1 failure, the components must fail in the order of A first and B second. Failure of component B only ever acts as an initiator and so can never occur unrevealed. This eliminates states $2_1^{(AB)}$, $4_1^{(AB)}$, $4_2^{(AB)}$, $4_5^{(AB)}$, and $4_6^{(AB)}$ from the model. If component A fails before component B fails, the enabling event allows the initiating event to cause phase 1 failure. This automatically reveals the fact that component A has failed and thus state $4_4^{(AB)}$ is also an impossible system state for this phase. The remaining states $1^{(AB)}$, $2_2^{(AB)}$, $3_1^{(AB)}$, $3_2^{(AB)}$, $4_3^{(AB)}$, $4_7^{(AB)}$, and $4_8^{(AB)}$, are all possible system states in phase 1 as shown in Figure 7.11.

It is assumed that all components begin the mission in the working state and so the probability that the system resides in state $1^{(AB)}$ is assigned the value of 1.0 whilst all other non-sequential states are assigned an initial probability of 0.0.

In the same way as in Section 5.2.3, the set of differential equations for this reduced Markov model are solved over the duration of Phase 1. Although states $4_3^{(AB)}$ and $4_7^{(AB)}$ represent both of the components in the failed state, the phase can still continue and restoration of the components is allowed. Since the only system state that causes phase termination is state $4_8^{(AB)}$, phase 1 reliability can be obtained by equation (7.22).

$$R(t_1) = 1 - P_{4_8}^{(AB)}(t_1) \tag{7.22}$$

Phase 2

The second phase of this mission introduces component C which until now has not been required. Since the component was known to be working at the start of the mission, the unavailability of component C at the end of the repairable first phase is found depending on the appropriate situation:

- Scheduled Inspection – phase 1 ends before first scheduled inspection point.
  Use: equation (7.14) where *i=1*

- Scheduled Inspection – phase 1 ends after first scheduled inspection
  Use: equation (7.15) where *i=1* and $t_{n_{(i-1)\max}} = 0$

- Constant Monitoring – component C failure automatically revealed (equation 5.46)
  Use: $q_C(t_i) = \frac{\lambda_C}{\lambda_C + \upsilon_C} + \frac{e^{-(\lambda_C+\upsilon_C)(t_i - t_{i-1})}}{\lambda_C + \upsilon_C}\left[\upsilon_C q_C(t_{i-1}) - \lambda_C a_C(t_{i-1})\right]$ where *i=1*

The availability of component C at the end of phase 1 can be found by $a_C(t_1)$, where $a_C(t_1) = 1 - q_C(t_1)$.

The beginning of a new phase requires a set of initial transition model system state probabilities. To calculate the initial system state probabilities in phase 2, the probability that the system resides in any working transition model state (Table 7.8) at the end of phase 1 is required.

Since component C was excluded from the phase 1 Markov model, the probability of component C being in the working or failed state at the end of the phase must now be incorporated. The probability that component C is in the failed and working state at the end of phase 1 is included using the calculation method for the unavailability of irrelevant components at the end of a phase (7.2.2.2). Component C is assumed to be maintained under scheduled inspection in phase 1. Since component C was not required in phase 1 and acts as an initiator in phase 2, the final phase 1 failure is classed as revealed. The final revealed failure probability of component C is obtained using equations (7.14) or (7.15). The transition model state probabilities at the end of the first phase are obtained from the working states of the reduced Markov model in Figure 7.11, as shown in Table 7.11.

Transition Model State Ref	Component States			Reduced Markov Model (Figure 7.10) with Component C Final State Probability
	A	B	C	
$1^{(ABC)}$	0	0	0	$P_{1}^{(AB)}(t_1)\cdot a_C(t_1)$
$2_{1}^{(ABC)}$	0	0	1_{U}	0
$2_{2}^{(ABC)}$	0	0	1_{R}	$P_{1}^{(AB)}(t_1)\cdot q_C(t_1)$
$3_{2}^{(ABC)}$	0	1_{1R}	0	$P_{2_2}^{(AB)}(t_1)\cdot a_C(t_1)$
$4_{5,6}^{(ABC)}$	0	1_{1R}	1_{U}	0
$4_{7,8}^{(ABC)}$	0	1_{1R}	1_{R}	$P_{2_2}^{(AB)}(t_1)\cdot q_C(t_1)$
$5_{1}^{(ABC)}$	1_{1U}	0	0	$P_{3_1}^{(AB)}(t_1)\cdot a_C(t_1)$
$5_{2}^{(ABC)}$	1_{1R}	0	0	$P_{3_2}^{(AB)}(t_1)\cdot a_C(t_1)$
$6_{1,2}^{(ABC)}$	1_{1U}	0	1_{U}	0
$6_{3,4}^{(ABC)}$	1_{1U}	0	1_{R}	$P_{3_1}^{(AB)}(t_1)\cdot q_C(t_1)$
$6_{5,6}^{(ABC)}$	1_{1R}	0	1_{U}	0
$6_{7,8}^{(ABC)}$	1_{1R}	0	1_{R}	$P_{3_2}^{(AB)}(t_1)\cdot q_C(t_1)$
$7_{3}^{(ABC)}$	1_{2U}	1_{1R}	0	$P_{4_3}^{(AB)}(t_1)\cdot a_C(t_1)$
$7_{7}^{(ABC)}$	1_{2R}	1_{1R}	0	$P_{4_7}^{(AB)}(t_1)\cdot a_C(t_1)$
$7_{8}^{(ABC)}$	1_{1R}	1_{2R}	0	0
$8_{13,15,16}^{(ABC)}$	1_{2U}	1_{1R}	1_{U}	0
$8_{19,21,22}^{(ABC)}$	1_{2U}	1_{1R}	1_{R}	$P_{4_3}^{(AB)}(t_1)\cdot q_C(t_1)$
$8_{37,39,40}^{(ABC)}$	1_{2R}	1_{1R}	1_{U}	0
$8_{38,41}^{(ABC)}$	1_{1R}	1_{2R}	1_{U}	0
$8_{43,45,46}^{(ABC)}$	1_{2R}	1_{1R}	1_{R}	$P_{4_7}^{(AB)}(t_1)\cdot q_C(t_1)$
$8_{44,47,48}^{(ABC)}$	1_{1R}	1_{2R}	1_{R}	0

Table 7.11 Phase 1 Final Transition Model State Probabilities

As described in Section 7.2.1.3, the enabling event of component A failure in phase 1 becomes an initiating event in phase 2. At the transition point between phases 1 and 2, the failure of component A will automatically become revealed. The probabilities of all transition model states (Table 7.11) representative of component A in the unrevealed state must be re-assigned to contribute to the identical system state with component A in the revealed state. The final re-assigned phase 1 transition model state probabilities are given in equations (7.23).

$$
\begin{aligned}
&P_{5_2}^{(ABC)}(t_1) = P_{5_1}^{(ABC)}(t_1) + P_{5_2}^{(ABC)}(t_1) && P_{5_1}^{(ABC)}(t_1) \to 0 \\
&P_{6_{7,8}}^{(ABC)}(t_1) = P_{6_{3,4}}^{(ABC)}(t_1) + P_{6_{7,8}}^{(ABC)}(t_1) && P_{6_{3,4}}^{(ABC)}(t_1) \to 0 \\
&P_{7_7}^{(ABC)}(t_1) = P_{7_3}^{(ABC)}(t_1) + P_{7_7}^{(ABC)}(t_1) && P_{7_3}^{(ABC)}(t_1) \to 0 \\
&P_{8_{43,45,46}}^{(ABC)}(t_1) = P_{8_{19,21,22}}^{(ABC)}(t_1) + P_{8_{43,45,46}}^{(ABC)}(t_1) && P_{8_{19,21,22}}^{(ABC)}(t_1) \to 0
\end{aligned}
\tag{7.23}
$$

Transition failure will occur if the system resides in any successful phase 1 state that represents the existence of a phase 2 minimal cut set. The phase 2 minimal cut sets are {A, C} and {B, C}, thus phase 2 transition failure will occur if the system resides in a transition model state with either components A and C, or B and C in the failed state at the end of phase 1, and is given in equation (7.5).

Since phase 2 is repairable and requires all three components, the Markov model shown in Figure 7.6 is solved over the duration of phase 2, $[t_1, t_2)$, with initial state probabilities given in Table 7.11 and redefined in equations (7.23). Any states that cause phase 1 or phase 2 failure are assigned an initial state probability value of zero. The reliability of phase 2 is found by the sum of the probabilities that the system resides in a successful state at the end of the phase ($t=t_2$) in equation (7.7).

Phase 3

Since the phase 2 Markov model required the full transition model states, the state probabilities can be passed directly to phase 3, and all states that caused phase 2 failure are assigned a probability of zero on entering phase 3. All components were required in phase 2 and so the final failure probabilities are classed as revealed. Transition failure will occur if the system resides in a working phase 2 state representing the existence of a phase 3 minimal cut set. There are two phase 3 minimal cut sets; non-sequential {C}, and sequential $\{A^{(E)},B^{(I)}\}$. Transition failure will occur if the system resides in a successful final phase 2 state with component C in the failed state ($2_2^{(ABC)}$), or in a state representative of the failure sequence of components A then B ($7_8^{(ABC)}$). In this case there are no successful phase 2 states that become unreachable and thus contribute to the transition failure in phase 3 (Section 7.2.1.3). The phase 3 transition failure is given by equation (7.8).

Since the third phase consists of only non-repairable components, the method described in Section 7.2.2.3 can be applied for solution. Component C is only input into a static gate and does not contribute to any later NPS sequential minimal cut sets, thus can be removed from the dynamic Markov model of the phase. To solve this reduced Markov model (Figure 7.15) we are only interested in the states of components A and B at the start of the third phase. The successful transition model states listed in Table 7.11 must be reduced to represent only the states of components

A and B and are given in Table 7.12. For example, state $7_7^{(ABC)}$ in Table 7.11 represents the event that component B fails revealed followed by component A revealed failure. Since component C is not required in the model, this state is equivalent to state $4_7^{(AB)}$ in Table 7.12 with the same failure combination of components A and B. All states that cause phase 3 failure are assigned an initial state probability of zero.

State Ref	Component States		Combination of Initial Transition State Probabilities (Table 7.11)
	A	B	
$1^{(AB)}$	0	0	$P_1^{(ABC)}(t_2)$
$2_2^{(AB)}$	0	1_{1R}	$P_{3_2}^{(ABC)}(t_2)$
$3_1^{(AB)}$	1_{1U}	0	0
$3_2^{(AB)}$	1_{1R}	0	$P_{5_2}^{(ABC)}(t_2)$
$4_3^{(AB)}$	1_{2U}	1_{1R}	0
$4_7^{(AB)}$	1_{2R}	1_{1R}	$P_{7_7}^{(ABC)}(t_2)$
$4_8^{(AB)}$	1_{1R}	1_{2R}	0

Table 7.12 Phase 3 Initial Non-Sequential State Probabilities

The set of Markov differential equations can now be solved over the duration of phase 3. The end system state probabilities can be combined with the unavailability of component C over the duration of the phase to calculate the reliability of phase 3. Using equations (7.19), (7.20) and (7.21), the reliability of phase 3 is expressed in equation (7.24)

$$R(t_3) = 1 - (q_{C_3} + P_{4_8}^{(AB)}(t_3) - (P_{4_8}^{(AB)}(t_3) \cdot q_{C_3})) \qquad (7.24)$$

where $q_{C_3} = a_C(t_2)(1 - e^{-\lambda_C(t_3 - t_2)})$

and (Figure 7.6) $a_C(t_2) = P_1^{(ABC)}(t_2) + P_{3_2}^{(ABC)}(t_2) + P_{5_2}^{(ABC)}(t_2) + P_{7_7}^{(ABC)}(t_2) + P_{7_8}^{(ABC)}(t_2)$

In many practical situations it is likely that a system will comprise of phase specific sequential cut sets. The inclusion of phase specific sequential cut sets is discussed in the following sections.

7.3 Phase Specific Initiators

This section considers the possibility of phase specific (PS) initiating events. In such a situation, failure during a phase will only be caused if the PS initiating event of a sequential minimal cut set occurs during the phase in question. If a PS sequential minimal cut set exists at the start of a phase, it will not contribute to the phase failure. This allows further state reduction between phases to achieve a minimal transition Markov model. The possibility of the minimisation of the model allows us to reduce the size of the phase transition matrices and decrease computational time.

Consider the example shown in Figure 7.1 where the initiating events of the sequential minimal cut sets are PS. The phase failure criteria are given in Figure 7.17.

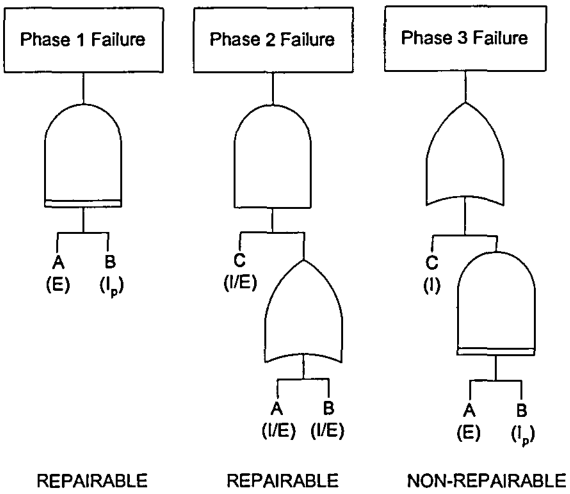


Figure 7.17 Mission with Phase Specific Initiating Events

7.3.1 Phase Transition Model

The transition model was discussed for only NPS sequential minimal cut sets in Section 7.2.2.1. This is the minimal model required at a particular point in the mission, and can be redefined at each transition point. All components that are not required for the remaining phases can be removed from the transition model. Any further components that do not contribute to any NPS sequential minimal cut sets in later phases can be eliminated from the ordering scheme of the most recent transition model. Since PS sequential minimal cut sets can only cause phase failure if the initiating event occurs during a particular phase, the transition model can be expanded at the start of the phase to include the order of failure of the components contributing to the cut set. At the end of the phase the expanded model is reduced back to the transition model for input to the next phase.

At the start of the mission in Figure 7.17, it can be seen that none of the components contribute to a NPS sequential cut set during any phase. The transition model is defined by eliminating the failure ordering of all components in the Markov model, as discussed in Section 7.2.1.2, from the full state listing in Table 7.6. This is given in Table 7.13.

It can be seen that the removal of the order of failure of all components has produced multiple states representing the same failure mode in the model. It is possible to combine all states with the same combination of component failures into a single state. The final combined states of the transition model are given in Table 7.14.

Since none of the transition model states in Table 7.14 represent component failure ordering, this is the minimal transition model possible and is defined as non-sequential for all components. No further minimisation can be implemented due to components not contributing to NPS sequential minimal cut sets at later phase boundaries. Also, since all components are required in phases 2 and 3, no components can be completely removed from the transition model at any stage.

PS sequential minimal cut sets must be identified at the start of each phase. The transition Markov model states between each phase must be expanded to allow for sequential failures during the proceeding phase.

State Ref	Component States			Phase 1	Phase 2	Phase 3
	A	B	C			
$1^{(ABC)}$	0	0	0	W	W	W
$2_1^{(ABC)}$	0	0	1_U	W	R	R
$2_2^{(ABC)}$	0	0	1_R	W	W	F
$3_2^{(ABC)}$	0	1_R	0	W	W	W
$4_5^{(ABC)}$	0	1_R	1_U	W	R	R
$4_6^{(ABC)}$	0	1_R	1_U	W	R	R
$4_7^{(ABC)}$	0	1_R	1_R	W	F	R
$4_8^{(ABC)}$	0	1_R	1_R	W	F	F
$5_1^{(ABC)}$	1_U	0	0	W	R	W
$5_2^{(ABC)}$	1_R	0	0	W	W	W
$6_1^{(ABC)}$	1_U	0	1_U	W	R	R
$6_2^{(ABC)}$	1_U	0	1_U	W	R	R
$6_3^{(ABC)}$	1_U	0	1_R	W	R	R
$6_4^{(ABC)}$	1_U	0	1_R	W	R	F
$6_5^{(ABC)}$	1_R	0	1_U	W	R	R
$6_6^{(ABC)}$	1_R	0	1_U	W	R	R
$6_7^{(ABC)}$	1_R	0	1_R	W	W	R
$6_8^{(ABC)}$	1_R	0	1_R	W	W	F
$7_3^{(ABC)}$	1_U	1_R	0	W	R	W
$7_7^{(ABC)}$	1_R	1_R	0	W	F	W
$7_8^{(ABC)}$	1_R	1_R	0	F	F	F
$8_{13}^{(ABC)}$	1_U	1_R	1_U	W	R	R
$8_{15}^{(ABC)}$	1_U	1_R	1_U	W	R	R
$8_{16}^{(ABC)}$	1_U	1_R	1_U	W	R	R
$8_{19}^{(ABC)}$	1_U	1_R	1_R	W	R	R
$8_{21}^{(ABC)}$	1_U	1_R	1_R	W	R	R
$8_{22}^{(ABC)}$	1_U	1_R	1_R	W	R	F
$8_{37}^{(ABC)}$	1_R	1_R	1_U	W	R	R
$8_{38}^{(ABC)}$	1_R	1_R	1_U	F	R	R
$8_{39}^{(ABC)}$	1_R	1_R	1_U	W	R	R
$8_{40}^{(ABC)}$	1_R	1_R	1_U	W	R	R
$8_{41}^{(ABC)}$	1_R	1_R	1_U	F	R	R
$8_{43}^{(ABC)}$	1_R	1_R	1_R	W	R	R
$8_{44}^{(ABC)}$	1_R	1_R	1_R	F	R	R
$8_{45}^{(ABC)}$	1_R	1_R	1_R	W	R	R
$8_{46}^{(ABC)}$	1_R	1_R	1_R	W	F	F
$8_{47}^{(ABC)}$	1_R	1_R	1_R	F	R	R
$8_{48}^{(ABC)}$	1_R	1_R	1_R	R	F	R

Table 7.13 Transition Model States for 3-Component System Example with PS Sequential Failures and Scheduled Inspection

Transition	Component States		
Model	A	B	C
$1^{(ABC)}$	0	0	0
$2_1^{(ABC)}$	0	0	1_U
$2_2^{(ABC)}$	0	0	1_R
$3_2^{(ABC)}$	0	1_R	0
$4_{5,6}^{(ABC)}$	0	1_R	1_U
$4_{7,8}^{(ABC)}$	0	1_R	1_R
$5_1^{(ABC)}$	1_U	0	0
$5_2^{(ABC)}$	1_R	0	0
$6_{1,2}^{(ABC)}$	1_U	0	1_U
$6_{3,4}^{(ABC)}$	1_U	0	1_R
$6_{5,6}^{(ABC)}$	1_R	0	1_U
$6_{7,8}^{(ABC)}$	1_R	0	1_R
$7_3^{(ABC)}$	1_U	1_R	0
$7_{7,8}^{(ABC)}$	1_R	1_R	0
$8_{13,15,16}^{(ABC)}$	1_U	1_R	1_U
$8_{19,21,22}^{(ABC)}$	1_U	1_R	1_R
$8_{37,38,39,40,41}^{(ABC)}$	1_R	1_R	1_U
$8_{43,44,45,46,47,48}^{(ABC)}$	1_R	1_R	1_R

Table 7.14 Transition Model State Listing

7.3.2 Phase Transitions for PS Sequential Cut Sets

When considering PS sequential minimal cut sets, it is not always possible to assign the probability of the system residing in a particular state to the same state in the next phase. Where phases contain dynamic gates, the system level outcome depends on the order of component failure. In some cases an initiating event may be PS and only relevant to the phase in which it occurs.

For example when considering the 3-phased mission in Figure 7.17, it is seen that there is a PS sequential failure relationship between components A and B (A must fail before B) in phase 3 which is reflected in the phase failure modes of the reduced Markov model in Figure 7.15. The enabling event of component A failure could have occurred in any phase prior to and including phase 3, however for this sequential cut set to occur, the PS initiating event of component B failure must occur during phase 3.

If the system reaches the state in phase 2 where component C is working and components A and B have failed in the order of A then B with both failures revealed, phase 2 failure will not occur. The state representative of this failure relationship is state $7_8^{(ABC)}$ in Table 7.8. If the same failure sequence occurred in phase 3, however, this would cause system failure.

Using the method for only NPS initiators as demonstrated in Section 7.2, if this state were achieved in phase 2 then failure would occur on transition to phase 3 (due to the NPS initiator) where it satisfies the phase failure requirements and state $7_8^{(ABC)}$ represents the absorbing failure state $4_8^{(AB)}$ of phase 3 (Figure 7.15). However, as failure of component B in phase 3 is a PS event this is not now the situation. Since the failure sequence occurred in phase 2, it is not representative of the same failure state in phase 3. Misrepresentation occurs if the two states are taken to be the same in the two phases. This state only results in failure in phase 3 if the initiating event, B, occurs in phase 3 not on phase transition if it has occurred previously.

In such cases, a temporary state is introduced to the phase model that represents the same combination of component failure conditions but makes a distinction as to the failure mode of the state. This state cannot occur during the phase, but can exist at the start of the phase. Thus no state transitions into the state are possible during the phase, however state transitions may be made out of the state during the phase. In the event that state transitions are possible out of a temporary state, the correct destination state must be identified with the appropriate failure mode. For example, considering the phase 3 Markov model in Figure 7.15, the only state that causes phase failure due to just the occurrence of the PS sequential minimal cut set is state $4_8^{(AB)}$. A temporary state is introduced, $4_{8*}^{(AB)}$, to represent the same component failure combination but with a failure outcome that does not cause phase failure. No state transitions are possible into the state during phase 3, and in this case since the phase is non-repairable and component C is not represented in the model, no transitions are possible out of the state. The probability of the system residing in this temporary state will remain constant until the end of the phase. This is demonstrated in Figure 7.18.

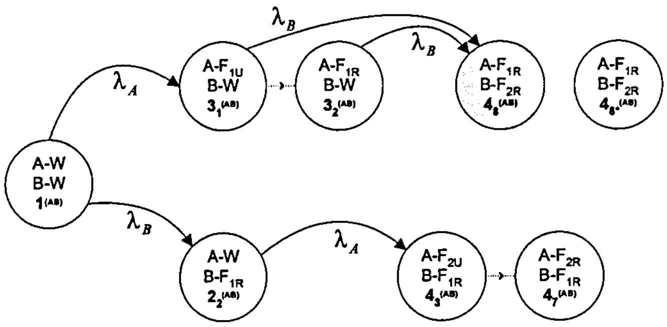


Figure 7.18 Reduced Phase 3 Markov Model

The reliability of phase 3 remains as given in equation (7.24). If there were later phases in the mission, the probability that the system resides in the original state with components A and B failed in the order of A then B at the end of the phase becomes equal to the temporary state ($4_{8*}^{(AB)}$) (equation (7.25)) for input to the next phase, and the temporary state is removed.

$$P_{4_8}^{(AB)}(t_3) = P_{4_{8*}}^{(AB)}(t_3) \qquad\qquad P_{4_{8*}}^{(AB)}(t_3) \rightarrow 0 \qquad\qquad (7.25)$$

7.3.3 Final Solution Process

The methods presented in Sections 7.2.2.2 and 7.2.2.3 can again be applied to systems comprising of PS sequential minimal cut sets as long as the failure order of components removed from the model is not required for any later NPS sequential minimal cut sets. The general method to solve a phased mission system comprising of PS and NPS initiating events is summarised in Figure 7.19.

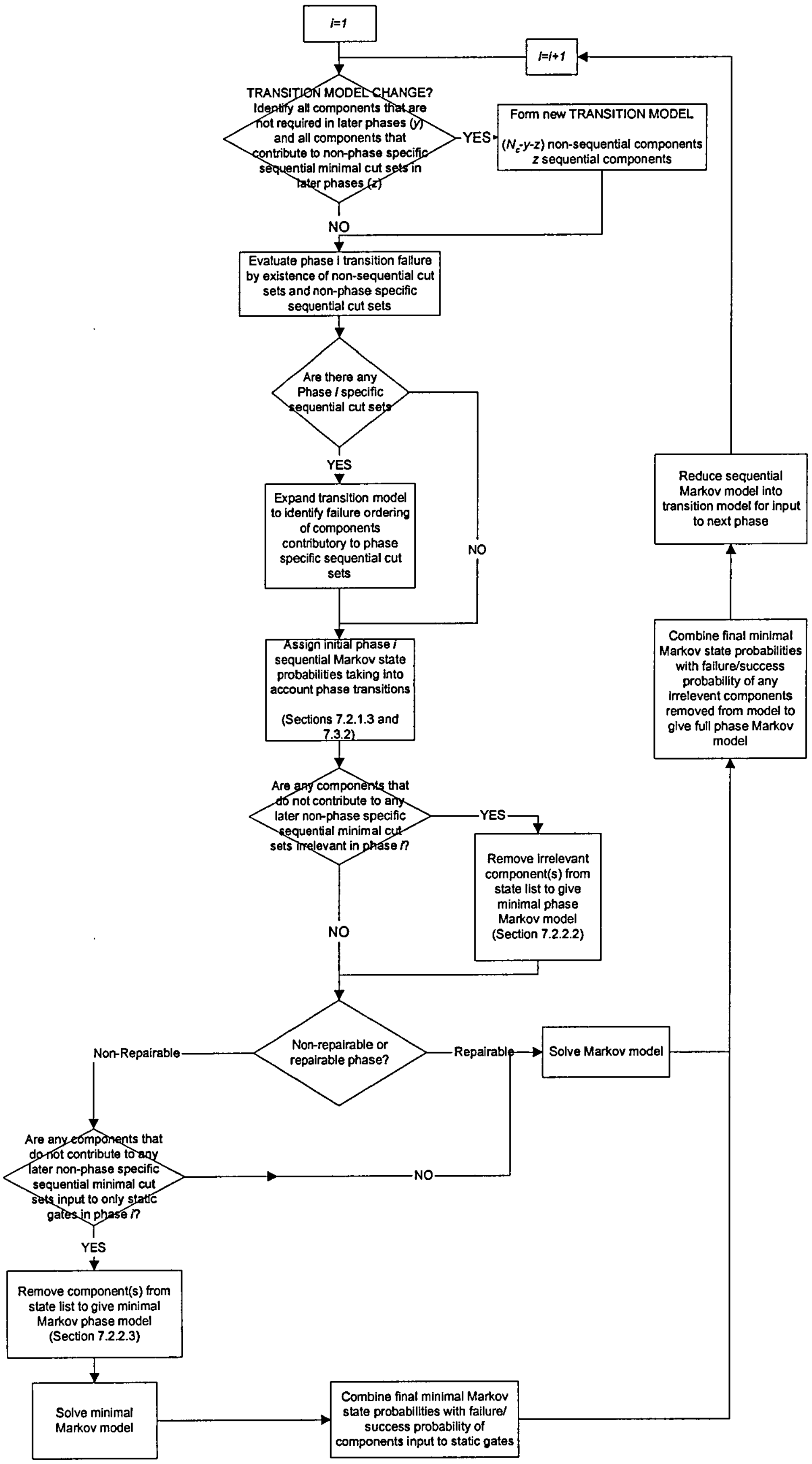

i=1
i=i+1
TRANSITION MODEL CHANGE? Identify all components that are not required in later phases (y) and all components that contribute to non-phase specific sequential minimal cut sets in later phases (z)
YES
Form new TRANSITION MODEL
(N_c-y-z) non-sequential components
z sequential components
NO
Evaluate phase I transition failure by existence of non-sequential cut sets and non-phase specific sequential cut sets
Are there any Phase I specific sequential cut sets
YES
Expand transition model to identify failure ordering of components contributory to phase specific sequential cut sets
NO
Assign initial phase i sequential Markov state probabilities taking into account phase transitions
(Sections 7.2.1.3 and 7.3.2)
Are any components that do not contribute to any later non-phase specific sequential minimal cut sets irrelevant in phase i?
YES
Remove irrelevant component(s) from state list to give minimal phase Markov model (Section 7.2.2.2)
NO
Non-Repairable
Non-repairable or repairable phase?
Repairable
Solve Markov model
Are any components that do not contribute to any later non-phase specific sequential minimal cut sets input to only static gates in phase i?
NO
YES
Remove component(s) from state list to give minimal Markov phase model (Section 7.2.2.3)
Solve minimal Markov model
Combine final minimal Markov state probabilities with failure/ success probability of components input to static gates
Combine final minimal Markov state probabilities with failure/success probability of any irrelevent components removed from model to give full phase Markov model
Reduce sequential Markov model into transition model for input to next phase

Figure 7.19 Algorithm to Demonstrate Solution to a Phased Mission System with both PS and NPS Sequential Failure Relationships

This may be applied to the example in Figure 7.17 in the following way:

Phase 1

Since no components contribute to any later NPS sequential cut sets, the failure ordering of all components can be removed from the full Markov model to reduce computational time and model complexity as discussed in Section 7.3.1. The transition model is defined by the non-sequential state listing in Table 7.14.

The initial sequential phase 1 states must represent the sequential failure relationship between components A and B, and are listed in Table 7.10. By application of the rules to identify all system states that are not required in phase 1 (Section 7.2.1.1), the possible states are $1^{(AB)}$, $2_2^{(AB)}$, $3_1^{(AB)}$, $3_2^{(AB)}$, $4_3^{(AB)}$, $4_7^{(AB)}$, and $4_8^{(AB)}$, and are shown in the phase 1 Markov model of Figure 7.11.

We assume that all components begin the mission in the working state and so the probability that the system resides in state $1^{(AB)}$ is assigned the value of 1.0 whilst all other non-sequential states are assigned an initial probability of 0.0. Since the only system state that causes phase termination is state $4_8^{(AB)}$, phase 1 reliability can be obtained by equation (7.22).

Phase 2

The beginning of a new phase requires a set of initial system state probabilities. To calculate the initial phase 2 system state probabilities, we require the probability that the system resides in any working state of the transition model at the end of phase 1.

The most minimal transition model listed in Table 7.14 requires no representation of component failure orderings. The Markov model states at the end of the first phase (Figure 7.11) may be represented in non-sequential form using Table 7.15. The state probabilities are assigned in equations (7.26) where all states that caused phase 1 failure are given a final probability of zero.

State Ref	Component A	Component B	Non-Sequential
$1^{(AB)}$	0	0	$1^{(AB)}$
$2_2^{(AB)}$	0	1_R	$2_2^{(AB)}$
$3_1^{(AB)}$	1_U	0	$3_1^{(AB)}$
$3_2^{(AB)}$	1_R	0	$3_2^{(AB)}$
$4_3^{(AB)}$	1_R	1_U	$4_3^{(AB)}$
$4_7^{(AB)}$	1_R	1_R	$4_{7,8}^{(AB)}$
$4_8^{(AB)}$	1_R	1_R	

Table 7.15 Final Phase 1 Non-Sequential States

$$\begin{array}{ccc}
\underline{\text{Final Phase 1}} & & \underline{\text{Final Phase 1}} \\
\underline{\text{Non-Sequential State}} & & \underline{\text{Sequential State}} \\
P_1^{(AB)}(t_1) & = & P_1^{(AB)}(t_1) \\
P_{2_2}^{(AB)}(t_1) & = & P_{2_2}^{(AB)}(t_1) \\
P_{3_1}^{(AB)}(t_1) & = & P_{3_1}^{(AB)}(t_1) \\
P_{3_2}^{(AB)}(t_1) & = & P_{3_2}^{(AB)}(t_1) \\
P_{4_3}^{(AB)}(t_1) & = & P_{4_3}^{(AB)}(t_1) \\
P_{4_{7,8}}^{(AB)}(t_1) & = & P_{4_7}^{(AB)}(t_1)+P_{4_8}^{(AB)}(t_1)=P_{4_7}^{(AB)}(t_1)
\end{array} \tag{7.26}$$

The second phase of this mission introduces component C which until now has not been required. The unavailability of component C at the end of the first phase is obtained in the same way as presented in Section 7.2.2.2 using equation (7.14) or (7.15). Since component C failure acts as an initiating event in phase 2, the final failure is classed as revealed. The probability of component C being in the working or failed state at the end of phase 1 must be included in this model. The transition model state probabilities at the end of the first phase using the working states of the reduced Markov model in equation (7.26) are found using Table 7.16.

As described in Section 7.2.1.3, the enabling event of component A failure in phase 1 becomes an initiating event in phase 2. At the transition point between phases 1 and 2, the failure of component A will automatically become revealed. The probabilities of all transition model states representative of component A in the unrevealed state must be re-assigned to contribute to the identical system state with component A in the revealed state. The final re-assigned phase 1 transition model state probabilities are given in equations (7.27).

$$\begin{array}{ll}
P_{5_2}^{(ABC)}(t_1)=P_{5_1}^{(ABC)}(t_1)+P_{5_2}^{(ABC)}(t_1) & P_{5_1}^{(ABC)}(t_1)\rightarrow 0 \\
P_{6_{7,8}}^{(ABC)}(t_1)=P_{6_{3,4}}^{(ABC)}(t_1)+P_{6_{7,8}}^{(ABC)}(t_1) & P_{6_{3,4}}^{(ABC)}(t_1)\rightarrow 0 \\
P_{7_{7,8}}^{(ABC)}(t_1)=P_{7_3}^{(ABC)}(t_1)+P_{7_{7,8}}^{(ABC)}(t_1) & P_{7_3}^{(ABC)}(t_1)\rightarrow 0 \\
P_{8_{43,45,46,47,48}}^{(ABC)}(t_1)=P_{8_{19,21,22}}^{(ABC)}(t_1)+P_{8_{43,45,46,47,48}}^{(ABC)}(t_1) & P_{8_{19,21,22}}^{(ABC)}(t_1)\rightarrow 0
\end{array} \tag{7.27}$$

Transition Model State Ref	Component States			Reduced Markov Model (Figure 7.10) with Final Component C State Probability
	A	B	C	
$1^{(ABC)}$	0	0	0	$P_1^{(AB)}(t_1)\cdot a_C(t_1)$
$2_1^{(ABC)}$	0	0	1_U	0
$2_2^{(ABC)}$	0	0	1_R	$P_1^{(AB)}(t_1)\cdot q_C(t_1)$
$3_2^{(ABC)}$	0	1_R	0	$P_{2_2}^{(AB)}(t_1)\cdot a_C(t_1)$
$4_{5,6}^{(ABC)}$	0	1_R	1_U	0
$4_{7,8}^{(ABC)}$	0	1_R	1_R	$P_{2_2}^{(AB)}(t_1)\cdot q_C(t_1)$
$5_1^{(ABC)}$	1_U	0	0	$P_{3_1}^{(AB)}(t_1)\cdot a_C(t_1)$
$5_2^{(ABC)}$	1_R	0	0	$P_{3_2}^{(AB)}(t_1)\cdot a_C(t_1)$
$6_{1,2}^{(ABC)}$	1_U	0	1_U	0
$6_{3,4}^{(ABC)}$	1_U	0	1_R	$P_{3_1}^{(AB)}(t_1)\cdot q_C(t_1)$
$6_{5,6}^{(ABC)}$	1_R	0	1_U	0
$6_{7,8}^{(ABC)}$	1_R	0	1_R	$P_{3_2}^{(AB)}(t_1)\cdot q_C(t_1)$
$7_3^{(ABC)}$	1_U	1_R	0	$P_{4_3}^{(AB)}(t_1)\cdot a_C(t_1)$
$7_{7,8}^{(ABC)}$	1_R	1_R	0	$P_{4_{7,8}}^{(AB)}(t_1)\cdot a_C(t_1)$
$8_{13,15,16}^{(ABC)}$	1_U	1_R	1_U	0
$8_{19,21,22}^{(ABC)}$	1_U	1_R	1_R	$P_{4_3}^{(AB)}(t_1)\cdot q_C(t_1)$
$8_{37,38,39,40,41}^{(ABC)}$	1_R	1_R	1_U	0
$8_{43,44,45,46,47,48}^{(ABC)}$	1_R	1_R	1_R	$P_{4_{7,8}}^{(AB)}(t_1)\cdot q_C(t_1)$

Table 7.16 Final Phase 1 Transition Model State

Transition failure will occur if the system resides in any successful phase 1 state that represents the existence of a phase 2 minimal cut set. The phase 2 minimal cut sets are {A, C} and {B, C}, thus phase 2 transition failure will occur if the system resides in a transition model state with either components A and C, or B and C in the failed state at the end of phase 1, and is given in equation (7.28).

$$Tr(t_1) = P_{4_{7,8}}^{(ABC)}(t_1) + P_{6_{7,8}}^{(ABC)}(t_1) + P_{8_{43,44,45,46,47,48}}^{(ABC)}(t_1) \tag{7.28}$$

Phase 2 is repairable and requires all three components. Since there are no sequential failure relationships that contribute to phase 2 failure, the transition model states do not need to be expanded and the phase 2 Markov model can be represented by Figure 7.20.

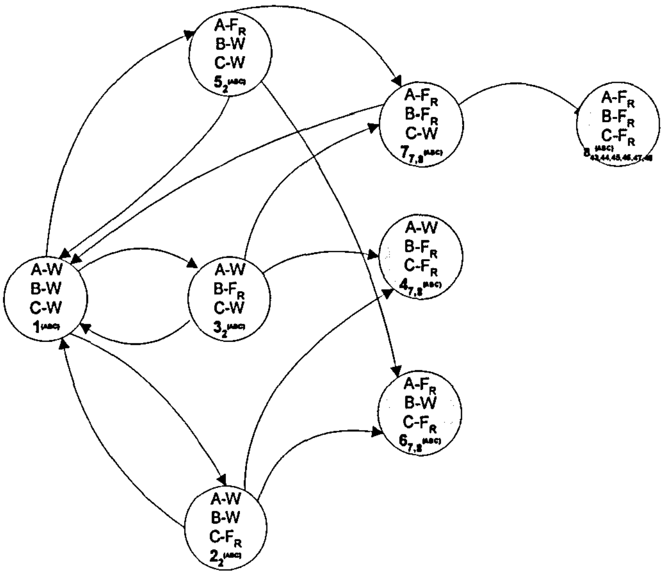


Figure 7.20 Non-Sequential Phase 2 Markov Model

The Markov model shown in Figure 7.20 is solved over the duration of phase 2, [t_1, t_2), with initial state probabilities given in Table 7.16 and equations (7.27). Any states that cause phase 1 or phase 2 failure are assigned an initial state probability value of zero. The reliability of phase 2 is found by the sum of the probabilities that the system resides in a successful state at the end of the phase in equation (7.29).

$$R(t_2) = P_1^{(ABC)}(t_2) + P_{2_2}^{(ABC)}(t_2) + P_{3_2}^{(ABC)}(t_2) + P_{5_2}^{(ABC)}(t_2) + P_{7_{7,8}}^{(ABC)}(t_2) \qquad (7.29)$$

Phase 3

Since the phase 2 Markov model required the full non-sequential states of the transition model, no reduction of sequential states is applied at the end of phase 2. The phase 2 failure states are assigned a final probability of zero, and all working transition model states can be passed directly to phase 3.

Transition failure will occur if the system resides in a state representing the existence of a phase 3 minimal cut set. There are two phase 3 minimal cut sets; non-sequential {C}, and sequential {$A^{(E)}$,$B^{(Ip)}$}. However since cut set {$A^{(E)}$,$B^{(Ip)}$} is PS, it cannot exist at the start of phase 3. Only non-sequential and NPS sequential minimal cut sets can exist at the start of a phase. Phase 3 transition failure can only occur if the system resides in a successful final phase 2 state with component C in the failed state ($2_2^{(ABC)}$ in Figure 7.20). The phase 3 transition failure becomes as given by equation (7.30).

$$Tr(t_2) = P_{2_2}^{(ABC)}(t_2) \tag{7.30}$$

Since the third phase consists of only non-repairable components, the method described in Section 7.2.2.3 can be applied for solution. We are only interested in the states of components A and B (Table 7.10) at the start of the third phase to solve the reduced Markov model. The phase 3 specific sequential minimal cut set {A$^{(E)}$,B$^{(Ip)}$} cannot exist at the start of the phase, and so state $4_8^{(AB)}$ is an impossible initial phase 3 state. As discussed in Section 7.3.2, a temporary state ($4_{8*}^{(AB)}$) is introduced to represent the same failure conditions but signifying a failure mode that does not cause phase 3 failure, and is shown in Figure 7.18.

The transition model states listed in Table 7.14 must be reduced to represent only the states of components A and B. In this case, since the transition model is representative of only non-sequential failures and the components are non-repairable, the probability that both components are in the failed state can be passed to either of the non-catastrophic failure mode states, $4_7^{(AB)}$ or $4_{8*}^{(AB)}$. In the event that the transition model contained sequential states or repairable components, this may not be possible. The reduced phase 3 Markov model states are obtained in Table 7.17. All states that cause phase 3 failure are assigned an initial state probability of zero.

State Ref		Component States		Combination of Initial Transition Model State Probabilities (Table 7.14)
		A	B	
$1^{(AB)}$		0	0	$P_1^{(ABC)}(t_2)$
$2_2^{(AB)}$		0	1_{1R}	$P_{3_2}^{(ABC)}(t_2)$
$3_1^{(AB)}$		1_{1U}	0	0
$3_2^{(AB)}$		1_{1R}	0	$P_{5_2}^{(ABC)}(t_2)$
$4_3^{(AB)}$		1_{2U}	1_{1R}	0
$4_7^{(AB)}$		1_{2R}	1_{1R}	0
$4_8^{(AB)}$		1_{1R}	1_{2R}	0
$4_{8*}^{(AB)}$		1_{1R}	1_{2R}	$P_{7_{7,8}}^{(ABC)}(t_2)$

Table 7.17 Phase 3 Initial Non-Sequential State Probabilities

The set of Markov differential equations can be solved over the duration of phase 3. The final system state probabilities can be combined with the unavailability of component C over the duration of the phase to calculate the reliability of phase 3. Using equations (7.19), (7.20) and (7.21), the reliability of phase 3 is expressed in equation (7.31)

$$R(t_3) = 1 - (q_{C_3} + P_{4_8}^{(AB)}(t_3) - (P_{4_8}^{(AB)}(t_3) \cdot q_{C_3})) \qquad (7.31)$$

where $q_{C_3} = a_C(t_2)(1 - e^{-\lambda_C(t_3 - t_2)})$

and (Figure 7.20) $a_C(t_2) = P_1^{(ABC)}(t_2) + P_{3_2}^{(ABC)}(t_2) + P_{5_2}^{(ABC)}(t_2) + P_{7_{7,8}}^{(ABC)}(t_2)$

7.4 Summary

The methods presented in this chapter provide a means of analysing a phased mission system with sequential failure relationships. The state explosion problem encountered when applying Markov models to phased mission systems is reduced by the definition of a minimal model between the phase transitions.

At each transition point, a new transition model is defined. All components that do not contribute to any further phases of the mission may be removed completely from the transition model. All remaining components that do not contribute to any NPS sequential minimal cut sets in later phases are expressed in non-sequential form, and all components that do contribute to a later NPS sequential minimal cut set must remain in sequential form. The model can then be expanded to represent PS failure relationships within each phase. Minimisation of each phase model due to either irrelevant components or components input to only static gates in a non-repairable phase may only be implemented if the components do not contribute to any NPS sequential minimal cut sets in later phases. At the end of each phase the minimised model is expanded back to the transition model for input to the next phase. By minimising the size of the Markov model, both at the phase boundaries and within each phase, an optimal solution for analysis is achieved.

Chapter 8 Importance Measures for Non-Repairable Phased Missions

8.1 Introduction

Measures of importance may be developed for components that are used in one or all phases of a multi-phased mission. Such measures will allow the criticality of each component to both individual phases and the entire mission to be calculated.

Although the importance of component failure will be assessed using the same method in each of the phases, the consequence of phase failure is not considered. For example in the flight pattern of an aircraft a failure in the initial phase where the aircraft is taxiing to the runway will not be catastrophic. The aircraft could remain grounded and repair initiated. However, if a later phase failure occurs while the aircraft is in flight, it is likely that the consequences would be more severe. From a risk perspective, components would have a higher importance in phases where failure has catastrophic consequences. Traditional importance measures can only analyse the importance of each component to a phase, the consequence of phase failure is not considered.

In this chapter, importance measures for non-repairable phased mission systems are developed. The minimal cut sets in each phase are non-sequential, and so phase failure will be caused by the occurrence of the events in a minimal cut set regardless of order. Further importance measures for repairable phased mission systems and sequential failure relationships are considered in Chapter 9.

All measures that are proposed to analyse the importance of components in non-repairable phased mission systems will be demonstrated by application to an example. In this case a mission comprising of 3 phases and non-repairable components A, B, C, and D will be used, shown in Figure 8.1.

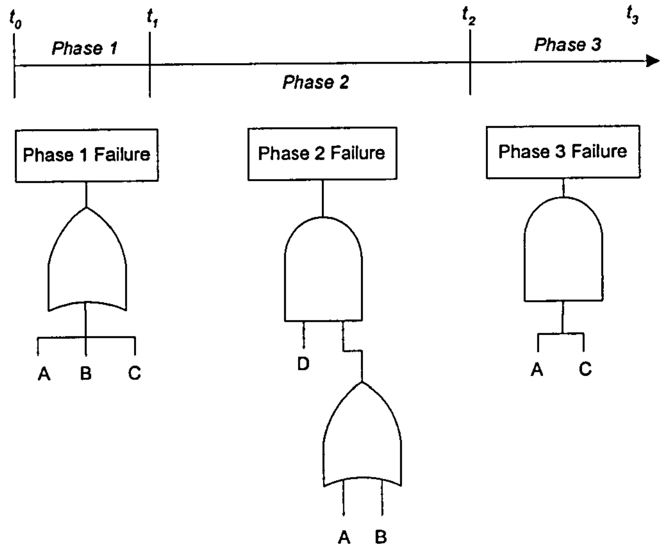


Figure 8.1 3-Phased Mission

8.2 Deterministic Importance Measures

A deterministic measure of importance will analyse the importance of a component to a phase with no reference to its probability of occurrence.

8.2.1 Phase Structural Importance Measure

For a single system comprising of *n* components, the structural measure of importance for a component was defined by equation (2.17). A component *c* is in a critical system state if the remaining (*n*-1) components are in a condition such that the failure of the component will cause the system to go from a working to a failed state.

If we treat each phase of the multi-phase mission in Figure 8.1 as a separate single-phase system, the critical states for component A in phases 1, 2 and 3 as defined in Section 2.2.3.5.1 are summarised in Table 8.1.

	States For Other Components in Phase			Critical State For Component
	B	C	D	
Phase 1	0	0	-	Yes
	0	1	-	No
	1	0	-	No
	1	1	-	No
Phase 2	0	-	0	No
	0	-	1	Yes
	1	-	0	No
	1	-	1	No
Phase 3	-	0	1	No
	-	1	0	Yes

where 0 = Component Success
1 = Component Failure
- = Not Required in Phase

Table 8.1 Critical States for Component A in Each Phase of Example

The structural measure of importance for component A in each of the phases is found using equation (2.17) to be:

$$I_{A_1} = \frac{1}{4} \qquad I_{A_2} = \frac{1}{4} \qquad I_{A_3} = \frac{1}{2} \tag{8.1}$$

However, since this measure does not take into account the behaviour of the components or the system through all previous phases, and also the performance of components that are not required in a particular phase, the results are not very informative. Treating each phase as a separate system assumes that all components are in the working state at the start of a phase. We require a method to obtain the critical system states for a component dependent on past and present behaviour of all other components in the system. The method must be capable of eliminating states which would have resulted in system failure in a previous phase.

The total number of components required in a multi-phased mission is N_c, however not all components will be required in every phase of the mission. There will be a total of N_{s_j} possible system states in phase j that are formed by the pattern of all N_c component success and failure combinations through all preceding phases up to and including phase j. The system will be in a critical state for a component if the combination of component states through the previous phases presents a working system state in phase j such that the failure of component c in phase j will cause phase failure. The structural measure of importance for a component c in phase j is defined in equation (8.2).

$$I_{c_j}^{ST} = \frac{\textit{number of critical system states for component c in phase j}}{\textit{number of phase j possible system states for } (N_c - 1) \textit{ remaining components}} \tag{8.2}$$

To obtain the possible system states in phase j, all valid combinations of component failure and success must be considered through all previous phases. As an example we can consider a system comprising of two components, A and B. To obtain the critical states for component A in phase 2 we must analyse the behaviour of component B through phases up to and including phase 2. There are four possibilities, B can work throughout phase j, $\overline{B_j}$, or fail during phase j, B_j, in each of the two phases (j=1,2). The four possibilities are presented in Table 8.2.

Performance of Component B				Definition	Combination
Phase 1	Event	Phase 2	Event		
Success	$\overline{B_1}$	Success	$\overline{B_2}$	Component works through both phases 1 and 2	$\overline{B_{12}}$
Success	$\overline{B_1}$	Failure	B_2	Component works through phase 1 and fails in phase 2	B_2
Failure	B_1	Success	$\overline{B_2}$	Not Possible. If component B fails in phase 1 it will remain failed in phase 2 as it is non-repairable. No further behaviour is considered.	B_1
Failure	B_1	Failure	B_2		

Table 8.2 Performance of Component B over 2 Phases

For a larger mission, the performance of components through the phases must be considered in a similar way with all impossible states eliminated. A state that is representative of component failure in a phase need not consider the later performance for that component since once it has failed it must remain in the failed state.

The identification of all possible component performance combinations does not generate an accurate list of all the possible system states in phase j. Some of the state combinations would have resulted in failure in a previous phase and must also be eliminated from the structural importance model. The remaining states are all possible phase j system states.

The structural importance for component A through each of the phases in the example given in Figure 8.1 will be determined to illustrate these points. The critical state of component A in phase 1 is not affected by component behaviour in previous phases and so can be obtained in the same way as for a single-phase system. However, since components which do not contribute to phase 1 failure will be required later in the mission, it is necessary to include the behaviour of all N_c - 1 components used in the mission. The critical states for phase 1 are summarised in Table 8.3.

Other Component States	Critical State For A
$(.,\overline{B_1},\overline{C_1},\overline{D_1})$	Yes
$(.,\overline{B_1},\overline{C_1},D_1)$	Yes
$(.,\overline{B_1},C_1,\overline{D_1})$	No
$(.,\overline{B_1},C_1,D_1)$	No
$(.,B_1,\overline{C_1},\overline{D_1})$	No
$(.,B_1,\overline{C_1},D_1)$	No
$(.,B_1,C_1,\overline{D_1})$	No
$(.,B_1,C_1,D_1)$	No

Table 8.3 Critical States for Component A in Phase 1

There is a possibility of 8 system states in phase 1. We can identify that 2 of the possible system states are critical for component A, and so the structural importance for component A in this first phase is given by equation (8.3)

$$I_{A_1}{}^{ST} = \frac{2}{8} = \frac{1}{4} \tag{8.3}$$

As expected, the structural importance for component A in the first phase is found to be identical to that obtained using conventional single system analysis.

To evaluate the importance of component A in the second phase, we must include the performance of all other components through the first phase. The list of possible system states in phase 2 is generated by the combination of the behaviour of components B, C, and D through both phases 1 and 2 in the same way as presented for component B in Table 8.2. The importance of component A in phase 2 is summarised in Table 8.4. Component behaviour combinations that cause failure in phase 1 cannot contribute to the importance of component A in phase 2 and are identified in column 2. From all possible phase 2 system states, those that are critical for component A are listed in column 3.

Other Component States	Fails in Phase 1	Critical State for Component A	Other Component States	Fails in Phase 1	Critical State for Component A
$(.,\overline{B_{12}},\overline{C_{12}},\overline{D_{12}})$	No	No	$(.,\overline{B_{12}},C_1,D_1)$	Yes	-
			$(.,\overline{B_{12}},C_1,D_2)$	Yes	-
$(.,B_1,\overline{C_{12}},\overline{D_{12}})$	Yes	-	$(.,\overline{B_{12}},C_2,D_1)$	No	Yes
$(.,B_2,\overline{C_{12}},\overline{D_{12}})$	No	No	$(.,\overline{B_{12}},C_2,D_2)$	No	Yes
$(.,\overline{B_{12}},C_1,\overline{D_{12}})$	Yes	-			
$(.,\overline{B_{12}},C_2,\overline{D_{12}})$	No	No	$(.,B_1,C_1,D_1)$	Yes	-
$(.,\overline{B_{12}},\overline{C_{12}},D_1)$	No	Yes	$(.,B_1,C_1,D_2)$	Yes	-
$(.,\overline{B_{12}},\overline{C_{12}},D_2)$	No	Yes	$(.,B_1,C_2,D_1)$	Yes	-
			$(.,B_1,C_2,D_2)$	Yes	-
$(.,B_1,C_1,\overline{D_{12}})$	Yes	-	$(.,B_2,C_1,D_1)$	Yes	-
$(.,B_1,C_2,\overline{D_{12}})$	Yes	-	$(.,B_2,C_1,D_2)$	Yes	-
$(.,B_2,C_1,\overline{D_{12}})$	Yes	-	$(.,B_2,C_2,D_1)$	No	No
$(.,B_2,C_2,\overline{D_{12}})$	No	No	$(.,B_2,C_2,D_2)$	No	No
$(.,B_1,\overline{C_{12}},D_1)$	Yes	-			
$(.,B_1,\overline{C_{12}},D_2)$	Yes	-			
$(.,B_2,\overline{C_{12}},D_1)$	No	No			
$(.,B_2,\overline{C_{12}},D_2)$	No	No			

Table 8.4 Critical States for Component A in Phase 2

There are 27 possible component performance combinations through phases 1 and 2. However, since the failure of components B or C in phase 1 would cause system failure, there are 15 component performance combinations that terminate the mission during phase 1 and are impossible phase 2 states (column 2). The remaining 12 states are all possible phase 2 states, and 4 of those are identified as critical states for component A (column 3). The structural importance of component A in phase 2 is given by equation (8.4),

$$I_{A_2}{}^{ST} = \frac{4}{12} = \frac{1}{3} \tag{8.4}$$

The structural importance for component A using this method is found to be greater than that obtained without accounting for the phased nature of the mission in equation (8.1). Treating the second phase as a separate system results in an optimistic assessment of structural importance for component A.

To evaluate the importance of component A in the final phase, we must again include the performance of all other components through the first and second phases. The list of possible system states in phase 3 is generated by the combination of components B, C, and D behaviour through phases 1, 2 and 3. The importance of component A in phase 3 is summarised in Table 8.5. Component behaviour combinations that cause failure in phases 1 or 2 cannot contribute to the importance of component A in phase 3 and are identified in columns 2 and 3. From all possible phase 3 system states, those that are critical for component A are listed in column 4.

There are 64 possible component performance combinations through phases 1, 2 and 3. However, certain combinations would have caused system failure during phases 1 or 2. The failure of components B or C in phase 1 would cause system failure and so 28 component behaviour combinations are eliminated from the possible phase 2 states (column 2). Phase 2 failure will occur if components B and D, or A and D, both fail either prior to or during phase 2, eliminating a further 6 component behaviour combinations from the possible phase 3 states (column 3). The remaining 30 component performance combinations are all possible phase 3 states, and 20 of those are identified as critical states for component A (column 4). The structural importance of component A in phase 3 is given by equation (8.5),

$$I_{A_3}{}^{ST} = \frac{20}{30} = \frac{2}{3} \tag{8.5}$$

The structural importance for component A using this method is again found to be greater than that obtained using conventional structural analysis on single systems in equation (8.1). Treating the final phase as a separate system for analysis again results in a optimistic assessment of structural importance for component A.

Other Component States	Fails in Phase 1	Fails in Phase 2	Critical State for Component A	Other Component States	Fails in Phase 1	Fails in Phase 2	Critical State for Component A
$(.,\overline{B_{123}},\overline{C_{123}},\overline{D_{123}})$	No	No	No	$(.\overline{B_{123}},C_2,D_2,)$	No	No	Yes
				$(.\overline{B_{123}},C_2,D_3,)$	No	No	Yes
$(.,B_1,\overline{C_{123}},\overline{D_{123}})$	Yes	-	-	$(.\overline{B_{123}},C_3,D_1,)$	No	No	Yes
$(.,B_2,\overline{C_{123}},\overline{D_{123}})$	No	No	No	$(.\overline{B_{123}},C_3,D_2,)$	No	No	Yes
$(.,B_3,\overline{C_{123}},\overline{D_{123}})$	No	No	No	$(.\overline{B_{123}},C_3,D_3,)$	No	No	Yes
$(.,\overline{B_{123}},C_1,\overline{D_{123}})$	Yes	-	-				
$(.,\overline{B_{123}},C_2,\overline{D_{123}})$	No	No	Yes	$(.,B_1,C_1,D_1)$	Yes	-	-
$(.,\overline{B_{123}},C_3,\overline{D_{123}})$	No	No	Yes	$(.,B_1,C_1,D_2)$	Yes	-	-
$(.,\overline{B_{123}},\overline{C_{123}},D_1)$	No	No	No	$(.,B_1,C_1,D_3)$	Yes	-	-
$(.,\overline{B_{123}},\overline{C_{123}},D_2)$	No	No	No	$(.,B_1,C_2,D_1)$	Yes	-	-
$(.,\overline{B_{123}},\overline{C_{123}},D_3)$	No	No	No	$(.,B_1,C_2,D_2)$	Yes	-	-
				$(.,B_1,C_2,D_3)$	Yes	-	-
$(.,B_1,C_1,\overline{D_{123}})$	Yes	-	-	$(.,B_1,C_3,D_1)$	Yes	-	-
$(.,B_1,C_2,\overline{D_{123}})$	Yes	-	-	$(.,B_1,C_3,D_2)$	Yes	-	-
$(.,B_1,C_3,\overline{D_{123}})$	Yes	-	-	$(.,B_1,C_3,D_3)$	Yes	-	-
$(.,B_2,C_1,\overline{D_{123}})$	Yes	-	-	$(.,B_2,C_1,D_1)$	Yes	-	-
$(.,B_2,C_2,\overline{D_{123}})$	No	No	Yes	$(.,B_2,C_1,D_2)$	Yes	-	-
$(.,B_2,C_3,\overline{D_{123}})$	No	No	Yes	$(.,B_2,C_1,D_3)$	Yes	-	-
$(.,B_3,C_1,\overline{D_{123}})$	Yes	-	-	$(.,B_2,C_2,D_1)$	No	Yes	-
$(.,B_3,C_2,\overline{D_{123}})$	No	No	Yes	$(.,B_2,C_2,D_2)$	No	Yes	-
$(.,B_3,C_3,\overline{D_{123}})$	No	No	Yes	$(.,B_2,C_2,D_3)$	No	No	Yes
$(.,B_1,\overline{C_{123}},D_1)$	Yes	-	-	$(.,B_2,C_3,D_1)$	No	Yes	-
$(.,B_1,\overline{C_{123}},D_2)$	Yes	-	-	$(.,B_2,C_3,D_2)$	No	Yes	-
$(.,B_1,\overline{C_{123}},D_3)$	Yes	-	-	$(.,B_2,C_3,D_3)$	No	No	Yes
$(.,B_2,\overline{C_{123}},D_1)$	No	Yes	-	$(.,B_3,C_1,D_1)$	Yes	-	-
$(.,B_2,\overline{C_{123}},D_2)$	No	Yes	-	$(.,B_3,C_1,D_2)$	Yes	-	-
$(.,B_2,\overline{C_{123}},D_3)$	No	No	No	$(.,B_3,C_1,D_3)$	Yes	-	-
$(.,B_3,\overline{C_{123}},D_1)$	No	No	No	$(.,B_3,C_2,D_1)$	No	No	Yes
$(.,B_3,\overline{C_{123}},D_2)$	No	No	No	$(.,B_3,C_2,D_2)$	No	No	Yes
$(.,B_3,\overline{C_{123}},D_3)$	No	No	No	$(.,B_3,C_2,D_3)$	No	No	Yes
$(.\overline{B_{123}},C_1,D_1,)$	Yes	-	-	$(.,B_3,C_3,D_1)$	No	No	Yes
$(.\overline{B_{123}},C_1,D_2,)$	Yes	-	-	$(.,B_3,C_3,D_2)$	No	No	Yes
$(.\overline{B_{123}},C_1,D_3,)$	Yes	-	-	$(.,B_3,C_3,D_2)$	No	No	Yes
$(.\overline{B_{123}},C_2,D_1,)$	No	No	Yes				

Table 8.5 Critical States for Component A in Phase 3

8.3 Probabilistic Measures of Importance

Probabilistic importance measures for components in non-repairable phased mission systems can be developed by appropriate extensions to the definitions presented for single phase systems in Section 2.2.3.5.2, and are discussed in the following sections.

8.3.1 Phase Criticality Function

The phase criticality function for a component *c* in a phase *j* is defined as the probability that the system is in a critical state for component *c* in phase *j*, and is denoted by $G_{c_j}(q(t))$. Since the mission is non-repairable, for the system to be in a critical state for component *c* in a phase, certain criteria must be met:

- All phases prior to phase *j* must have been completed successfully.
- Component *c* is in the working state at the start of phase *j*, i.e. has not failed in a previous phase.

The phase criticality function for component *c* may also be defined as the sum of the probabilities of occurrence of the critical states for component *c* in phase *j*.

The phase criticality function for component A in each phase for the example given in Figure 8.1 will be illustrated. Since the critical states for component A in each of the three phases (Tables 8.3, 8.4 and 8.5) has already been identified it is possible to calculate the probability of occurrence of the critical states to achieve phase criticality functions for component A. The critical states for component A in each of the three phases with associated probability is summarised in Table 8.6.

Critical State	Probability	Critical State	Probability
Phase 1:		Phase 3 Cont.	
$(.,\overline{B_1},\overline{C_1},\overline{D_1})$	$(1-q_{B_1})(1-q_{C_1})(1-q_{D_1})$	$(.,B_3,C_3,\overline{D_{123}})$	$q_{B_3}q_{C_3}(1-q_{D_{123}})$
$(.,\overline{B_1},\overline{C_1},D_1)$	$(1-q_{B_1})(1-q_{C_1})q_{D_1}$	$(\overline{B_{123}},C_2,D_1,)$	$(1-q_{B_{123}})q_{C_2}q_{D_1}$
		$(\overline{B_{123}},C_2,D_2,)$	$(1-q_{B_{123}})q_{C_2}q_{D_2}$
Phase 2:		$(\overline{B_{123}},C_2,D_3,)$	$(1-q_{B_{123}})q_{C_2}q_{D_3}$
$(.,\overline{B_{12}},\overline{C_{12}},D_1)$	$(1-q_{B_{12}})(1-q_{C_{12}})q_{D_1}$	$(\overline{B_{123}},C_3,D_1,)$	$(1-q_{B_{123}})q_{C_3}q_{D_1}$
$(.,\overline{B_{12}},\overline{C_{12}},D_2)$	$(1-q_{B_{12}})(1-q_{C_{12}})q_{D_2}$	$(\overline{B_{123}},C_3,D_2,)$	$(1-q_{B_{123}})q_{C_3}q_{D_2}$
$(.,\overline{B_{12}},C_2,D_1)$	$(1-q_{B_{12}})q_{C_2}q_{D_1}$	$(\overline{B_{123}},C_3,D_3,)$	$(1-q_{B_{123}})q_{C_3}q_{D_3}$
$(.,\overline{B_{12}},C_2,D_2)$	$(1-q_{B_{12}})q_{C_2}q_{D_2}$	$(.,B_2,C_2,D_3)$	$q_{B_2}q_{C_2}q_{D_3}$
		$(.,B_2,C_3,D_3)$	$q_{B_2}q_{C_3}q_{D_3}$
Phase 3:		$(.,B_3,C_2,D_1)$	$q_{B_3}q_{C_2}q_{D_1}$
$(.,\overline{B_{123}},C_2,\overline{D_{123}})$	$(1-q_{B_{123}})q_{C_2}(1-q_{D_{123}})$	$(.,B_3,C_2,D_2)$	$q_{B_3}q_{C_2}q_{D_2}$
$(.,\overline{B_{123}},C_3,\overline{D_{123}})$	$(1-q_{B_{123}})q_{C_3}(1-q_{D_{123}})$	$(.,B_3,C_2,D_3)$	$q_{B_3}q_{C_2}q_{D_3}$
$(.,B_2,C_2,\overline{D_{123}})$	$q_{B_2}q_{C_2}(1-q_{D_{123}})$	$(.,B_3,C_3,D_1)$	$q_{B_3}q_{C_3}q_{D_1}$
$(.,B_2,C_3,\overline{D_{123}})$	$q_{B_2}q_{C_3}(1-q_{D_{123}})$	$(.,B_3,C_3,D_2)$	$q_{B_3}q_{C_3}q_{D_2}$
$(.,B_3,C_2,\overline{D_{123}})$	$q_{B_3}q_{C_2}(1-q_{D_{123}})$	$(.,B_3,C_3,D_2)$	$q_{B_3}q_{C_3}q_{D_3}$

Table 8.6 Probability of Critical States for Component A

The resulting expressions to represent the sum of the probabilities that the system has not failed in a previous phase and is in a critical state for component A in phases 1, 2 and 3 are given by equations (8.6), (8.7) and (8.8) respectively.

$$G_{A_1}(q(t)) = Q(\textit{critical for A in phase 1})$$

$$= (1-q_{B_1})(1-q_{C_1})(1-q_{D_1}) + (1-q_{B_1})(1-q_{C_1})q_{D_1}$$

$$= (1-q_{B_1})(1-q_{C_1}) \tag{8.6}$$

$$G_{A_2}(q(t)) = Q(\textit{no failure in phase1 \& critical for A in phase 2})$$

$$= (1-q_{B_{12}})(1-q_{C_{12}})q_{D_1} + (1-q_{B_{12}})(1-q_{C_{12}})q_{D_2} + (1-q_{B_{12}})q_{C_2}q_{D_1} + (1-q_{B_{12}})q_{C_2}q_{D_2}$$
$$= (1-q_{B_{12}})q_{D_{12}}(1-q_{C_1}) \tag{8.7}$$

$$
\begin{aligned}
&G_{A_3}(\boldsymbol{q}(t)) = Q(\textit{no failure in phases 1 and 2 \& critical for A in phase 3}) \\
&=(1-q_{B_{123}})q_{C_2}(1-q_{D_{123}})+(1-q_{B_{123}})q_{C_3}(1-q_{D_{123}}) \\
&+q_{B_2}q_{C_2}(1-q_{D_{123}})+q_{B_2}q_{C_3}(1-q_{D_{123}})+q_{B_3}q_{C_2}(1-q_{D_{123}})+q_{B_3}q_{C_3}(1-q_{D_{123}}) \\
&+(1-q_{B_{123}})q_{C_2}q_{D_1}+(1-q_{B_{123}})q_{C_2}q_{D_2}+(1-q_{B_{123}})q_{C_2}q_{D_3}+(1-q_{B_{123}})q_{C_3}q_{D_1}+(1-q_{B_{123}})q_{C_3}q_{D_2}+(1-q_{B_{123}})q_{C_3}q_{D_3} \\
&+q_{B_2}q_{C_2}q_{D_3}+q_{B_2}q_{C_3}q_{D_3}+q_{B_3}q_{C_2}q_{D_1}+q_{B_3}q_{C_2}q_{D_2}+q_{B_3}q_{C_2}q_{D_3}+q_{B_3}q_{C_3}q_{D_1}+q_{B_3}q_{C_3}q_{D_2}+q_{B_3}q_{C_3}q_{D_3} \\
&=(1-q_{B_1})q_{C_{23}}-q_{B_2}q_{C_{23}}q_{D_{12}} \qquad (8.8)
\end{aligned}
$$

The process of identifying the critical states and calculating the sum of the probabilities of occurrence of each state becomes more complex as the number of phases and components increases. Alternative methods of calculating the criticality function are implemented for single phase missions whereby the expression for the probability of the system being in a critical state for a component can be obtained directly from the system failure probability equation (equations (2.20) and (2.22)). Similar methods are developed to obtain an expression for the probability that the system is in a critical state for a component in any phase of a multi-phased mission using the phase failure probability equation, and are presented in the following sections.

8.3.1.1 Phase Criticality Function using the Phase Failure Function

It is not possible to calculate the failure probability of a phase as the probability that one or more minimal cut sets occur during the phase duration as this does not take into account the successful outcome of all previous phases. Similarly as presented in Chapter 4, it is not possible to multiply the probability of success or failure of individual phases as this assumes that phases are independent and that all components are in the working state at the start of each phase.

A method to overcome these problems and obtain the phase failure probability was presented in Chapter 4, where the performance of a system is considered not only for the duration of the phase in question, but also for all preceding phases. A component that by being in the failed state in a phase would put the system in a critical state for another component could have failed at any point up to that time. By considering the component failing in each phase as a separate event, component failure in a particular phase fault tree is replaced by an OR combination of the events for the component failing in that and all preceding phases. The component failure in phase *j* is expressed as the event that the component could have failed during any phase up to and including phase *j*.

System failure in phase *j* is then represented by the AND of the success of phases 1..*j*-1 and the failure during phase *j* (Figure. 8.2).

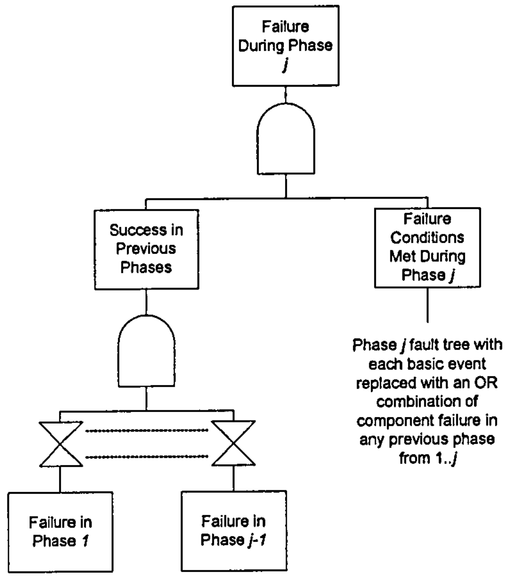
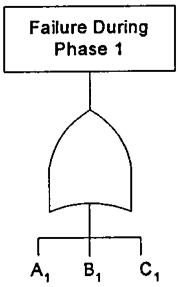

Failure During Phase j
Success in Previous Phases
Failure Conditions Met During Phase j
Phase j fault tree with each basic event replaced with an OR combination of component failure in any previous phase from 1..j
Failure in Phase 1
Failure in Phase j-1

Figure 8.2 Generalised Phase Failure Fault Tree

All phase failures may then be combined using an OR gate to represent causes of overall mission failure as any phase failure will mean the mission does not complete successfully.

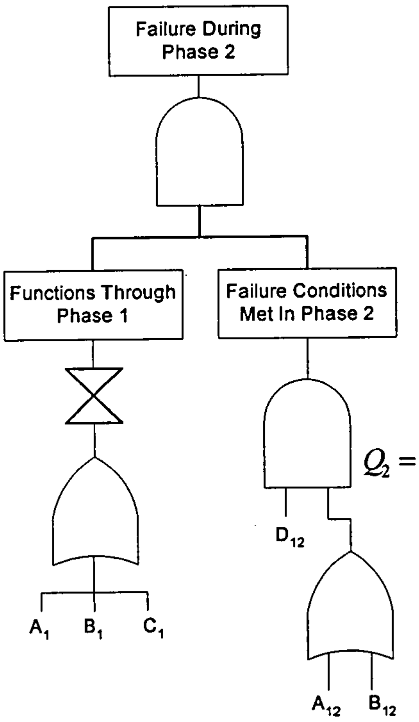
For the 3-phased mission in Figure 8.1, the phase failure fault trees and unavailability quantifications are given in Figures 8.3, 8.4, and 8.5 and equations (8.9), (8.10), and (8.11) respectively.



$$T_1 = A_1 + B_1 + C_1$$

$$Q_1 = q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1} \tag{8.9}$$

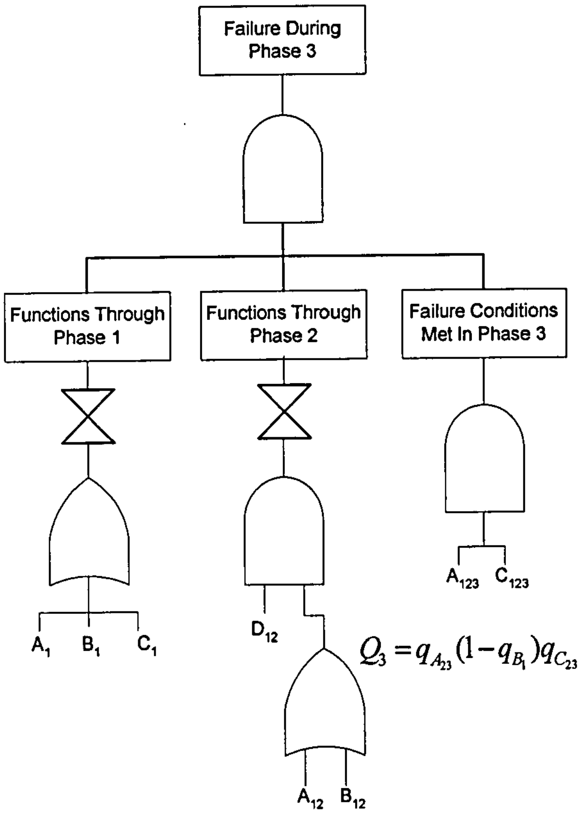
Figure 8.3 Phase 1 Failure



$$T_2 = \overline{A_1}\,\overline{B_1}\,\overline{C_1}(D_{12}(A_{12}+B_{12}))$$
$$= A_2\overline{B_1 C_1}D_{12} + \overline{A_1}B_2\overline{C_1}D_{12}$$

$$Q_2 = q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}} \tag{8.10}$$

Figure 8.4 Phase 2 Failure


Failure During Phase 3
Functions Through Phase 1
Functions Through Phase 2
Failure Conditions Met In Phase 3
A_1
B_1
C_1
D_{12}
A_{12}
B_{12}
A_{123}
C_{123}

$$T_3 = \overline{A_1}\,\overline{B_1}\,\overline{C_1}(\overline{D_{12}} + \overline{A_{12}}\,\overline{B_{12}})A_{123}C_{123}$$
$$= A_{23}\overline{B_1}C_{23}\overline{D_{12}} + A_3\overline{B_{12}}C_{23}$$

$$Q_3 = q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}}) \tag{8.11}$$

Figure 8.5 Phase 3 Failure

Once the prime implicant sets and probability of phase failure have been obtained it is possible to directly calculate the probability that the system is in a critical state for all components in the phase in a similar way as for a single phase system presented in Section 2.2.3.5.2. The phase failure probability equations (8.9), (8.10), and (8.11) are used.

An expression to obtain the probability that the system is in a critical state for a component c in phase j is derived using equation (2.20) and is given in equation (8.12).

$$G_{c_j}(\boldsymbol{q}(t)) = Q_j(1_{c_j}, \boldsymbol{q}(t)) - Q_j(0_{c_j}, \boldsymbol{q}(t)) \tag{8.12}$$

where $Q_j(1_{c_j}, \boldsymbol{q}(t))$ is the unavailability of phase j with component c failing in phase j

$Q_j(0_{c_j}, \boldsymbol{q}(t))$ is the unavailability of phase j with component c working in phase j

This is the probability that the system fails in phase j with component c failing in phase j minus the probability that the system fails in phase j with component c working throughout phase j, i.e. the system fails in phase j due to component c failing in phase j.

To obtain the phase criticality function for a component c in phase j, the event that component c failed at any point from the start of phase i to the end of phase j, $q_{c_{ij}}$, in the phase failure probability equation must be expanded into two separate terms. The only interest is the term that represents the failure of component c in phase j, q_{c_j}, and so the expression is expanded as shown in equation (8.13).

$$q_{c_{ij}} \rightarrow q_{c_{ij-1}} + q_{c_j} \tag{8.13}$$

This is necessary since if the system is in a critical state for component c in phase j it implies that component c cannot have failed in a previous phase. When obtaining the probability that the system fails in phase j with component c failing in phase j minus the probability that the system fails in phase j with component c working throughout phase j, the terms including $q_{c_{ij-1}}$ become irrelevant.

This method may be applied to the example in Figure 8.1. The evaluation of the phase criticality function for component A in phases 1, 2 and 3 is given by equations (8.14), (8.15), and (8.16).

Phase 1

$$Q_1 = q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}$$

$$Q(1_{A_1}, \boldsymbol{q}(t)) = 1 + q_{B_1} + q_{C_1} - q_{B_1} - q_{C_1} - q_{B_1}q_{C_1} + q_{B_1}q_{C_1} = 1$$

$$Q(0_{A_1}, \boldsymbol{q}(t)) = q_{B_1} + q_{C_1} - q_{B_1}q_{C_1}$$

$$G_{A_1}(\boldsymbol{q}(t)) = Q(1_{A_1}, \boldsymbol{q}(t)) - Q(0_{A_1}, \boldsymbol{q}(t)) = 1 - q_{B_1} - q_{C_1} + q_{B_1}q_{C_1} = (1 - q_{B_1})(1 - q_{C_1}) \quad (8.14)$$

Phase 2

Expand all $q_{A_{i..2}} \rightarrow q_{A_1} + q_{A_2}$

$$Q_2 = q_{A_2}(1 - q_{B_1})(1 - q_{C_1})q_{D_{12}} + (1 - q_{A_1})q_{B_2}(1 - q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1 - q_{C_1})q_{D_{12}}$$

$$Q(1_{A_2}, \boldsymbol{q}(t)) = (1 - q_{B_1})(1 - q_{C_1})q_{D_{12}} + (1 - q_{A_1})q_{B_2}(1 - q_{C_1})q_{D_{12}} - q_{B_2}(1 - q_{C_1})q_{D_{12}}$$
$$Q(0_{A_2}, \boldsymbol{q}(t)) = (1 - q_{A_1})q_{B_2}(1 - q_{C_1})q_{D_{12}}$$

$$\begin{aligned} G_{A_2}(\boldsymbol{q}(t)) = Q(1_{A_2}, \boldsymbol{q}(t)) - Q(0_{A_2}, \boldsymbol{q}(t)) &= (1 - q_{B_1})(1 - q_{C_1})q_{D_{12}} + (1 - q_{A_1})q_{B_2}(1 - q_{C_1})q_{D_{12}} \\ &\quad - q_{B_2}(1 - q_{C_1})q_{D_{12}} - (1 - q_{A_1})q_{B_2}(1 - q_{C_1})q_{D_{12}} \\ &= (1 - q_{B_{12}})(1 - q_{C_1})q_{D_{12}} \qquad (8.15) \end{aligned}$$

Phase 3

Expand all $q_{A_{i..3}} \rightarrow q_{A_{i..2}} + q_{A_3}$

$$\begin{aligned} Q_3 &= (q_{A_2} + q_{A_3})(1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}}) + q_{A_3}(1 - q_{B_{12}})q_{C_{23}} - q_{A_3}(1 - q_{B_{12}})q_{C_{23}}(1 - q_{D_{12}}) \\ &= q_{A_2}(1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}}) + q_{A_3}(1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}}) + q_{A_3}(1 - q_{B_{12}})q_{C_{23}} - q_{A_3}(1 - q_{B_{12}})q_{C_{23}}(1 - q_{D_{12}}) \end{aligned}$$

$$Q(1_{A_3}, \boldsymbol{q}(t)) = q_{A_2}(1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}}) + (1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}}) + (1 - q_{B_{12}})q_{C_{23}} - (1 - q_{B_{12}})q_{C_{23}}(1 - q_{D_{12}})$$
$$Q(0_{A_3}, \boldsymbol{q}(t)) = q_{A_2}(1 - q_{B_1})q_{C_{23}}(1 - q_{D_{12}})$$

$$\begin{aligned} G_{A_3}(q(t)) = Q(1_{A_3},q(t)) - Q(0_{A_3},q(t)) &= q_{A_2}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + (1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + (1-q_{B_{12}})q_{C_{23}} \\ &\quad -(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}}) - q_{A_2}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) \\ &= (1-q_{B_1})q_{C_{23}} - q_{B_2}q_{C_{23}}q_{D_{12}} \end{aligned} \tag{8.16}$$

It can be seen that equations (8.14), (8.15) and (8.16) are identical to those calculated by the sum of the occurrences of the critical states (equations (8.6), (8.7) and (8.8)). The same methods can also be applied to components B, C and D for the mission.

8.3.1.2 Phase Criticality Function using the Derivative of the Phase Failure Function

The probability of failure in phase *j*, Q_j, is linear in the probability that component *c* fails in phase *j*, q_{c_j}. The phase criticality function of component *c* in phase $j, G_{c_j}(q(t))$, can be derived from equation (2.22) and is given in equation (8.17).

$$G_{c_j}(q(t)) = \frac{\partial Q_j(q(t))}{\partial q_{c_j}(t)} \tag{8.17}$$

This method will again be demonstrated by application to the example in Figure 8.1 using the expansion technique to separate terms given in equation (8.13). Birnbaum's measure of importance for component A in phases 1, 2 and 3 is derived and given in equations (8.18), (8.19) and (8.20).

Phase 1

$$Q_1 = q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}$$

$$G_{A_1}(q) = \frac{\partial Q_1}{\partial q_{A_1}} = 1 - q_{B_1} - q_{C_1} + q_{B_1}q_{C_1} = (1-q_{B_1})(1-q_{C_1}) \tag{8.18}$$

Phase 2

Expand all $q_{A_{1..2}} \rightarrow q_{A_1} + q_{A_2}$

$$Q_2 = q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}$$

$$G_{A_2}(q) = \frac{\partial Q_2}{\partial q_{A_2}} = (1-q_{B_1})(1-q_{C_1})q_{D_{12}} - q_{B_2}(1-q_{C_1})q_{D_{12}} = (1-q_{B_{12}})(1-q_{C_1})q_{D_{12}} \quad (8.19)$$

Phase 3

Expand all $q_{A_{i..3}} \rightarrow q_{A_{i..2}} + q_{A_3}$

$$Q_3 = (q_{A_2} + q_{A_3})(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})$$

$$= q_{A_2}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})$$

$$G_{A_3}(q) = \frac{\partial Q_3}{\partial q_{A_3}} = (1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + (1-q_{B_{12}})q_{C_{23}} - (1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})$$

$$= (1-q_{B_1})q_{C_{23}} - q_{B_2}q_{C_{23}}q_{D_{12}} \quad (8.20)$$

The results obtained by this direct partial differentiation of the phase failure probability equation (equations (8.18), (8.19) and (8.20)) are identical to those found by calculating the sum of the occurrences of the critical states in equations (8.6), (8.7) and (8.8). The critical states with associated probabilities for components B, C, and D are identified, and the phase criticality function is calculated as both a sum of the probability of occurrence of the critical states and using equation (8.17), given in Appendix B.

8.3.2 Mission Criticality Function

It is possible to combine the results of each phase criticality function to achieve an overall mission criticality function with ranking for all components. Since each phase may have different time duration, taking an average of all the phase criticality functions for each component would not give an accurate representation of the importance of a component to the entire mission. The period of time for which a phase is in operation must be accounted for when calculating the mission criticality function since a component with higher importance in a shorter phase could be just as significant as the same component with lower importance in a longer phase.

The mission criticality function for a component is defined as the probability that the system is in a critical state for component c in a multi-phased mission, and is denoted by $G_{c_{MISS}}(q(t))$. This can be represented by equation (8.21).

$$G_{c_{MISS}} = \sum_{j=1}^{m} \text{P(System is critical for component } c \text{ in phase } j \mid \text{in phase } j) * \text{P(In phase } j) \tag{8.21}$$

where P(System is critical for component c in phase j | in phase j) = $G_{c_j}(q(t))$

$$\text{P(In phase } j) = \frac{t_j - t_{j-1}}{t_m}$$

The mission criticality function for component A in the example given in Figure 8.1 can be found by equation (8.22).

$$G_{A_{MISS}}(q(t)) = \frac{\left(G_{A_1}(q(t)) * t_1\right) + \left(G_{A_2}(q(t)) * (t_2 - t_1)\right) + \left(G_{A_3}(q(t)) * (t_3 - t_2)\right)}{t_3} \tag{8.22}$$

It is possible to rank the components in order of importance by the criticality function for both each individual phase and the entire mission. To demonstrate this, numerical values are assigned to the component failure probabilities in phases 1, 2, and 3 in Figure 8.1, given in equations (8.23).

Mission Data	Component Data
Phase 1 = 2 hours	$\lambda_A = 0.01$ /h
Phase 2 = 10 hours	$\lambda_B = 0.02$ /h
Phase 3 = 5 hours	$\lambda_C = 0.03$ /h
	$\lambda_D = 0.04$ /h

Component Failure Probabilities

$$\begin{array}{lll} \text{Phase 1} & \text{Phase 2} & \text{Phase 3} \\ q_{A_1}=0.020 & q_{A_2}=0.093 & q_{A_3}=0.043 \\ q_{B_1}=0.039 & q_{B_2}=0.174 & q_{B_3}=0.075 \\ q_{C_1}=0.058 & q_{C_2}=0.244 & q_{C_3}=0.097 \\ q_{D_1}=0.077 & q_{D_2}=0.304 & q_{D_3}=0.112 \end{array} \qquad (8.23)$$

The criticality function with ranking for components A, B, C and D in phases 1, 2 and 3 and for the entire mission are summarised in Table 8.7.

Component		Phase 1 Criticality Function	Rank	Phase 2 Criticality Function	Rank	Phase 3 Criticality Function	Rank	Mission Criticality Function	Mission Rank
A		0.905262	3	0.2824559	2	0.3050947	1	0.3623857	1
B		0.92316	2	0.3183461	1	0	3	0.2958695	2
C		0.94178	1	0	4	0.0937942	2	0.1383842	3
D		0	4	0.2295758	3	0	3	0.1350446	4

Table 8.7 Phase and Mission Criticality Functions

It can be seen that the component importance values in phase 1 are significantly larger than in any other phase. This is due to the series arrangement of the components in the first phase compared with parallel and combined parallel and series arrangements in the final two phases. Since components A and B are less likely to fail in the first phase, the system is more likely to be in a critical state for component C and so it has the highest importance ranking. This is followed by component B, and then component A. In phase 2, the parallel arrangement means that as component D has the highest failure rate, components A and B will have the highest importance. In phase 3, components A and C are again arranged in parallel and so since component C has the higher failure rate, the system is more likely to be in a critical state for component A.

Component A has the overall highest importance ranking due to the fact it is the only component required in all three phases. Component B has the second highest importance ranking since from the two phases of requirement it is always connected in a series arrangement with other components. Components C and D have lower values of importance since they are required in fewer phases and are generally arranged in parallel with other components. The system is most likely to be in a critical state for components A and B.

If each phase is treated as a separate system, using the critical states given in Table 8.1, Birnbaum's importance for component A in would be represented by equations (8.24).

$$\begin{aligned} &Q(\text{critical in phase 1}) = (1-q_{B_1})(1-q_{C_1}) \\ &Q(\text{critical in phase 2}) = (1-q_{B_2})q_{D_2} \qquad (8.24) \\ &Q(\text{critical in phase 3}) = q_{C_3} \end{aligned}$$

Numerically, the criticality function for each of the components when treating each phase as a separate system produces the results shown in Table 8.8.

Component		Phase 1 Criticality Function	Rank	Phase 2 Criticality Function	Rank	Phase 3 Criticality Function	Rank	Mission Criticality Function	Mission Rank
A		0.905262	3	0.251104	2	0.097	1	0.2827391	1
B		0.92316	2	0.275728	1	0	3	0.2708	2
C		0.94178	1	0	4	0.043	2	0.1234447	4
D		0	4	0.250818	3	0	3	0.14754	3

Table 8.8 Phase and Mission Criticality Functions Treating Each Phase as a Separate System

It is seen that although the rankings remain consistent to those in Table 8.7 through the phases, the values obtained for the criticality function of each component become increasingly inaccurate as the phases progress. When treating each phase as a separate system, the values of importance are generally smaller through the phases, implying that the probability of the system being in a critical state for each component is less than it actually would be. This is due to the assumption that all components are in the working state at the start of a phase. The overall mission rankings using equations (8.24) produce a different result to the proposed method, implying that component D is more important than component C.

8.3.3 Criticality Measures of Component Importance

The criticality measure of importance is defined as the proportion of system failures caused because the system is in a critical state for component *c*, and component *c* has failed. For a single phase system, this could be directly obtained using the criticality function. The criticality measure of importance for a single phase mission is calculated as the product of the criticality function (Birnbaum's measure of importance) and the component failure probability at time *t*, weighted by the system failure probability in equation (2.23).

The criticality importance measure may be developed further to include the possibility of phased mission systems. This is the probability that the system is in a critical state for component *c* in phase *j*, and component *c* has failed (weighted by the phase *j* system failure probability). However, if the system is in a critical state for component *c* in phase *j*, it is possible that component *c* could fail during phase *j* or exist in the failed state at the start of phase *j*. Both events would cause phase *j* failure.

Two new importance measures are developed, the *criticality measure of in-phase component importance* and the *criticality measure of transition component importance.* The criticality measure of in-phase component importance, $I_{c_j}^{CR(I-p)}$, is defined as the probability that the system is in a critical state for component *c* in phase *j*, and component *c* has failed **during phase *j*.** The criticality measure of transition component importance, $I_{c_j}^{CR(Tr)}$, is defined as the probability that the system is in a critical state for component *c* in phase *j*, and component *c* has failed **prior to phase *j*.** Both are weighted by the phase *j* system failure probability.

The total *criticality measure of phase component importance,* $I_{c_j}^{CR}$, is then derived as the sum of the contribution of in-phase and transition criticality importances, given in equation (8.25).

$$I_{c_j}^{CR} = I_{c_j}^{CR(I-p)} + I_{c_j}^{CR(Tr)} \qquad (8.25)$$

The criticality measure of in-phase component importance is obtained using the same approach as for a single phase mission, by multiplying the probability that the system is in a critical state for component *c* in phase *j* with the probability that component *c* fails in phase *j*. This is given in algebraic form in equation (8.26).

$$I_{c_j}^{CR(I-p)} = \frac{G_{c_j}(q(t))q_{c_j}(t)}{Q_j(q(t))} \tag{8.26}$$

Where the probability that component *c* fails in phase *j*, $q_{c_j} = \int_{t_{j-1}}^{t_j} f_c(t)\,dt$

The phase *j* failure probability, $Q_j(q(t))$, is derived by considering the method of combining previous phase successes with phase *j* failure (Figure 8.2).

This measure is best demonstrated by considering the example given in Figure 8.1. The criticality measure of in-phase importance for component A in phase 3 is given in equation (8.27).

$$I_{A_3}^{CR(I-p)} = \frac{((1-q_{B_1})q_{C_{23}} - q_{B_2}q_{C_{23}}q_{D_{12}})q_{A_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = \frac{((1-q_{B_1}) - q_{B_2}q_{D_{12}})q_{A_3}}{q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}} \tag{8.27}$$

This method has evaluated the probability that the system is in a critical state for component A in phase 3, and component 3 fails **during** phase 3 (weighted by the phase 3 system failure probability).

To account for the event that component A exists in the failed state at the start of phase 3, the criticality measure of transition component importance is required. The method given in equation (8.26) can be adjusted to represent the probability that the system is in a critical state for component *c* in phase *j*, and component *c* fails in any phase up to but not including phase *j*. This is summarised in equation (8.28).

$$I_{c_j}^{CR(Tr)} = \frac{G_{c_j}(q(t))q_{c_{1j-1}}(t)}{Q_j(q(t))} \tag{8.28}$$

This may be evaluated for component A in phase 3 in equation (8.29).

$$I_{A_3}^{CR} = \frac{((1-q_{B_1})q_{C_{23}} - q_{B_2}q_{C_{23}}q_{D_{12}})q_{A_{12}}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}}q_{D_{12}}} = \frac{((1-q_{B_1}) - q_{B_2}q_{D_{12}})q_{A_{12}}}{q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}} \tag{8.29}$$

It can be seen that the method presented in equation (8.28) is wrong since if component A fails in phase 1, phase 1 failure will occur and the mission will not transfer to phase 2. It is only possible for component A to be failed at the start of phase 3 due to failure in phase 2, q_{A_2}. However, the combination of this event (q_{A_2}) with the second term of Birnbaum's measure of phase importance for component A in phase 3 ($q_{B_2}q_{C_{23}}q_{D_{12}}$), represents the occurrence of a phase 2 implicant set, $A_2\overline{B_1C_1}D_{12}$. This would cause phase 2 failure and so since phase 3 would not be reached successfully it is also an incorrect method of obtaining the criticality measure of transition importance.

A new method is presented to derive the correct criticality measure of transition importance for a component *c* in phase *j*. The probability that the system is in a critical state at the start of phase *j* for the **failure** of component *c* in any phase *k* up to but not including phase *j*, and the component has failed in phase *k* is required. This is represented algebraically in equation (8.30).

$$I_{c_j}^{CR(Tr)} = \frac{\sum_{k=1}^{j-1}\left(\frac{\partial Q_j(q(t))}{\partial q_{c_k}(t)}\right)\cdot q_{c_k}(t)}{Q_j(q(t))} \tag{8.30}$$

This method may be applied to derive the criticality measure of transition importance for component A in phase 3 of example 8.1 and is given in equation (8.31).

$$I_{A_3}^{CR(Tr)} = \frac{\left(\frac{\partial Q_3(\boldsymbol{q})}{\partial q_{A_1}}\right)\cdot q_{A_1} + \left(\frac{\partial Q_3(\boldsymbol{q})}{\partial q_{A_2}}\right)\cdot q_{A_2}}{Q_3(\boldsymbol{q})}$$

$$\text{where } \left(\frac{\partial Q_3(\boldsymbol{q})}{\partial q_{A_1}}\right)\cdot q_{A_1} = 0\cdot q_{A_1} = 0$$

$$\left(\frac{\partial Q_3(\boldsymbol{q})}{\partial q_{A_2}}\right)\cdot q_{A_2} = \left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_2}$$

$$I_{A_3}^{CR(Tr)} = \frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_2}}{Q_3(\boldsymbol{q})} = \frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_2}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} \tag{8.31}$$

The total criticality measure of phase importance for component c in phase j is found by the sum of the contribution of the in-phase and transition criticality importances. This is derived in equation (8.32).

$$\begin{aligned}
I_{c_j}^{\ CR} &= I_{c_j}^{\ CR(I-p)} + I_{c_j}^{\ CR(Tr)} \\
&= \frac{G_{c_j}(q(t))q_{c_j}(t)}{Q_j(q(t))} + \frac{\sum_{k=1}^{j-1}\left(\frac{\partial Q_j(q(t))}{\partial q_{c_k}}\right)\cdot q_{c_k}(t)}{Q_j(q(t))} \\
&= \frac{\left(\frac{\partial Q_j(q(t))}{\partial q_{c_j}(t)}\right)\cdot q_{c_j}(t)}{Q_j(q(t))} + \frac{\sum_{k=1}^{j-1}\left(\frac{\partial Q_j(q(t))}{\partial q_{c_k}(t)}\right)\cdot q_{c_k}(t)}{Q_j(q(t))} \\
&= \frac{\sum_{k=1}^{j}\left(\frac{\partial Q_j(q(t))}{\partial q_{c_k}(t)}\right)\cdot q_{c_k}(t)}{Q_j(q(t))}
\end{aligned} \qquad (8.32)$$

The total criticality measure of phase importance for component A in phase 3 of example 8.1 is given in equation (8.33).

$$\begin{aligned}
I_{A_3}^{\ CR} &= \frac{\sum_{k=1}^{3}\left(\frac{\partial Q_3(q)}{\partial q_{A_k}}\right)\cdot q_{A_k}}{Q_3(q)} \\
&= \frac{\left(\frac{\partial Q_3(q)}{\partial q_{A_1}}\right)\cdot q_{A_1} + \left(\frac{\partial Q_3(q)}{\partial q_{A_2}}\right)\cdot q_{A_2} + \left(\frac{\partial Q_3(q)}{\partial q_{A_3}}\right)\cdot q_{A_3}}{Q_3(q)}
\end{aligned}$$

where $\left(\frac{\partial Q_j(q)}{\partial q_{A_1}}\right)\cdot q_{A_1} = 0\cdot q_{A_1} = 0$

$$\left(\frac{\partial Q_j(q)}{\partial q_{A_2}}\right)\cdot q_{A_2} = \big((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\big)\cdot q_{A_2}$$

$$\left(\frac{\partial Q_j(q)}{\partial q_{A_3}}\right)\cdot q_{A_3} = \big((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + (1-q_{B_{12}})q_{C_{23}} - (1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})\big)\cdot q_{A_3}$$

$$I_{A_3}{}^{CR} = \frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_2} + \left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + (1-q_{B_{12}})q_{C_{23}} - (1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_3}}{Q_3(q(t))}$$

$$I_{A_3}{}^{CR} = \frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_{23}} + \left((1-q_{B_{12}})q_{C_{23}} - (1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = 1$$

(8.33)

For phase 3 failure to occur, component A must either exist in the failed state at the start of phase 3 or fail during phase 3 (with component C failed) due to the parallel arrangement between components A and C. The result of unity in equation (8.33) is consistent with this and shows that for phase 3 failure to occur, component A must be in the failed state.

The criticality measures of importance for components A, B, C and D in the three phases of Figure 8.1 are derived using the methods presented and are given in equations (8.34), (8.35), and (8.36) respectively.

Phase 1

Failure Probability $Q_1(q) = q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}$

Criticality Measure of Component Phase Importance

$$I_{A_1}{}^{CR} = I_{A_1}{}^{CR(I-P)} = \frac{\left(\frac{\partial Q_1(q)}{\partial q_{A_1}}\right)\cdot q_{A_1}}{Q_1(q)} = \frac{(1-q_{B_1})(1-q_{C_1})q_{A_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{B_1}{}^{CR} = I_{B_1}{}^{CR(I-P)} = \frac{\left(\frac{\partial Q_1(q)}{\partial q_{B_1}}\right)\cdot q_{B_1}}{Q_1(q)} = \frac{(1-q_{A_1})(1-q_{C_1})q_{B_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{C_1}{}^{CR} = I_{C_1}{}^{CR(I-P)} = \frac{\left(\frac{\partial Q_1(q)}{\partial q_{C_1}}\right)\cdot q_{C_1}}{Q_1(q)} = \frac{(1-q_{A_1})(1-q_{B_1})q_{C_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{D_1}{}^{CR} = I_{D_1}{}^{CR(I-P)} = \frac{\left(\frac{\partial Q_1(q)}{\partial q_{D_1}}\right)\cdot q_{D_1}}{Q_1(q)} = \frac{0\cdot q_{D_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}} = 0$$

(8.34)

Phase 2

Failure Probability

$$Q_2(q)=q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}$$

Criticality Measure of Component Importance

$$I_{A_2}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{A_1}}\right)\cdot q_{A_1}}{Q_2(q)}=\frac{0\cdot q_{A_1}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=0$$

$$I_{A_2}{}^{CR}=I_{A_2}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{A_2}}\right)\cdot q_{A_2}}{Q_2(q)}=\frac{\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)q_{A_2}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=\frac{(1-q_{B_{12}})q_{A_2}}{q_{A_2}(1-q_{B_{12}})+(1-q_{A_1})q_{B_2}}$$

$$I_{B_2}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{B_1}}\right)\cdot q_{B_1}}{Q_2(q)}=\frac{0\cdot q_{B_1}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=0$$

$$I_{B_2}{}^{CR}=I_{B_2}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{B_2}}\right)\cdot q_{B_2}}{Q_2(q)}=\frac{\left((1-q_{A_1})(1-q_{C_1})q_{D_{12}}-q_{A_2}(1-q_{C_1})q_{D_{12}}\right)q_{B_2}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=\frac{(1-q_{A_{12}})q_{B_2}}{q_{A_2}(1-q_{B_{12}})+(1-q_{A_1})q_{B_2}}$$

$$I_{C_2}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{C_1}}\right)\cdot q_{C_1}}{Q_2(q)}=\frac{0\cdot q_{C_1}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=0$$

$$I_{C_2}{}^{CR}=I_{C_2}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{C_2}}\right)\cdot q_{C_2}}{Q_2(q)}=\frac{0\cdot q_{C_2}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=0$$

$$I_{D_2}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{D_1}}\right)\cdot q_{D_1}}{Q_2(q)}=\frac{\left(q_{A_2}(1-q_{B_1})(1-q_{C_1})+(1-q_{A_1})q_{B_2}(1-q_{C_1})-q_{A_2}q_{B_2}(1-q_{C_1})\right)\cdot q_{D_1}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}$$

$$I_{D_2}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{D_2}}\right)\cdot q_{D_2}}{Q_2(q)}=\frac{\left(q_{A_2}(1-q_{B_1})(1-q_{C_1})+(1-q_{A_1})q_{B_2}(1-q_{C_1})-q_{A_2}q_{B_2}(1-q_{C_1})\right)\cdot q_{D_2}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}$$

$$I_{D_2}{}^{CR}=I_{D_2}{}^{CR(Tr)}+I_{D_2}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_2(q)}{\partial q_{D_1}}\right)\cdot q_{D_1}+\left(\frac{\partial Q_2(q)}{\partial q_{D_2}}\right)\cdot q_{D_2}}{Q_2(q)}=\frac{\left(q_{A_2}(1-q_{B_1})(1-q_{C_1})+(1-q_{A_1})q_{B_2}(1-q_{C_1})-q_{A_2}q_{B_2}(1-q_{C_1})\right)\cdot\left(q_{D_1}+q_{D_2}\right)}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}=1 \tag{8.35}$$

Phase 3

Failure Probability

$$Q_3(q)=q_{A_2}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})$$

Criticality Measure of Component Importance

$$I_{A_3}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{A_1}}\right)\cdot q_{A_1}+\left(\frac{\partial Q_3(q)}{\partial q_{A_2}}\right)\cdot q_{A_2}}{Q_3(q)}=\frac{0\cdot q_{A_1}+\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_2}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}$$

$$I_{A_3}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{A_3}}\right)\cdot q_{A_3}}{Q_3(q)}=\frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+(1-q_{B_{12}})q_{C_{23}}-(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}$$

$$I_{A_3}{}^{CR}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{A_1}}\right)\cdot q_{A_1}+\left(\frac{\partial Q_3(q)}{\partial q_{A_2}}\right)\cdot q_{A_2}+\left(\frac{\partial Q_3(q)}{\partial q_{A_3}}\right)\cdot q_{A_3}}{Q_3(q)}=\frac{\left((1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_{23}}+\left((1-q_{B_{12}})q_{C_{23}}-(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})\right)\cdot q_{A_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=1$$

$$I_{B_3}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{B_1}}\right)\cdot q_{B_1}+\left(\frac{\partial Q_3(q)}{\partial q_{B_2}}\right)\cdot q_{B_2}}{Q_3(q)}=\frac{0\cdot q_{B_1}+0\cdot q_{B_2}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=0$$

$$I_{B_3}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{B_3}}\right)\cdot q_{B_3}}{Q_3(q)}=\frac{0\cdot q_{B_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=0$$

$$I_{B_3}{}^{CR}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{B_1}}\right)\cdot q_{B_1}+\left(\frac{\partial Q_3(q)}{\partial q_{B_2}}\right)\cdot q_{B_2}+\left(\frac{\partial Q_3(q)}{\partial q_{B_3}}\right)\cdot q_{B_3}}{Q_3(q)}=\frac{0\cdot q_{B_1}+0\cdot q_{B_2}+0\cdot q_{B_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=0$$

$$I_{C_3}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{C_1}}\right)\cdot q_{C_1}+\left(\frac{\partial Q_3(q)}{\partial q_{C_2}}\right)\cdot q_{C_2}}{Q_3(q)}=\frac{\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})-q_{A_3}(1-q_{B_{12}})(1-q_{D_{12}})\right)\cdot q_{C_2}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}$$

$$I_{C_3}{}^{CR(I-p)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{C_3}}\right)\cdot q_{C_3}}{Q_3(q)}=\frac{\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})-q_{A_3}(1-q_{B_{12}})(1-q_{D_{12}})\right)\cdot q_{C_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}$$

$$I_{C_3}{}^{CR}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{C_1}}\right)\cdot q_{C_1}+\left(\frac{\partial Q_3(q)}{\partial q_{C_2}}\right)\cdot q_{C_2}+\left(\frac{\partial Q_3(q)}{\partial q_{C_3}}\right)\cdot q_{C_3}}{Q_3(q)}=\frac{\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})-q_{A_3}(1-q_{B_{12}})(1-q_{D_{12}})\right)\cdot(q_{C_2}+q_{C_3})}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=1$$

$$I_{D_3}{}^{CR(Tr)}=\frac{\left(\frac{\partial Q_3(q)}{\partial q_{D_1}}\right)\cdot q_{D_1}+\left(\frac{\partial Q_3(q)}{\partial q_{D_2}}\right)\cdot q_{D_2}}{Q_3(q)}=\frac{0\cdot q_{D_1}+0\cdot q_{D_2}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}=0$$

$$I_{D_3}{}^{CR(I-p)} = \frac{\left(\frac{\partial Q_3(q)}{\partial q_{D_3}}\right)\cdot q_{D_3}}{Q_3(q)} = \frac{0\cdot q_{D_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = 0$$

$$I_{D_3}{}^{CR} = \frac{\left(\frac{\partial Q_3(q)}{\partial q_{D_1}}\right)\cdot q_{D_1} + \left(\frac{\partial Q_3(q)}{\partial q_{D_2}}\right)\cdot q_{D_2} + \left(\frac{\partial Q_3(q)}{\partial q_{D_3}}\right)\cdot q_{D_3}}{Q_3(q)} = \frac{0\cdot q_{D_1}+0\cdot q_{D_2}+0\cdot q_{D_3}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{C_{23}}-q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = 0$$

(8.36)

As for the mission criticality function (equation (8.21)), it is possible to obtain a measure of the criticality of each component in the entire mission. This is defined as the probability that the system is in a critical state for component *c* during any phase *j* of a multi-phased mission, and component *c* has failed (weighted by the mission failure probability). Since the probability of component *c* failure in phase *j* accounts for the duration of phase *j*, the period of time for which the phase is in operation for is not included. The criticality measure of mission component importance is obtained by the sum of each individual phase *j* criticality importance given that phase *j* has been reached successfully and is derived in equation (8.37).

$I_{c_{MISS}}{}^{CR} = \sum_{j=1}^{m}$ P(System is critical for component *c* in phase *j*, and component *c* has

failed | in phase *j*) (weighted by the mission failure probability)

$$I_{c_{MISS}}{}^{CR} = \frac{\sum_{j=1}^{m}\sum_{k=1}^{j}\left(\frac{\partial Q_j(q(t))}{\partial q_{c_k}(t)}\right)\cdot q_{c_k}(t)}{Q_{MISS}(q(t))} \qquad (8.37)$$

Using the mission data given in equations (8.23) it is possible to obtain the criticality measure of phase and mission importance for each component in Figure 8.1. The results of this are summarised in Table 8.9.

Component		Criticality Phase 1 Importance	Rank	Criticality Phase 2 Importance	Rank	Criticality Phase 3 Importance	Rank	Criticality Mission Importance	Mission Rank
A		0.1604459	3	0.3003188	3	1	1	0.3287084	4
B		0.3190554	2	0.6332829	2	0	2	0.3934449	1
C		0.484063	1	0	4	1	1	0.3728316	3
D		0	4	1	1	0	2	0.3765393	2
		Phase 1		Phase 2		Phase 3		Mission	
Unavailability		0.1128432		0.0874684		0.0319838		0.2322954	

Table 8.9 Criticality Measure of Component Phase and Mission Importance

The criticality measure of importance can be used to analyse which of the components are most likely to be in the failed state when the system is failed. In phase 1, component C has the highest importance ranking since it is the most likely to fail and contribute to phase failure, followed by component B, and component D has the lowest. For phase 2 failure to occur, component D must fail, and so if the system fails in this phase it is definite that component D is in the failed state. The series arrangement between components A and B results in an equal system contribution however since component B has a higher failure rate, it is more likely to be in the failed state when phase 2 failure occurs. In phase 3, components A and C are arranged in parallel, and both must be in the failed state for phase 3 failure to occur.

From the components with the highest value of mission criticality function, A and B, it is component B that is most likely to be in the failed state when the system fails. Component A is the least likely to be in the failed state when the system fails.

If the results are again compared to those obtained by treating each phase as a separate system, it is possible to see the inaccuracies when disregarding the performance of components through all previous phases, shown in Table 8.10.

Component		Criticality Phase 1 Importance	Rank	Criticality Phase 2 Importance	Rank	Criticality Phase 3 Importance	Rank	Criticality Mission Importance	Mission Rank
A		0.1604459	3	0.3062699	3	1	1	0.2360976	4
B		0.3190554	2	0.6292132	2	0	2	0.4345371	1
C		0.484063	1	0	4	1	1	0.3042189	3
D		0	4	1	1	0	2	0.3945334	2
		Phase 1		Phase 2		Phase 3		Mission	
Unavailability		0.1128432		0.0762487		0.004171		0.1932629	

Table 8.10 Criticality Measure of Component Phase and Mission Importance when Treating each Phase as a Separate System

Comparisons between treating each phase as a separate system with the combination of previous phase success with current phase failure shows that the component criticality importance rankings through the phases are identical and the importance values in this simple example are very similar.

However, the phase unavailability is seen to become increasingly more inaccurate as the phases progress. This is due to the fact that no account is taken of previous phase outcome, and the assumption that all components are in the working state at the start of each phase. Therefore the importance values for components that do not contribute to all implicant sets of a phase will also become more inaccurate as the phases progress.

In this simple example, the greatest inconsistency is seen when considering the overall mission values. This is accounted for by considering the increasing inaccuracies in the values of phase and mission unavailability when treating each phase as a separate system.

8.3.4 Measures of Component Importance

For phase failure to arise, it is possible that one or more phase prime implicant sets could have occurred. The failure of a component can contribute to the failure of a system without being critical. Component *c* will contribute to the failure of a phase *j* by the occurrence of a prime implicant set containing the failure of *c*.

The occurrence of a prime implicant set in phase *j* could arise at the time of transition due to a component failure in a previous phase. An example of this is the prime implicant set in the third phase of Figure 8.1, $A_{23}\overline{B_1}C_{23}\overline{D_{12}}$. This phase 3 prime implicant set is representative of components A and C failing in either of phases 2 or 3, and so if the components failed in the second phase it will cause phase 3 failure at the time of transition. The prime implicant sets that contain the event of a component failure must be considered regardless of which phase(s) the failure could have occurred in.

For phased mission analysis, an extension of the Fussell-Vesely measure of importance is defined, the *Measure of Phase Component Importance*. This is the probability of the union of the occurrence of phase *j* prime implicant sets, ε_{k_j}, containing the failure of component *c* (in any phase) given that phase *j* failure has occurred, and is weighted by the phase failure probability in equation (8.38).

$$I_{c_j}{}^{FV} = \frac{P(\bigcup_{k_j|c\in k_j} \varepsilon_{k_j})}{Q_j(\boldsymbol{q}(t))} \tag{8.38}$$

This measure may be applied to the example in Figure 8.1. The prime implicant sets of the mission are given in Figure 8.6.

	Reference	Implicant Set
Phase 1	1_1	A_1
	2_1	B_1
	3_1	C_1
Phase 2	1_2	$A_2\overline{B_1 C_1}D_{12}$
	2_2	$\overline{A_1}B_2\overline{C_1}D_{12}$
Phase 3	1_3	$A_{23}\overline{B_1}C_{23}\overline{D_{12}}$
	2_3	$A_3\overline{B_{12}}C_{23}$

Figure 8.6 Mission Implicant Sets

The measure of phase importance for each of the components in phases 1, 2, and 3 are given in equations (8.39), (8.40) and (8.41) respectively.

Phase 1

$$I_{A_1}{}^{FV} = \frac{q_{A_1}}{q_{A_1}+q_{B_1}+q_{C_1}-q_{A_1}q_{B_1}-q_{A_1}q_{C_1}-q_{B_1}q_{C_1}+q_{A_1}q_{B_1}q_{C_1}} \qquad I_{B_1}{}^{FV} = \frac{q_{B_1}}{q_{A_1}+q_{B_1}+q_{C_1}-q_{A_1}q_{B_1}-q_{A_1}q_{C_1}-q_{B_1}q_{C_1}+q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{C_1}{}^{FV} = \frac{q_{C_1}}{q_{A_1}+q_{B_1}+q_{C_1}-q_{A_1}q_{B_1}-q_{A_1}q_{C_1}-q_{B_1}q_{C_1}+q_{A_1}q_{B_1}q_{C_1}} \qquad I_{D_1}{}^{FV} = 0 \tag{8.39}$$

Phase 2

$$I_{A_2}{}^{FV} = \frac{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}} = \frac{q_{A_2}(1-q_{B_1})}{q_{A_2}(1-q_{B_{12}})+(1-q_{A_1})q_{B_2}}$$

$$I_{B_2}{}^{FV} = \frac{(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}+(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}-q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}} = \frac{(1-q_{A_1})q_{B_2}}{q_{A_2}(1-q_{B_{12}})+(1-q_{A_1})q_{B_2}}$$

$$I_{C_2}{}^{FV} = 0$$

$$I_{D_2}{}^{FV} = \frac{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}} = 1$$

(8.40)

Phase 3

$$I_{A_3}{}^{FV} = \frac{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = 1$$

$$I_{B_3}{}^{FV} = 0$$

$$I_{C_3}{}^{FV} = \frac{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = 1$$

$$I_{D_3}{}^{FV} = 0$$

(8.41)

As for the criticality measure of mission component importance (equation (8.37)), it is possible to obtain a measure of mission importance for each component. This is defined as the sum of the probabilities of the union of the occurrence of prime implicant sets ε_{k_j} containing the failure of component *c* (in any phase) given that phase *j* failure has occurred, and is weighted by the mission unavailability. This measure may be obtained by the sum of each individual phase *j* component importance given that phase *j* has been reached successfully, and is shown in equation (8.42).

$I_{c_{MISS}}{}^{FV} = \sum_{j=1}^{m}$ P(Union of the ε_{k_j} implicant sets containing failure of *c* (in any phase) | phase *j* failure has occurred) (weighted by the mission failure probability)

$$I_{c_{MISS}}{}^{FV} = \frac{\sum_{j=1}^{m} P(\bigcup_{k_j|c\in k_j} \varepsilon_{k_j})}{Q_{MISS}(q(t))} \qquad (8.42)$$

Using the mission data given in equations (8.23) it is possible to obtain the measure of phase and mission importance for each component in Figure 8.1. The results of this are summarised in Table 8.11.

Component		Phase 1 Importance	Rank	Phase 2 Importance	Rank	Phase 3 Importance	Rank	Mission Importance	Mission Rank
A		0.177237	3	0.3438838	3	1	1	0.3618667	4
B		0.3456122	2	0.6561162	2	0	2	0.4313471	1
C		0.5139874	1	0	4	1	1	0.3873681	2
D		0	4	1	1	0	2	0.3765393	3
		Phase 1		Phase 2		Phase 3		Mission	
Unavailability		0.1128432		0.0874684		0.0319838		0.2322954	

Table 8.11 Measure of Component Phase and Mission Importance

This measure of importance ranks the contribution each component failure makes to system failure. In phase 1, component C has the highest value of importance followed by component B and component D has the lowest. Since the components are linked in series, from the three first order cut sets, {C} will contribute most highly to phase failure as component C has a greater failure rate than components A and B. In phase 2, component D is present in both prime implicant sets of the phase and so for phase 2 failure to occur, component D must have failed. In phase 3, components A and C contribute to both prime implicant sets, and so they are of equal importance to the success of the phase. For the overall mission, component B has the highest ranking followed by component C.

The phase importance rankings are seen to be identical to those obtained using the criticality measure of importance and so produce the same conclusions. The mission importance rankings are different in that component C is now more important to the overall mission than component D.

It is possible to compare the component phase and mission importance values to those obtained by treating each phase as a separate system. The results are given in Table 8.12.

Component		Phase 1 Importance	Rank	Phase 2 Importance	Rank	Phase 3 Importance	Rank	Mission Importance	Mission Rank
A		0.177237	3	0.3707868	3	1	1	0.2713557	4
B		0.3456122	2	0.6937301	2	0	2	0.4754973	2
C		0.5139874	1	0	4	1	1	0.3216913	3
D		0	4	1	1	0	2	0.3945334	1
		Phase 1		Phase 2		Phase 3		Mission	
Unavailability		0.1128432		0.0762487		0.004171		0.1932629	

Table 8.12 Measure of Component Phase and Mission Importance when Treating each Phase as a Separate System

Component failures that contribute to all implicant sets in a phase result in the same phase importance value of unity as the presented method. Component failures that contribute to only some of the implicant sets in a phase produce a different importance value for all phases after the first phase when treating each phase as a separate system. By considering each phase separately, the phase importance values are generally higher which implies that components make a higher contribution to phase failure than is true. This is due to the assumption made that all components are in the working state at the start of a phase.

The mission importance rankings are different when treating each phase as a separate system as component D is considered to be the most important rather than component B. This is due to the increasing inaccuracy in the phase unavailability calculation as the phases progress.

8.3.5 Measures of Prime Implicant Set Importance

A measure exists to rank the importance of each cut set in a single phase mission. This Fussell-Vesely measure of minimal cut set importance defines the probability of occurrence of each minimal cut set given that the system has failed (equation (2.27)).

This measure may be extended for application to phased mission systems. A *measure of phase prime implicant set importance* is defined as the probability of occurrence of prime implicant set ε_{k_j} given that phase j has failed (weighted by the phase j system failure probability), and is expressed in equation (8.43).

$$I_{\varepsilon_{k_j}}{}^{FV} = \frac{P(\varepsilon_{k_j})}{Q_j(q(t))} \tag{8.43}$$

The measure of phase prime implicant set importance may be applied to the example in Figure 8.1, and the importance for the prime implicant sets in each of the 3 phases (Figure 8.6) are given in equations (8.44), (8.45) and (8.46) respectively.

<u>Phase 1</u>

$$I_{1_1}{}^{FV} = \frac{q_{A_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{2_1}{}^{FV} = \frac{q_{B_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

$$I_{3_1}{}^{FV} = \frac{q_{C_1}}{q_{A_1} + q_{B_1} + q_{C_1} - q_{A_1}q_{B_1} - q_{A_1}q_{C_1} - q_{B_1}q_{C_1} + q_{A_1}q_{B_1}q_{C_1}}$$

(8.44)

<u>Phase 2</u>

$$I_{1_2}{}^{FV} = \frac{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}} = \frac{q_{A_2}(1-q_{B_1})}{q_{A_2}(1-q_{B_{12}}) + (1-q_{A_1})q_{B_2} - q_{A_2}q_{B_2}}$$

$$I_{2_2}{}^{FV} = \frac{(1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}}}{q_{A_2}(1-q_{B_1})(1-q_{C_1})q_{D_{12}} + (1-q_{A_1})q_{B_2}(1-q_{C_1})q_{D_{12}} - q_{A_2}q_{B_2}(1-q_{C_1})q_{D_{12}}} = \frac{(1-q_{A_1})q_{B_2}}{q_{A_2}(1-q_{B_{12}}) + (1-q_{A_1})q_{B_2} - q_{A_2}q_{B_2}}$$

(8.45)

<u>Phase 3</u>

$$I_{1_3}{}^{FV} = \frac{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}})}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = \frac{q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})}{q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}}$$

$$I_{2_3}{}^{FV} = \frac{q_{A_3}(1-q_{B_{12}})q_{C_{23}}}{q_{A_{23}}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_{23}} - q_{A_3}(1-q_{B_{12}})q_{C_{23}}(1-q_{D_{12}})} = \frac{q_{A_3}(1-q_{B_{12}})}{q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}}$$

(8.46)

The event of mission failure is represented by the OR combination of the system failure during each of the phases. It is possible to obtain a measure of prime implicant set importance for the contribution of prime implicant sets to the failure of the entire mission. This is defined as the probability of occurrence of prime implicant set ε_{k_j} given that phase j has failed (weighted by the mission failure probability), and is given in equation (8.47).

$I_{\varepsilon_{k_{MISS}}}{}^{FV}$ =P(Occurrence of prime implicant set ε_{k_j} | phase j fails) (weighted by the mission failure probability)

$$I_{\varepsilon_{k_{MISS}}}{}^{FV} = \frac{\sum_{j=1}^{m} P(\varepsilon_{k_j})}{Q_{MISS}(q(t))} \qquad (8.47)$$

Using the mission data given in equations (8.23) it is possible to obtain the measures of prime implicant set importance for each of the prime implicant sets in Figure 8.6. The results of this are summarised in Table 8.13.

Cut Set	Phase 1 Prime Implicant Set Importance	Rank	Phase 2 Prime Implicant Set Importance	Rank	Phase 3 Prime Implicant Set Importance	Rank	Mission Prime Implicant Set Importance	Mission Rank
1_1	0.177237	3	-	-	-	-	0.0860973	6
2_1	0.3456122	2	-	-	-	-	0.1678896	3
3_1	0.5139874	1	-	-	-	-	0.249682	2
1_2	-	-	0.3438838	2	-	-	0.1380834	4
2_2	-	-	0.6561162	1	-	-	0.2634575	1
1_3	-	-	-	-	0.8625351	1	0.118759	5
2_3	-	-	-	-	0.3608004	2	0.0496772	7

Table 8.13 Measure of Prime Implicant Set Importance

In this example, the prime implicant sets with the highest importance to the mission are in the first two phases of the mission.

If each phase is treated as a separate system, the phase minimal cut sets would be as given in Figure 8.7.

	Reference	Minimal Cut Sets
Phase 1	1_1	A_1
	2_1	B_1
	3_1	C_1
Phase 2	1_2	A_2D_2
	2_2	B_2D_2
Phase 3	1_3	A_3C_3

Figure 8.7 Mission Cut Sets when Treating each Phase as a Separate System

The Fussell-Vesely measures of cut set importance would be found as given in Table 8.14.

Cut Set	Fussell-Vesely Phase 1 Cut Set Importance	Rank	Fussell-Vesely Phase 2 Cut Set Importance	Rank	Fussell-Vesely Phase 3 Cut Set Importance	Rank	Fussell-Vesely Mission Cut Set Importance	Mission Rank
1_1	0.177237	3	-	-	-	-	0.103486	5
2_1	0.3456122	2	-	-	-	-	0.2017976	3
3_1	0.5139874	1	-	-	-	-	0.3001093	1
1_2	-	-	0.3707868	2	-	-	0.1462878	4
2_2	-	-	0.6937301	1	-	-	0.2736997	2
1_3	-	-	-	-	1	1	0.021582	6

Table 8.14 Fussell-Vesely Measure of Cut Set Importance when Treating each Phase as a Separate System

Considering each phase as a separate system results in different importance values and rankings for the mission minimal cut sets. Treating the prime implicant sets as minimal cut sets does not take into account the requirement for previous phase successes. The difference in minimal cut set importance is due to the assumption that all components are working at the start of a phase.

8.4 Summary

The analysis of importance is a very useful tool in the design and optimisation stages of a system. Since many systems comprise of multiple phases, it is useful to be able to implement importance measures during these initial stages.

The importance measures presented for single phase systems (Section 2.2.3.5.2) have been successfully developed to allow the assessment of component importance in non-repairable multi-phased missions. Probabilistic measures can easily be obtained using combinatorial methods, and are weighted according to either the phase or mission failure probability as appropriate. Further measures for initiating and enabling events and repairable systems are presented in the following chapter.

Chapter 9 Importance Measures for Initiating and Enabling Events in Phased Missions

9.1 Introduction

The importance measures described in the previous chapter assumed that the order of component failures in a minimal cut set is irrelevant. In some cases the top event of a fault tree may only be caused by a certain sequence of basic event occurrences. Probabilistic measures of importance are presented in Section 9.2 to deal with the interval reliability of a system where the order of component failures is significant.

Markov models are implemented for the solution to repairable multi-phased missions. The model state probabilities can be used to calculate the importance of components rather than using combinatorial approaches. Methods to assess the probabilistic importance of repairable components using Markov models are presented in Section 9.3.

9.2 Probabilistic Measures for Initiating and Enabling Events

The inclusion of sequential failure relationships in phased mission analysis allows us to extend the current initiator and enabler importance measures to derive further measures for multi-phased systems. Probabilistic measures of importance are presented to deal with the interval reliability of a multi-phased mission where the order of component failures is important. It is assumed that a mission is taking place, and all such measures are weighted according to the expected number of phase j failures, $W_j(t_{j-1}, t_j)$.

The example in Figure 8.1 has been modified to include representation of sequential failure relationships. This will be used to demonstrate the sequential importance measures developed for phased mission analysis and is given in Figure 9.1.

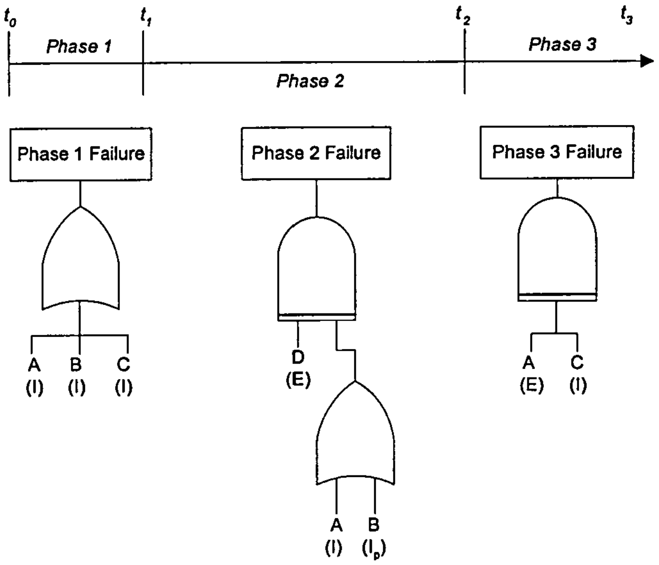


Figure 9.1 3-Phased Mission with Sequential Failure Relationships

9.2.1 Expected Number of Phase Failures

The unconditional phase failure intensity for single phased missions can be derived using the criticality function as presented in Section 2.2.3.5.3, given in equation (9.1).

$$
\begin{aligned}
w_{SYS} &= \sum_{\substack{i=1 \\ i \text{ initiator}}}^{N_i} G_i(q(t)) \cdot w_i \\
&= \sum_{\substack{i=1 \\ i \text{ initiator}}}^{N_i} \left(\frac{\partial Q_{SYS}(q(t))}{\partial q_i(t)} \right) \cdot w_i
\end{aligned}
\qquad (9.1)
$$

where N_i is the number of initiating events

This is the sum of the probabilities that the system is in a critical state for initiating event i, and initiating event i occurs.

In a multi-phased mission, phase j failure can occur due to either the occurrence of an initiating i event during phase j or the existence of initiating event i at the start of phase j (if i is non-phase specific). The system can therefore be in a phase j critical state for the event of component i failure in any phase k up to and including phase j.

The unconditional failure intensity for a phase *j*, w_j , is defined as the sum of the probabilities that the system is in a phase *j* critical state for component *i* failure in any phase *k* up to and including phase *j*, and the frequency that event *i* occurs during phase *k*. This is expressed in equation (9.2).

$$w_j = \sum_{\substack{i=1 \\ \text{phase } j \\ \text{initiating event}}}^{N_{i_j}} \sum_{k=1}^{k=j} G_{i_j}(q(t)) \cdot w_{i_k}$$

$$= \sum_{\substack{i=1 \\ \text{phase } j \\ \text{initiating event}}}^{N_{i_j}} \sum_{k=1}^{k=j} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)} \right) \cdot w_{i_k} \tag{9.2}$$

where N_{i_j} is the number of initiating events in phase *j*

w_{i_k} is the is the frequency that initiating event *i* occurs during phase *k*

The unconditional failure intensity of an initiating event *i* in phase *k*, w_{i_k}, is obtained from the component *i* failure probability in phase *k*, q_{i_k}, using equation (9.3).

$$w_{i_k} = q_{i_k} \lambda_i \tag{9.3}$$

where $q_{i_k} = e^{-\lambda_i t_{k-1}} - e^{-\lambda_i t_k}$

The expected number of failures for a single phase system can be obtained by the integral of the unconditional system failure intensity over the mission duration [0, *t*) (Section 2.2.3.5.3, equation (2.30)). We require a similar method to obtain the expected number of system failures during each phase *j* of a multi-phased mission. Phase *j* failure may occur due to the existence of non-sequential and non-phase specific sequential minimal cut sets at the start of the phase, or due to the occurrence of any minimal cut sets during the phase. The expected number of phase failures may be separated into two discrete terms, the *expected number of phase transition failures*, and the *expected number of in-phase failures*. The total expected number of phase failures is obtained as the sum of the two terms.

The expected number of phase j transition failures, $W_j^{Tr}(t_{j-1})$, is obtained by the integral of the occurrence of non-sequential and non-phase specific phase j minimal cut sets prior to the start of phase j which do not cause failure in a previous phase. We require the expected number of phase j failures due to the occurrence of any non-phase j specific initiating event i in any phase k up to but not including phase j. This is the integral of the phase j unconditional failure intensity due to initiating events that occurred prior to phase j over the interval $[t_{k-1}, t_k)$, and is represented algebraically in equation (9.4).

$$W_j^{Tr}(t_{j-1}) = \underset{\substack{non-phase\ j \\ specific\ initiating\ event}}{\sum_{i=1}^{N_{ij}}} \sum_{k=1}^{k=j-1} \int_{t_{k-1}}^{t_k} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)} \right) \cdot w_{i_k} dt \qquad (9.4)$$

The expected number of in-phase j failures, $W_j^{I-p}(t_{j-1}, t_j)$, is obtained by the integral of the occurrence of all phase j minimal cut sets during phase j. We require the expected number of system failures due to all initiating events i in phase j. This is represented algebraically in equation (9.5).

$$W_j^{I-p}(t_{j-1}, t_j) = \underset{\substack{i\ phase\ j \\ initiating\ event}}{\sum_{i=1}^{N_{ij}}} \int_{t_{j-1}}^{t_j} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_j}(t)} \right) \cdot w_{i_j} dt \qquad (9.5)$$

The total expected number of phase j failures is obtained by the contribution of both the expected number of phase j transition failures and the expected number of in-phase j failures. This combines equations (9.4) and (9.5), and is summarised in equation (9.6).

$$W_j(t_{j-1}, t_j) = W_j^{Tr}(t_{j-1}) + W_j^{I-p}(t_{j-1}, t_j) = \left(\underset{\substack{i\,phase\,j \\ initiating\,event}}{\sum_{i=1}^{N_{ij}}} \sum_{k=1}^{k=j} \int_{t_{k-1}}^{t_k} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)} \right) \cdot w_{i_k} dt \right) \qquad (9.6)$$

The inclusion of sequential failure relationships in the example in Figure 9.1 means that the top event and thus the phase failure probability equations (8.9) - (8.11) need to be adjusted. Since phase failure will only occur if all enabling events occur before the initiating event in a sequential cut set, any component failure combinations which do not represent the required sequential relationship of the cut set must be eliminated from the phase failure probability equation.

In phase 1 there are no sequential cut sets and so the phase 1 failure probability remains as given in equation (8.9). In phase 2, there are two prime implicant sets, $A_2\overline{B_1}\,\overline{C_1}D_{12}$ and $\overline{A_1}B_2\overline{C_1}D_{12}$. However since both represent the event that D occurs before A or B, the phase 2 failure probability remains as given in equation (8.10).

In phase 3 there are two prime implicant sets, $A_{23}\overline{B_1}C_{23}\overline{D_{12}}$ and $A_3\overline{B_{12}}C_{23}$. With the inclusion of sequential failure relationships, for phase 3 failure to occur, event A must occur prior to event C. The prime implicant sets must be altered to represent this, and become:

$$A_{23}\overline{B_1}C_{23}\overline{D_{12}} \xrightarrow{\text{Expand}} \begin{array}{l} A_2\overline{B_1}C_2\overline{D_{12}} \\ A_2\overline{B_1}C_3\overline{D_{12}} \\ A_3\overline{B_1}C_2\overline{D_{12}}\ ^* \\ A_3\overline{B_1}C_3\overline{D_{12}} \end{array} \longrightarrow \begin{array}{l} A_2\overline{B_1}C_2\overline{D_{12}} \\ A_2\overline{B_1}C_3\overline{D_{12}} \\ A_3\overline{B_1}C_3\overline{D_{12}} \end{array} \longrightarrow \begin{array}{l} A_2\overline{B_1}C_{23}\overline{D_{12}} \\ A_3\overline{B_1}C_3\overline{D_{12}} \end{array}$$

$$A_3\overline{B_{12}}C_{23} \xrightarrow{\text{Expand}} \begin{array}{l} A_3\overline{B_{12}}C_2\ ^* \\ A_3\overline{B_{12}}C_3 \end{array} \longrightarrow A_3\overline{B_{12}}C_3$$

*No longer a prime implicant set

There are now three prime implicant sets, $A_2\overline{B_1}C_{23}\overline{D_{12}}$, $A_3\overline{B_1}C_3\overline{D_{12}}$, and $A_3\overline{B_{12}}C_3$. The probability of phase 3 failure becomes as given in equation (9.7).

$$Q_3 = q_{A_2}(1-q_{B_1})q_{C_{23}}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_1})q_{C_3}(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{C_3} - q_{A_3}(1-q_{B_{12}})q_{C_3}(1-q_{D_{12}}) \tag{9.7}$$

The expected number of system failures in each phase of the example in Figure 9.1 can be obtained in the following way:

Phase 1

For the first phase of the mission, no previous component performance is considered. The expected number of phase 1 failures due to each phase 1 initiating event is obtained using equation (9.5), and is given in equation (9.8).

$$W_1^{I-P}(0,t_1)=\sum_{\substack{i=1\\ i\ phase\ 1\\ initiating\ event}}^{3}\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{i_1}}\right)\cdot w_{i_1}dt$$

$$=\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{A_1}}\right)\cdot w_{A_1}dt+\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{B_1}}\right)\cdot w_{B_1}dt+\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{C_1}}\right)\cdot w_{C_1}dt$$

$$=\int_0^{t_1}(1-q_{B_1})(1-q_{C_1})w_{A_1}+(1-q_{A_1})(1-q_{C_1})w_{B_1}+(1-q_{A_1})(1-q_{B_1})w_{C_1}\ dt \tag{9.8}$$

Phase 2

The second phase of the mission consists of enabling event (D), phase-specific initiating event (B), and non-phase specific initiating event (A). Phase 2 transition failure can only be caused by initiating event A if it occurs prior to phase 2 with component D failed. The expected number of phase transition failures is obtained using equation (9.4) and is given in equation (9.9).

$$W_2^{Tr}(t_1)=\int_0^{t_1}\left(\frac{\partial Q_2(q)}{\partial q_{A_1}}\right)\cdot w_{A_1}dt$$

$$=\int_0^{t_1}(0)\cdot w_{A_1}dt=0 \tag{9.9}$$

Failure in phase 2 can be caused by initiating events A or B if either occurs during phase 2 with component D failed. The expected number of in-phase system failures is obtained using equation (9.5), and is given in equation (9.10).

$$W_2^{I-p}(t_1,t_2)=\sum_{\substack{i=1\\ i\ \textit{phase 2}\\ \textit{initiating event}}}^{2}\int_{t_1}^{t_2}\left(\frac{\partial Q_2(q)}{\partial q_{i_2}}\right)\cdot w_{i_2}dt$$

$$=\int_{t_1}^{t_2}\left(\frac{\partial Q_2(q)}{\partial q_{A_2}}\right)\cdot w_{A_2}dt+\int_{t_1}^{t_2}\left(\frac{\partial Q_2(q)}{\partial q_{B_2}}\right)\cdot w_{B_2}dt$$

$$=\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{A_2}dt+\int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{B_2}dt \tag{9.10}$$

The total expected number of phase 2 failures is obtained by the sum of the contributions of both the expected number of phase 2 transition failures (equation (9.9)) and the expected number of in-phase 2 failures (equation (9.10)), and is summarised in equation (9.11).

$$W_2(t_1,t_2)=W_2^{Tr}(t_1)+W_2^{I-p}(t_1,t_2)$$

$$=0+\left(\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{A_2}dt+\int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{B_2}dt\right) \tag{9.11}$$

Alternatively the total number of phase 2 failures could be obtained directly using equation (9.6).

Phase 3

The third phase of the mission consists of enabling event A in a sequential failure configuration with non-phase specific initiating event C. Phase 3 failure can be caused by initiating event C either at the phase transition if it occurs prior to phase 3 with component A failed, or during phase 3 if it occurs in phase 3 with component A failed.

The expected number of transition system failures is obtained using equation (9.4), and is given in equation (9.12).

$$\begin{aligned} W_3^{Tr}(t_2) &= \sum_{k=1}^{k=2} \int_{t_{k-1}}^{t_k} \left(\frac{\partial Q_3(q)}{\partial q_{C_k}} \right) \cdot w_{C_k} dt \\ &= \int_0^{t_1} \left(\frac{\partial Q_3(q)}{\partial q_{C_1}} \right) \cdot w_{C_1} dt + \int_{t_1}^{t_2} \left(\frac{\partial Q_3(q)}{\partial q_{C_2}} \right) \cdot w_{C_2} dt \\ &= \int_0^{t_1} 0 \cdot w_{C_1} dt + \int_{t_1}^{t_2} \left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}}) \right) \cdot w_{C_2} dt \qquad (9.12) \end{aligned}$$

The expected number of in-phase system failures is obtained using equation (9.5) and is given in equation (9.13).

$$\begin{aligned} W_3^{I-p}(t_2,t_3) &= \int_{t_2}^{t_3} \left(\frac{\partial Q_3(q)}{\partial q_{C_3}} \right) \cdot w_{C_3} dt \\ &= \int_{t_2}^{t_3} \left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}} \right) \cdot w_{C_3} dt \qquad (9.13) \end{aligned}$$

The total expected number of phase 3 failures is obtained by sum of the contributions of both the expected number of phase 3 transition failures (equation (9.12)), and the expected number of in-phase 3 failures (equation (9.13)), and is summarised in equation (9.14).

$$\begin{aligned} W_3(t_2,t_3) &= W_3^{Tr}(t_2) + W_3^{I-p}(t_2,t_3) \\ &= \int_{t_1}^{t_2} \left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}}) \right) \cdot w_{C_2} dt + \int_{t_2}^{t_3} \left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}} \right) \cdot w_{C_3} dt \end{aligned}$$

$$(9.14)$$

Alternatively the total number of phase 3 failures could be obtained directly using equation (9.6).

9.2.2 Measures of Initiator Importance

Barlow and Proschan presented a time-dependent approach in analysing the importance of initiating events in a single phase system (Section 2.2.3.5.3). If only one component can fail in a small transition of time *dt*, then system failure must have occurred due to the failure of that component. The Barlow-Proschan measure of importance defined a method to calculate the probability that initiating event *i* causes system failure over the interval $[0,t)$. This was given in terms of the criticality function and weighted according to the expected number of failures, $W(0,t)$, in equation (2.31).

The Barlow-Proschan measure of importance is extended to give two new importance measures for phased mission analysis. The first is the *measure of in-phase initiator importance*, $I_{i_j}^{BP(I-p)}$. This is the probability that initiating event i causes system failure during phase j $[t_{j-1}, t_j)$. The second is the *measure of phase transition initiator importance*, $I_{i_j}^{BP(Tr)}$, and is the probability that initiating event i causes system failure at the transition into phase j due to failure in a previous phase. The total *measure of phase initiator importance,* $I_{i_j}^{BP}$, is the sum of the contribution of in-phase and phase transition initiator importances.

A phase j specific initiating event can only cause system failure if it occurs during phase j. All other initiating events can cause system failure by occurring prior to or during phase j. The phase j failure probability, Q_j, includes contribution of all possible component failure combinations with account for sequential failures. The measure of in-phase j importance for initiating event i, $I_{i_j}^{BP(I-p)}$, can be derived from equation (2.31) and is given in equation (9.15).

$$I_{i_j}^{BP(I-p)} = \frac{\int_{t_{j-1}}^{t_j} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_j}(t)} \right) w_{i_j} dt}{W_j(t_{j-1}, t_j)} \tag{9.15}$$

The measure of phase j transition importance for initiating event i, $I_{i_j}^{BP(Tr)}$, is the probability that initiating event i causes system failure at t_{j-1} due to failure of the initiating event in any phase k up to but not including phase j. This is derived and given in equation (9.16).

$$I_{i_j}^{BP(Tr)} = \frac{\sum_{k=1}^{j-1} \int_{t_{k-1}}^{t_k} \left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)} \right) w_{i_k} dt}{W_j(t_{j-1}, t_j)} \tag{9.16}$$

The total measure of phase initiator importance is found by the sum of the contribution of in-phase and phase transition initiator importances (equations (9.15) and (9.16)) in equation (9.17).

$$I_{i_j}^{BP}=\frac{\sum_{k=1}^{j}\int_{t_{k-1}}^{t_k}\left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)}\right)w_{i_k}\,dt}{W_j(t_{j-1},t_j)} \tag{9.17}$$

The measures of phase initiator importance may be applied to the initiating events of the example in Figure 9.1 in the following way:

Phase 1

The measure of phase initiator importance due to each phase 1 initiating event is given in equations (9.18).

$$I_{A_1}^{BP(I-p)}=\frac{\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{A_1}}\right)w_{A_1}dt}{W_1(0,t_1)}=\frac{\int_0^{t_1}(1-q_{B_1})(1-q_{C_1})w_{A_1}dt}{\int_0^{t_1}(1-q_{B_1})(1-q_{C_1})w_{A_1}+(1-q_{A_1})(1-q_{C_1})w_{B_1}+(1-q_{A_1})(1-q_{B_1})w_{C_1}\;dt}$$

$$I_{B_1}^{BP(I-p)}=\frac{\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{B_1}}\right)w_{B_1}dt}{W_1(0,t_1)}=\frac{\int_0^{t_1}(1-q_{A_1})(1-q_{C_1})w_{B_1}dt}{\int_0^{t_1}(1-q_{B_1})(1-q_{C_1})w_{A_1}+(1-q_{A_1})(1-q_{C_1})w_{B_1}+(1-q_{A_1})(1-q_{B_1})w_{C_1}\;dt}$$

$$I_{C_1}^{BP(I-p)}=\frac{\int_0^{t_1}\left(\frac{\partial Q_1(q)}{\partial q_{C_1}}\right)w_{C_1}dt}{W_1(0,t_1)}=\frac{\int_0^{t_1}(1-q_{A_1})(1-q_{B_1})w_{C_1}dt}{\int_0^{t_1}(1-q_{B_1})(1-q_{C_1})w_{A_1}+(1-q_{A_1})(1-q_{C_1})w_{B_1}+(1-q_{A_1})(1-q_{B_1})w_{C_1}\;dt}$$

(9.18)

Phase 2

The second phase of the mission consists of two initiating events, phase-specific initiating event (B), and non-phase specific initiating event (A). The Barlow-Proschan measure of phase initiator importance for events B and A are given in equations (9.19) and (9.20) respectively.

$$I_{B_2}{}^{BP} = I_{B_2}{}^{BP(I-p)} = \frac{\int_{t_1}^{t_2}\left(\frac{\partial Q_2(q)}{\partial q_{B_2}}\right)w_{B_2}\,dt}{W_2(t_1,t_2)} = \frac{\int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)w_{B_2}\,dt}{\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{A_2}\,dt + \int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{B_2}\,dt} \qquad (9.19)$$

$$I_{A_2}{}^{BP(Tr)} = \frac{\int_{0}^{t_1}\left(\frac{\partial Q_2(q)}{\partial q_{A_1}}\right)w_{A_1}\,dt}{W_2(t_1,t_2)} = \frac{\int_{0}^{t_1}\{0\}w_{A_1}\,dt}{\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{A_2}\,dt + \int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{B_2}\,dt} = 0$$

$$I_{A_2}{}^{BP} = I_{A_2}{}^{BP(I-p)} = \frac{\int_{t_1}^{t_2}\left(\frac{\partial Q_2(q)}{\partial q_{A_2}}\right)w_{A_2}\,dt}{W_2(t_1,t_2)} = \frac{\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)w_{A_2}\,dt}{\int_{t_1}^{t_2}\left((1-q_{B_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{A_2}\,dt + \int_{t_1}^{t_2}\left((1-q_{A_{12}})(1-q_{C_1})q_{D_{12}}\right)\cdot w_{B_2}\,dt} \qquad (9.20)$$

Phase 3

The third phase of the mission consists of only one initiating event, non-phase specific initiating event C. Phase 3 failure can be caused by initiating event C if it occurs prior to or during the phase with component A already failed. The Barlow-Proschan measure of phase initiator importance for event C in phase 3 is given in equation (9.21).

$$I_{C_3}{}^{BP(Tr)} = \frac{\sum_{k=1}^{2}\int_{t_{k-1}}^{t_k}\left(\frac{\partial Q_3(q)}{\partial q_{C_k}}\right)w_{C_k}\,dt}{W_3(t_2,t_3)} = \frac{\int_{0}^{t_1}\{0\}w_{A_1}\,dt + \int_{t_1}^{t_2}\left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\right)w_{C_2}\,dt}{\int_{t_1}^{t_2}\left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\right)\cdot w_{C_2}\,dt + \int_{t_2}^{t_3}\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\right)\cdot w_{C_3}\,dt}$$

$$I_{C_3}{}^{BP(I-p)} = \frac{\int_{t_2}^{t_3}\left(\frac{\partial Q_3(q)}{\partial q_{C_3}}\right)w_{C_3}\,dt}{W_3(t_2,t_3)} = \frac{\int_{t_2}^{t_3}\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\right)w_{C_3}\,dt}{\int_{t_1}^{t_2}\left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\right)\cdot w_{C_2}\,dt + \int_{t_2}^{t_3}\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\right)\cdot w_{C_3}\,dt}$$

$$I_{C_3}{}^{BP} = I_{C_3}{}^{BP(Tr)} + I_{C_3}{}^{BP(I-p)} = \frac{\int_{t_1}^{t_2}\left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\right)w_{C_2}\,dt + \int_{t_2}^{t_3}\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\right)w_{C_3}\,dt}{\int_{t_1}^{t_2}\left(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\right)\cdot w_{C_2}\,dt + \int_{t_2}^{t_3}\left(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\right)\cdot w_{C_3}\,dt} = 1$$

(9.21)

It is possible to obtain a measure of the initiator importance of each component in the entire mission. This is defined as the probability that initiating event *i* causes system failure during any phase *j*, $[t_{j-1}, t_j)$, of a multi-phased mission (weighted by the expected number of mission failures). The measure of mission initiator importance is obtained by the sum of each individual phase *j* initiator importance given that phase *j* has been reached successfully in equation (9.22).

$$I_{i_{MISS}}{}^{BP} = \sum_{j=1}^{m} \text{P(Initiating event } i \text{ causes system failure during phase } j \mid \text{in phase } j)$$

(weighted by the expected number of mission failures)

$$I_{i_{MISS}}{}^{BP} = \frac{\displaystyle\sum_{j=1}^{m}\sum_{k=1}^{j}\int_{t_{k-1}}^{t_k}\left(\frac{\partial Q_j(q(t))}{\partial q_{i_k}(t)}\right)w_{i_k}dt}{W_{MISS}(0,t_m)} \quad \text{where } W_{MISS}(0,t_m)=\sum_{j=1}^{m}W_j(t_{j-1},t_j) \qquad (9.22)$$

The total measures of phase importance for all initiating events in Figure 9.1 may be quantified and ranked using the mission data given in equations (8.23). Since the importance measures are time dependent, the equations are solved numerically and the Runge-Kutta method is used for solution. The results of this are summarised in Table 9.1.

Component	Phase 1 Initiator Importance	Rank	Phase 2 Initiator Importance	Rank	Phase 3 Initiator Importance	Rank	Mission Initiator Importance	Mission Rank
A	0.166666	3	0.328079	2	0	2	0.1838108	3
B	0.333332	2	0.671911	1	0	2	0.3719455	2
C	0.5	1	0	3	1	1	0.4442423	1
D	0	4	0	3	0	2	0	4
Expected Number of Failures	Phase 1		Phase 2		Phase 3		Mission	
	0.113068		0.0551839		0.0327668		0.2010187	

Table 9.1 Measure of Initiator Phase and Mission Importance

The measure of initiator importance ranks the probability that each initiating event *i* causes system failure during phase *j*. In phase 1, component C has the highest value of importance followed by components B and A. In phase 2 there are only 2 initiating events, A and B. Component B has a higher failure rate thus has a higher importance value during phase 2. Component C failure must be the initiating event to cause phase 3 failure, and so has an importance value of 1.

For the overall mission, component C has the highest initiator importance ranking followed by component B, and then components A and D. During the first and final phases it is most likely that component C causes system failure, and this is reflected in the overall mission rankings.

It is possible to compare the initiator importance values to those obtained by treating each phase as a separate system. The results are given in Table 9.2.

Component	Phase 1 Initiator Importance	Rank	Phase 2 Initiator Importance	Rank	Phase 3 Initiator Importance	Rank	Mission Initiator Importance	Mission Rank
A	0.166666	3	0.333337	2	0	2	0.2012932	3
B	0.333332	2	0.666674	1	0	2	0.4025858	1
C	0.5	1	0	3	1	1	0.3961247	2
D	0	4	0	3	0	2	0	4
Expected Number of Failures	Phase 1		Phase 2		Phase 3		Mission	
	0.113068		0.040313		0.0069945		0.1603755	

Table 9.2 Measure of Initiator Phase and Mission Importance when Treating each Phase as a Separate System

Comparisons between treating each phase as a separate system and combining previous phase success with current phase failure shows that the initiator importance rankings through the phases are identical, and the importance values are very similar for this simple example. However, as the phases progress, the expected number of failures is increasingly inconsistent. This is due to the fact that no account is taken of previous phase outcome and the assumption that all components are in the working state at the start of each phase. The inaccuracies in the expected number of phase and therefore mission failures are reflected in the mission initiator values which show greater inconsistencies.

9.2.3 Measures of Enabler Importance

In a sequential failure relationship, system failure will only be caused if the order of component failures occurs in the correct sequence. It is possible that the failure of a component can permit the failure of another component to cause system failure, but is not able to cause system failure alone. The Dunglinson-Lambert measure of enabler importance for a single phase system presented a method to approximate the probability that enabling event *e* permits an initiating event *i* to cause system failure over $[0,t)$ in equation (2.33). A new importance measure is presented to give the probability that enabling event *e* permits an initiating event *i* to cause system failure during phase *j*, $[t_{j-1}, t_j)$. This is an extension of the Dunglinson-Lambert measure and is defined as the *measure of phase enabler importance.*

We require the measure of enabler importance ($I_{e_j}{}^{DL}$) for enabling event *e* in phase *j*. This is the fraction of time that prime implicant sets containing event *e* have caused the top event to occur given that the top event has occurred. This can be expressed as two separate measures, the *measure of in-phase enabler importance*, and the *measure of phase transition enabler importance.*

The *measure of in-phase enabler importance*, $I_{e_j}{}^{DL(I-p)}$, is the probability that enabling event *e* permits an initiating event *i* to cause system failure during phase *j*. This is found by the expected number of phase *j* failures due to the union of all prime implicant sets ε_{k_j} with contribution of enabling event *e* and occurrence of initiating event *i* in phase *j*, and is weighted by the expected number of phase *j* failures in equation (9.23).

$$I_{e_j}{}^{DL(I-p)} = \frac{\sum_{i=1}^{N_I} \int_{t_{j-1}}^{t_j} P(\bigcup_{k_j|i_j,e\in k_j} E_{k_j(i_j)}) w_{i_j} dt}{W_j(t_{j-1},t_j)} \tag{9.23}$$

where $E_{k_j(i_j)}$ is the event that phase *j* prime implicant set ε_{k_j} occurs with initiating event *i* in phase *j* set to true

The *measure of phase transition enabler importance*, $I_{e_j}{}^{DL(Tr)}$, is the probability that enabling event *e* permits an initiating event *i* to cause phase *j* failure at the time of transition. This is found by the expected number of phase *j* failures due to the union of all prime implicant sets ε_{k_j} with contribution of enabling event *e* and occurrence of initiating event *i* in any phase *l* up to but not including phase *j*, and is weighted by the expected number of phase *j* failures in equation (9.24).

$$I_{e_j}{}^{DL} = \frac{\sum_{i=1}^{N_I} \int_{t_{l-1}}^{t_l} \sum_{l=1}^{j-1} P(\bigcup_{k_j|i_l,e\in k_j} E_{k_j(i_l)}) w_{i_l} dt}{W_j(t_{j-1},t_j)} \tag{9.24}$$

where $E_{k_j(i_l)}$ is the event that phase *j* prime implicant set ε_{k_j} occurs with initiating event *i* in phase *l* set to true

The total *measure of phase enabler importance*, $I_{e_j}{}^{DL}$, is obtained by the contribution of both the in-phase and phase transition enabler importances. This is the expected number of phase j failures due to the union of all prime implicant sets ε_{k_j} with contribution of enabling event *e* and occurrence of initiating event *i* in any phase *l* up to and including phase *j*, and is weighted by the expected number of phase j failures in equation (9.25).

$$I_{e_j}{}^{DL} = I_{e_j}{}^{DL(I-p)} + I_{e_j}{}^{DL(Tr)} = \frac{\sum_{i=1}^{N_l} \int_{t_{l-1}}^{t_l} \sum_{l=1}^{j} P(\bigcup_{k_j|i_l, e\in k_j} E_{k_j(i_l)}) w_{i_l} dt}{W_j(t_{j-1}, t_j)} \tag{9.25}$$

This approximation is demonstrated by application to the enabling events of the example in Figure 9.1 as follows:

Phase 1

Since the components are arranged in series, all events are initiating and there are no enabling events that can allow system failure in this first phase.

Phase 2

There are two phase 2 prime implicant sets:

$$\varepsilon_{1_2} = A_2 \overline{B_1 C_1} D_{12}$$

$$\varepsilon_{2_2} = \overline{A_1} B_2 \overline{C_1} D_{12}.$$

The phase enabler measure of importance for enabling event D in phase 2, $I_{D_2}{}^{DL}$, is given in equation (9.26).

$$I_{D_2}{}^{DL(Tr)} = \frac{\sum_{i=1}^{2} \int_{0}^{t_1} P(\bigcup_{k_2|i_1, D\in k_2} E_{k_2(i_1)}) w_{i_1} dt}{W_2(t_1, t_2)} = \frac{\int_0^{t_1} \left(\{0\}\cdot w_{A_1} + \{0\}\cdot w_{B_1}\right) dt}{\int_{t_1}^{t_2} \left((1-q_{B_{12}})(1-q_{C_1}) q_{D_{12}}\right)\cdot w_{A_2} dt + \int_{t_1}^{t_2} \left((1-q_{A_{12}})(1-q_{C_1}) q_{D_{12}}\right)\cdot w_{B_2} dt} = 0$$

$$I_{D_2}{}^{DL} = I_{D_2}{}^{DL(I-p)} = \frac{\sum_{i=1}^{2} \int_{t_1}^{t_2} P(\bigcup_{k_2|i_2, D\in k_2} E_{k_2(i_2)}) w_{i_2} dt}{W_2(t_1, t_2)} = \frac{\int_{t_1}^{t_2} \left((1-q_{B_{12}})(1-q_{C_1}) q_{D_{12}} w_{A_2} + (1-q_{A_{12}})(1-q_{C_1}) q_{D_{12}} w_{B_2}\right) dt}{\int_{t_1}^{t_2} \left((1-q_{B_{12}})(1-q_{C_1}) q_{D_{12}}\right)\cdot w_{A_2} dt + \int_{t_1}^{t_2} \left((1-q_{A_{12}})(1-q_{C_1}) q_{D_{12}}\right)\cdot w_{B_2} dt} = 1 \tag{9.26}$$

For phase 2 failure to occur, enabling event D must have occurred before either of initiating events A or B. This is consistent with the result of unity in equation (9.26).

Phase 3

There are four phase 3 prime implicant sets,

$$\begin{array}{l} A_2\overline{B_1}C_{23}\overline{D_{12}} \\ A_3\overline{B_1}C_3\overline{D_{12}} \\ A_3\overline{B_{12}}C_3 \end{array} \xrightarrow{\text{Expand}} \begin{array}{l} \varepsilon_{1_3} = A_2\overline{B_1}C_2\overline{D_{12}} \\ \varepsilon_{2_3} = A_2\overline{B_1}C_3\overline{D_{12}} \\ \varepsilon_{3_3} = A_3\overline{B_1}C_3\overline{D_{12}} \\ \varepsilon_{4_3} = A_3\overline{B_{12}}C_3 \end{array}$$

The measure of phase enabler importance ($I_{A_3}{}^{DL}$) for enabling event A in phase 3 is given in equation (9.27).

$$I_{A_3}{}^{DL(Tr)} = \frac{\sum_{l=1}^{2}\int_{t_{l-1}}^{t_l} P(\bigcup_{k_3|C_l,A\in k_3} E_{k_3})w_{C_l}dt}{W_3(t_2,t_3)} = \frac{\int_0^{t_1}\{0\}\cdot w_{C_2}dt + \int_{t_1}^{t_2} q_{A_2}(1-q_{B_1})(1-q_{D_{12}})w_{C_2}dt}{\int_{t_1}^{t_2}\Big(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\Big)\cdot w_{C_2}dt + \int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\Big)\cdot w_{C_3}dt}$$

$$I_{A_3}{}^{DL(I-p)} = \frac{\int_{t_2}^{t_3} P(\bigcup_{k_3|C_3,A\in k_3} E_{k_3})w_{C_3}dt}{W_3(t_2,t_3)} = \frac{\int_{t_2}^{t_3}\Big(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})w_{C_3} + q_{A_3}(1-q_{B_1})(1-q_{D_{12}})w_{C_3} + q_{A_3}(1-q_{B_{12}})w_{C_3} - q_{A_3}(1-q_{B_{12}})(1-q_{D_{12}})w_{C_3}\Big)dt}{\int_{t_1}^{t_2}\Big(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\Big)\cdot w_{C_2}dt + \int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\Big)\cdot w_{C_3}dt}$$

$$= \frac{\int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})w_{C_3} + q_{A_3}(1-q_{B_{12}})q_{D_{12}}w_{C_3}\Big)dt}{\int_{t_1}^{t_2}\Big(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\Big)\cdot w_{C_2}dt + \int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\Big)\cdot w_{C_3}dt}$$

$$I_{A_3}{}^{DL} = I_{A_3}{}^{DL(Tr)} + I_{A_3}{}^{DL(I-p)} = \frac{\sum_{l=1}^{3}\int_{t_{l-1}}^{t_l} P(\bigcup_{k_3|C_l,A\in k_3} E_{k_3})w_{C_l}dt}{W_3(t_2,t_3)} = \frac{\int_{t_1}^{t_2} q_{A_2}(1-q_{B_1})(1-q_{D_{12}})w_{C_2}dt + \int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})w_{C_3} + q_{A_3}(1-q_{B_{12}})q_{D_{12}}w_{C_3}\Big)dt}{\int_{t_1}^{t_2}\Big(q_{A_2}(1-q_{B_1})(1-q_{D_{12}})\Big)\cdot w_{C_2}dt + \int_{t_2}^{t_3}\Big(q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}}) + q_{A_3}(1-q_{B_{12}})q_{D_{12}}\Big)\cdot w_{C_3}dt} = 1 \qquad (9.27)$$

Phase 3 failure will only occur if enabling event A occurs before initiating event C. This is consistent with the result of unity in equation (9.27).

It is possible to obtain a measure of enabler importance of each component in the entire mission. This is defined as the probability that enabling event *e* permits an initiating event to cause system failure during any phase *j*, [t_{j-1}, t_j), of a multi-phased mission. The measure of mission enabler importance is obtained by the sum of each individual phase *j* enabler importance given that phase *j* has been reached successfully, and is weighted by the expected number of mission failures in equation (9.28).

$I_{e_{MISS}}{}^{DL} = \sum_{j=1}^{m}$ P(Enabling event *e* permits an initiating event to cause system failure during phase *j* | in phase *j*) (weighted by the expected number of mission failures)

$$I_{e_{MISS}}{}^{DL} = \frac{\sum_{i=1}^{N_l} \int_{t_{l-1}}^{t_l} \sum_{l=1}^{j} P(\bigcup_{k_j|i_l, e\in k_j} E_{k_j(i_l)}) w_{i_l} dt}{W_{MISS}(0,t_m)} \tag{9.28}$$

The total measures of phase importance for all enabling events in Figure 9.1 may be quantified using the Runge-Kutta method and ranked using the mission data given in equations (8.23). The results of this are summarised in Table 9.3.

Component	Phase 1 Enabler Importance	Rank	Phase 2 Enabler Importance			Rank	Phase 3 Enabler Importance	Rank	Mission Enabler Importance	Mission Rank
			Cut Set {D,B}	Cut Set {D,A}	Total					
A	0	-	0	0	-	-	1	1	0.16300374	2
B	0	-	0	0	-	-	0	-	0	-
C	0	-	0	0	-	-	0	-	0	-
D	0	-	0.671911	0.328079	1	1	0	-	0.27452123	1
Expected Number of Failures	Phase 1		Phase 2				Phase 3		Mission	
	0.113068		0.0551839				0.0327668		0.2010187	

Table 9.3 Measure of Enabler Phase and Mission Importance

The measure of enabler importance ranks the probability that enabling event *e* permits an initiating event to cause system failure during phase *j*. Since in this example there is never more than one enabling event in a phase, comparisons within individual phases cannot be made. However, it can be seen that the probability that enabling event D allows initiating event B to cause phase 2 failure is much greater than the probability that enabling event D allows initiating event A to cause phase 2 failure. This is due to the fact that initiating event B has a higher rate of occurrence.

For the overall mission, Component D has the highest ranking of enabler importance followed by component A. During the longest phase 2, it is most likely that component D allows an initiating event to cause system failure and this is reflected in the overall mission rankings.

It is possible to compare the enabler importance values to those obtained when treating each phase as a separate system. The results are given in Table 9.4.

Component	Phase 1 Enabler Importance	Rank	Phase 2 Enabler Importance			Rank	Phase 3 Enabler Importance	Rank	Mission Enabler Importance	Mission Rank
			Cut Set {D,B}	Cut Set {D,A}	Total					
A	0	-	0	0	-	-	1	1	0.04361321	2
B	0	-	0	0	-	-	0	-	0	-
C	0	-	0	0	-	-	0	-	0	-
D	0	-	0.666674	0.333337	1	1	0	-	0.25136634	1
Expected Number of Failures	Phase 1		Phase 2				Phase 3		Mission	
	0.113068		0.040313				0.0069945		0.1603755	

Table 9.4 Measure of Enabler Phase and Mission Importance when Treating each Phase as a Separate System

Comparisons between treating each phase as a separate system with the combination of previous phase success with current phase failure show that the importance rankings through the phases are identical and the values are very similar. However, a larger inconsistency is seen in the mission importance values. This is again due to the increasing inaccuracy of the expected number of phase failures as the phases progress.

9.3 Repairable Systems

The importance measures presented in the previous sections can be applied to repairable as well as non-repairable systems. If a Markov model is implemented for solution to a repairable multi-phased mission, the model state probabilities can be used to calculate the importance of components rather than using the combinatorial approaches described previously in this chapter.

Methods to assess the probabilistic repairable component importance with Markov models are presented in the following sections.

9.3.1 Probabilistic Measures of Importance

Probabilistic measures of importance for phased mission systems where the order of component failures in a minimal cut set is irrelevant (Section 8.3) can be demonstrated by example to the second phase of a simple 2-phased mission, given in Figure 9.2. The Markov model for the repairable second phase is given in Figure 9.3.

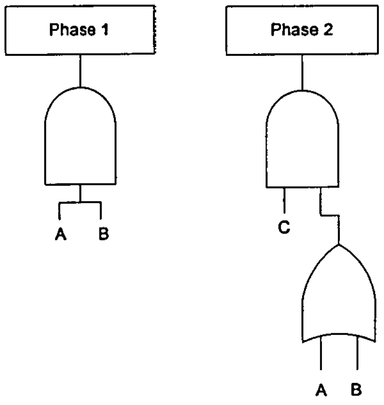


Figure 9.2 Example 2-Phase Mission

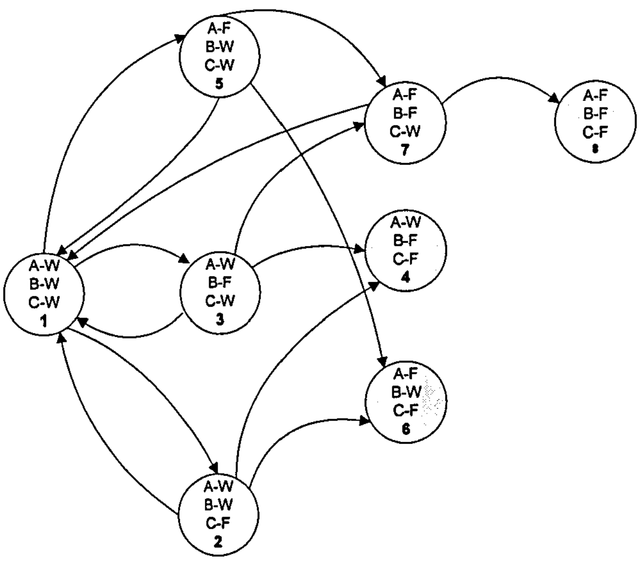


Figure 9.3 Phase 2 Markov model

The initial state probabilities of this phase 2 Markov model are determined by the final Markov system state probabilities at the end of phase 1 using the methods presented in Chapter 5. The importance measures can then be calculated using only the phase 2 Markov model since the previous phase is accounted for in the initial phase system state probability vector.

The unavailability of the system at time t in phase j, $Q_j(t)$, can be calculated as the sum of the probabilities that the system resides in an absorbing phase j failure state at time t. This is summarised in equation (9.29).

$$Q_j(t) = \sum_{\substack{s \text{ all phase } j \\ \text{failure states}}} P_s(t) \tag{9.29}$$

where t is measured from the start of the mission

For the example in Figure 9.3, the unavailability at time t in phase 2 would be found by the sum of the probabilities that the system resides in an absorbing phase 2 failure state (**4**, **6**, or **8**) at time t in equation (9.30).

$$Q_2(t) = P_4(t) + P_6(t) + P_8(t) \tag{9.30}$$

9.3.1.1 Phase Criticality Function

The phase j criticality function for a component c is the probability that the system is in a critical state for component c in phase j at time t. The Markov model states can be identified that are critical for component c such that if component c fails, transition to an absorbing phase failure state will occur. The criticality function for component c in phase j at time t is given in equation (9.31).

$$G_{c_j}(q(t)) = \sum_{\substack{s \text{ all phase } j \\ \text{critical states for } c}} P_s(t) \tag{9.31}$$

This measure may be demonstrated by application to the phase 2 Markov model in Figure 9.3. The critical states for components A, B, and C can be identified as:

Component	Critical States
A	**2**
B	**2**
C	**3, 5, 7**

The criticality function for each of the components at time t in phase 2 is calculated in equations (9.32).

$$G_{A_2}(q(t)) = P_2(t) \qquad G_{B_2}(q(t)) = P_2(t) \qquad G_{C_2}(q(t)) = P_3(t) + P_5(t) + P_7(t) \quad (9.32)$$

9.3.1.2 Criticality Measure of Phase Component Importance

The criticality measure of importance for component c in phase j is the probability that the system is in a critical state for component c in phase j, and c fails. Using a Markov model, this is the sum of the probabilities that the system is a critical phase j Markov system state for component c at time t, and component c fails. This is obtained using the phase j criticality function for component c at time t and is weighted by the phase j unavailability at time t in equation (9.33).

$$I_{c_j}{}^{CR}(t) = \frac{G_{c_j}(q(t)) \cdot q_c(t)}{Q_j(t)} \qquad \text{where} \qquad q_c(t) = \frac{\lambda_c}{\lambda_c + \upsilon_c}(1 - e^{-(\lambda_c + \upsilon_c)t}) \qquad (9.33)$$

The criticality measure of importance for components A, B, and C in the example in Figure 9.3 are given in equations (9.34).

$$I_{A_2}{}^{CR}(t) = \frac{G_{A_2}(q(t)) \cdot q_A(t)}{Q_2(t)} = \frac{P_2(t) \cdot q_A(t)}{Q_2(t)}$$

$$I_{B_2}{}^{CR}(t) = \frac{G_{B_2}(q(t)) \cdot q_B(t)}{Q_2(t)} = \frac{P_2(t) \cdot q_B(t)}{Q_2(t)}$$

$$I_{C_2}{}^{CR}(t) = \frac{G_{C_2}(q(t)) \cdot q_C(t)}{Q_2(t)} = \frac{(P_3(t) + P_5(t) + P_7(t)) \cdot q_C(t)}{Q_2(t)}$$

(9.34)

9.3.1.3 Measure of Phase Component Importance

The measure of phase component importance is the probability of the union of phase j minimal cut set occurrences, C_{k_j}, containing the failure of component c given that phase j failure has occurred. Using a Markov model, this is the sum of the probabilities that the system resides in an absorbing failure state representative of the existence of minimal cut sets C_{k_j} at time t in phase j, and is weighted by the phase j failure probability at time t in equation (9.35).

$$I_{c_j}^{FV}(t) = \frac{\sum\limits_{\substack{s \text{ all phase } j \text{ states} \\ \text{representing existence of } C_{k_j} \\ \text{where } c \in C_{k_j}}} P_s(t)}{Q_j(t)} \tag{9.35}$$

This measure may be demonstrated by application to the example in Figure 9.3. The measures of phase importance for components A, B, and C are obtained in equations (9.36).

Component	Cut Sets Including Component	States Representing Existence of Cut Set
A	{A, C}	**6, 8**
B	{B, C}	**4, 8**
C	{A, C},{B, C}	**4, 6, 8**

$$I_{A_2}^{FV}(t) = \frac{P_6(t) + P_8(t)}{Q_2(t)} \quad I_{B_2}^{FV}(t) = \frac{P_4(t) + P_8(t)}{Q_2(t)} \quad I_{C_2}^{FV}(t) = \frac{P_4(t) + P_6(t) + P_8(t)}{Q_2(t)} \tag{9.36}$$

9.3.1.4 Measure of Minimal Cut Set Importance

The measure of phase minimal cut set importance is the probability of the existence of minimal cut set C_{k_j} given that phase j has failed. For a repairable system represented by a Markov model, this is the sum of the probabilities that the system resides in an absorbing failure state due to the occurrence of minimal cut set C_{k_j} at time t, and is weighted by the phase j system failure probability at time t in equation (9.37).

$$I_{C_{k_j}}^{FV}(t) = \frac{\sum\limits_{\substack{s \text{ all phase } j \\ \text{states representing} \\ \text{existence of } C_{k_j}}} P_s(t)}{Q_j(t)} \tag{9.37}$$

The measure of minimal cut set importance for each of the minimal cut sets in the phase 2 Markov model in Figure 9.3 is obtained in equations (9.38).

Phase 2 Minimal Cut Sets: $1_2 = \{A, C\}$
$2_2 = \{B, C\}$

$$I_{1_2}^{FV}(t) = \frac{P_6(t) + P_8(t)}{Q_2(t)} \qquad I_{2_2}^{FV}(t) = \frac{P_4(t) + P_8(t)}{Q_2(t)} \qquad (9.38)$$

9.3.2 Probabilistic Measures for Initiating and Enabling Events

Probabilistic measures of importance for phased mission systems where the order of component failures in a minimal cut set is important (Section 9.2) can be demonstrated for a repairable system using an extension of the example in Figure 9.2, shown in Figure 9.4. The Markov model for the second phase is given in Figure 9.5.

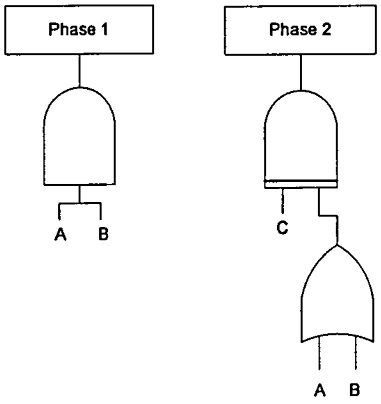


Figure 9.4 Example 2-Phase Mission

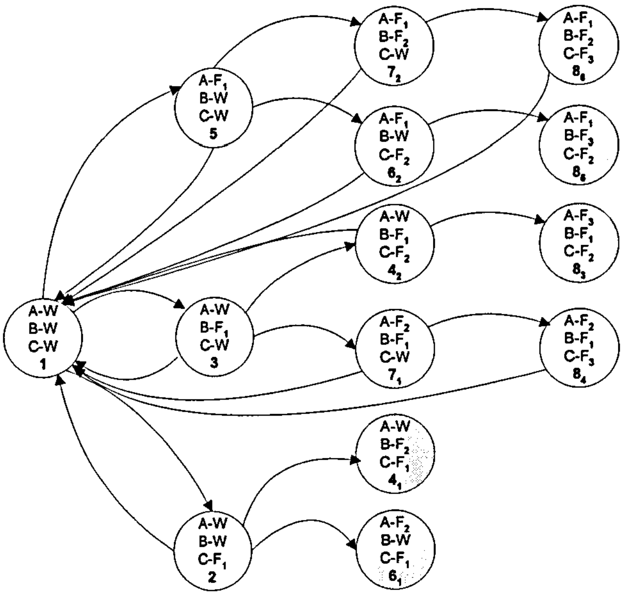

A-W B-W C-W 1
A-F$_1$ B-W C-W 5
A-W B-F$_1$ C-W 3
A-W B-W C-F$_1$ 2
A-F$_1$ B-F$_2$ C-W 7_2
A-F$_1$ B-W C-F$_2$ 6_2
A-W B-F$_1$ C-F$_2$ 4_2
A-F$_2$ B-F$_1$ C-W 7_1
A-W B-F$_2$ C-F$_1$ 4_1
A-F$_2$ B-W C-F$_1$ 6_1
A-F$_1$ B-F$_2$ C-F$_3$ 8_6
A-F$_1$ B-F$_3$ C-F$_2$ 8_5
A-F$_3$ B-F$_1$ C-F$_2$ 8_3
A-F$_2$ B-F$_1$ C-F$_3$ 8_4

Figure 9.5 Phase 2 Markov model

9.3.2.1 Expected Number of Phase Failures

The rate of phase j failure, $w_j(t)$, is the rate that phase j failure occurs at time t between $[t_{j-1}, t_j)$. Using a Markov model, this may be found by the sum of the probabilities that the system is in a critical state for initiating event i at time t, and the frequency that event i occurs at time t in equation (9.39).

$$w_j(t) = \sum_{\substack{i\ phase\ j\\ initiating\ event}} G_{i_j}(q(t)) \cdot \lambda_i \qquad \text{where } G_{i_j}(q(t)) = \sum_{\substack{s\ all\ phase\ j\\ critical\ states\ for\ i}} P_s(t) \qquad (9.39)$$

The expected number of phase j failures is the integral of the unconditional phase j failure intensity (equation (9.39)) over the time interval $[t_{j-1}, t_j)$, and is given in equation (9.40).

$$\begin{aligned} W_j(t_{j-1}, t_j) &= \int_{t_{j-1}}^{t_j} w_j(t)\, dt \\ &= \int_{t_{j-1}}^{t_j} \left(\sum_{\substack{i\ phase\ j\\ initiating\ event}} G_{i_j}(q(t)) \cdot \lambda_i \right) dt \qquad (9.40) \end{aligned}$$

In the example given in Figure 9.5, the initiating events are the failures of components A and B. The expected number of phase 2 failures can be obtained using the critical states for initiating events A and B and is given in equation (9.41):

Initiating Event	Critical States
A	**2, 4₂**
B	**2, 6₂**

$$W_2(t_1,t_2) = \int_{t_1}^{t_2} \sum_{\substack{i\ phase\ 2 \\ initiating\ event}} G_{i_2}(q(t))\cdot\lambda_i\ dt = \int_{t_1}^{t_2}\left(G_{A_2}(q(t))\cdot\lambda_A + G_{B_2}(q(t))\cdot\lambda_B\ \right)dt$$

where $G_{A_2}(q(t)) = P_2(t) + P_{4_2}(t)$

$G_{B_2}(q(t)) = P_2(t) + P_{6_2}(t)$

$$W_2(t_1,t_2) = \int_{t_1}^{t_2}\left(\left(P_2(t)+P_{4_2}(t)\right)\cdot\lambda_A + \left(P_2(t)+P_{6_2}(t)\right)\cdot\lambda_B\ \right)dt \qquad (9.41)$$

9.3.2.2 Measure of Phase Initiator Importance

The measure of phase initiator importance is the probability that initiating event *i* causes system failure during phase *j*. Using Markov models, this is the integral of the sum of the probabilities that the system is in a critical state for event *i* at time *t*, and the frequency that *i* occurs at time *t* in equation (9.42).

$$I_{i_j}{}^{BP} = \frac{\int_{t_{j-1}}^{t_j} G_{i_j}(q(t))\cdot\lambda_i dt}{W_j(t_{j-1},t_j)} \quad \text{where } G_{i_j}(q(t)) = \sum_{\substack{s\ all\ phase\ j \\ critical\ states\ for\ i}} P_s(t) \qquad (9.42)$$

The phase initiator importance for initiating events A and B in Figure 9.5 is obtained using equation (9.42) as follows:

$$I_{A_2}{}^{BP} = \frac{\int_{t_1}^{t_2} G_{A_2}(q(t))\cdot\lambda_A dt}{W_2(t_1,t_2)} \quad \text{where } G_{A_2}(q(t)) = P_2(t) + P_{4_2}(t)$$

$$I_{B_2}{}^{BP} = \frac{\int_{t_1}^{t_2} G_{B_2}(q(t))\cdot\lambda_B dt}{W_2(t_1,t_2)} \quad \text{where } G_{B_2}(q(t)) = P_2(t) + P_{6_2}(t)$$

(9.43)

9.3.2.3 Measure of Phase Enabler Importance

The measure of phase enabler importance ($I_{e_j}{}^{DL}$) for enabling event *e* in phase *j* is the expected number of failures due to the union of all phase *j* minimal cut sets C_{k_j} with contribution of enabling event *e*. Using a Markov model, this is the integral of the sum of the probabilities that the system is in a critical state for an initiating event *i* contributing to the same minimal cut set as *e*, multiplied by the rate of occurrence of *i*. This is weighted by the expected number of phase *j* failures and is given in equation (9.44).

$$I_{e_j}{}^{DL} = \frac{\int_{t_{j-1}}^{t_j} \sum_{i=1}^{N_I} \left\{ \sum_{\substack{s \text{ all phase } j \\ \text{critical states for } i \\ \text{such that } C_{k_j} \text{ will occur} \\ \text{if } i \text{ occurs, and } e \in C_{k_j}}} P_s(t) \right\} \lambda_i dt}{W_j(t_{j-1}, t_j)} \tag{9.44}$$

In the example shown in Figure 9.5, component C failure is the only enabling event. Enabling event C contributes to two sequential minimal cut sets, {C$^{(E)}$, A$^{(I)}$} and {C$^{(E)}$, B$^{(I)}$}. The critical system states for initiating events A and B such that the failure of either event would cause a minimal cut set containing C to occur are:

Initiating Event	Critical States for Occurrence of Cut Set Containing C
A	$2, 4_2$
B	$2, 6_2$

The measure of enabler importance for enabling event C in phase 2 is therefore:

$$I_{C_2}{}^{DL} = \frac{\int_{t_1}^{t_2} \sum_{i=1}^{2} \left\{ \sum_{\substack{s \text{ all phase} 2 \\ \text{critical states for } i \\ \text{such that } C_{k_j} \text{ will occur} \\ \text{if } i \text{ occurs, and } e \in C_{k_j}}} P_s(t) \right\} \lambda_i dt}{W_2(t_1, t_2)} = \frac{\int_{t_1}^{t_2} \left(\left(P_2(t) + P_{4_2}(t)\right) \cdot \lambda_A + \left(P_2(t) + P_{6_2}(t)\right) \cdot \lambda_B \right) dt}{W_2(t_1, t_2)} \tag{9.45}$$

9.3.3 Mission Importance Measures for Repairable Systems

The phase importance measures for a repairable system are obtained using separate phase models, and the outcome of the previous phases are accounted for in the initial system state probability vector. Since the duration of each phase is accounted for in the solution of each Markov model, the mission importance measures can be obtained as an average of the individual phase importance measures.

9.4 Summary

The importance measures presented for initiating and enabling events in single phase systems have been successfully developed to allow the assessment of component importance in multi-phased missions where the order of component failure is relevant. The probabilistic measures are weighted according to the expected number of phase failures.

For repairable systems, the Markov phase system state probabilities can be used to accurately assess the importance of both individual components and minimal cut sets, rather than the approximations obtained using combinatorial techniques.

Chapter 10 Conclusions and Further Work

10.1 Summary

The concept of a phased mission has been introduced as a sequential set of objectives that operate over different time intervals. During each phase of the mission, the system may alter such that the logic model, system configuration, or system failure characteristics may change to accomplish a required objective.

The unreliability of a phased mission cannot be obtained by the simple multiplication of the individual phase unreliabilities due to the fact that the system must occupy a state that allows both of the involved phases to function at the phase change times. The phases of a mission are statistically dependent. The event of component failure can be critical for either the phase in which it occurs, or for a later phase of the mission. As such it can be the transition from one phase to another that is the critical event leading to mission failure.

The most common existing techniques for solution to non-repairable phased mission systems are fault tree analysis and binary decision diagrams. Due to the potential system state explosion problem encountered when employing Markov methods, it is useful to be able to implement alternative combinatorial techniques. Many of the existing techniques also concentrate on the transformation of a multi-phased mission into an equivalent single phased mission. The main disadvantage identified in the existing approaches is that due to cut set cancellation between phases, it is not possible to accurately calculate the failure probability of individual phases, only the mission as a whole.

A new fault tree method has been proposed to overcome some of the deficiencies of other fault tree methods, and enable the probability of failure in each phase to be determined in addition to the whole mission unreliability. Phase changes are assumed to be instantaneous, and component failure rates are assumed to be constant through the mission. The basic events are expanded into a series of sub-events representing the separate performance of the component in each phase of the mission. For any phase, the method combines the causes of success of previous phases with the causes of failure for the phase being considered to allow both qualitative and quantitative analysis of both phase failure and mission failure. A new set of Boolean laws is introduced to combine component success and failure events through multiple phases so that the expression for each phase failure can be reduced into minimal form. The application of these laws allow the prime implicant sets to be obtained for each phase.

The fault tree structure efficiently represents the non-repairable phase failure logic, but is not an ideal form for mathematical analysis. The binary decision diagram (BDD) method offers an alternative approach to the fault tree method and reduces the complexity of the problem. For larger fault trees it is more efficient to convert to a BDD prior to analysis, and this is particularly true of the non-coherent phase failure fault trees. The standard BDD technique has been extended to develop a method for use in missions of multiple phases, allowing the exact phase and mission unreliability to be calculated.

The current importance measures defined for single phase systems have been developed for missions of multiple phases. This allows the importance of a component, minimal cut set, or prime implicant set to each individual phase and the entire mission to be calculated.

Markov methods are considered for analysis of phased missions where repair of components is possible, and also for situations that prevent the assumption of independence between component failure or repair being made. A full Markov model is generated by using a single model which works over all phases of the mission, and is constructed by the inclusion of all components featured in every stage. The model is formed by considering the different requirements for each phase success and mission success, and the state transition matrix is used to obtain the probability of the system residing in each of the possible system states. By identifying certain types of phases and components, it is possible to reduce this full Markov model further.

The phases of a mission may be characterised in certain ways. If a phase requires the relevant system function to work at an instant in time it is defined as discrete. No state transitions may occur during a discrete phase, and any component failures that exist would have occurred prior to the phase. A continuous phase requires the appropriate system configuration to be reliable for the specified phase duration.

The components in each phase may be non-repairable or repairable. The most simplistic repair model assumes that failures are detected instantly and upon repair a component is considered to be as good as new. However if a component is not monitored continuously, this assumption cannot be made. A maintenance policy is considered where components can be subject to scheduled inspection. In this case the failure of a component will occur unrevealed and remain in this state until it is revealed at the next scheduled inspection point, when it can be restored to good as new condition.

The concept of sequential failure relationships has been introduced to missions of multiple phases. Component failures can be identified as initiating or enabling events. The occurrence of an initiating event can directly cause phase failure, where as the occurrence of an enabling event can permit the failure of another component to cause phase failure, but is not able to cause system failure alone. The function of a component is subject to change through the mission duration.

Modified Markov methods have been presented to account for the possible types of phase, component, and maintenance policy, and the conclusions from this work are discussed in the following section.

10.2 Conclusions

The aim of this research was to consider analytical techniques for the efficient representation and solution of phased mission systems. The following conclusions are made:

10.2.1 Non-Repairable Missions

- The proposed fault tree technique for combining the causes of success of previous phases with the causes of failure for the phase being considered allows the phase failure probability to be determined in addition to the mission failure probability. This method is seen to be more suitable for the solution of systems which operate over a small number of phases. As the number of phases increases, this fault tree technique is susceptible to a large state explosion which leads to extra computational time and effort being required.

- Since each phase is obtained as a combination of current phase failure with previous phase successes, the basic events can represent either component failure or success in different phases. The top event of phase or mission failure can also contain multiple events belonging to the same component. A new set of Boolean laws is introduced which allows the expression for each phase failure to be reduced into minimal form, and the prime implicant sets to be obtained.

- The BDD approach is found to provide an efficient and accurate alternative to the fault tree technique. With an optimal ordering scheme, the combination of phase failure with previous phase successes can be very simple as the events of components failing through sequential phases are considered only once. The quantification of the binary decision diagram approach leads to an exact answer rather than the approximation calculated by the fault tree method.

- Once the phase or mission failure probability is calculated using either fault tree analysis or BDDs, the frequency of phase and mission failure can be easily obtained using the mission frequency.

- Standard deterministic and probabilistic importance measures for single phase systems have been successfully developed to allow the assessment of component importance in multi-phased missions. For non-repairable systems, the probabilistic measures can easily be obtained using combinatorial methods, and are weighted according to either the phase failure probability or expected number of phase failures as appropriate.

10.2.2 Repairable Missions

- The full Markov model generated by using a single model which works over all phases of the mission and constructed by the inclusion of all components featured in every stage can get very large and in some cases become too large to generate and solve. This full Markov model may be reduced in the following situations:

- **Discrete and Continuous Phases.** It is only the continuous phases where the reliability calculations necessitate the use of Markov methods. Components that only feature in discrete phases are segregated from those which contribute to the failure of continuous phases. Discrete phases can be solved using fault tree analysis and continuous phases can be solved using Markov models. Only components contributing to each phase failure are included in the model. The full set of states for the total mission are reduced to evaluate initial conditions for each phase, and expanded out again at the end of a phase to enable calculation of successful entry to the immediately succeeding phase.

- **Non-Repairable and Repairable Phases.** A non-repairable phase can be solved using standard fault tree techniques, and a repairable phase can be solved by application of a minimal Markov model. The expansion of the state probabilities at the end of each phase allows the unavailability or availability of all components to be calculated for transition to the next phase, and thus any sequence of repairable and non-repairable phases can be modelled.

- **Scheduled Inspection.** A scheduled inspection routine is introduced for components that are not monitored continuously. The Markov model states for each phase of the mission can be expanded to represent the possibility of both unrevealed and revealed component failures.

- **Initiating and Enabling Events.** The consideration of sequential failure relationships in phased mission Markov analysis is susceptible to state explosion problems, and so a minimal model is defined at each transition point. Initiating events that can only cause system failure by occurring in a particular phase are defined as phase specific. All components that do not contribute to any further phases of the mission may be removed completely from the transition model at each phase boundary. All remaining components that do not contribute to any non-phase specific sequential minimal cut sets in later phases are expressed in non-sequential form, and all components that do contribute to a later non-phase specific sequential minimal cut set must remain in sequential form. The model can then be expanded to represent phase specific failure relationships within each phase. If components do not contribute to non-phase specific sequential minimal cut sets in later phases, it is possible to remove them from the model during phases in which they are not required, and also apply fault tree techniques where they are input to static gates in non-repairable phases.

- If a system is too complex to use deterministic analysis, or if the failure or repair distributions of a component do not have a constant failure or repair rate, simulation may be necessary. Simulation techniques typically offer the greatest generality in representation, but are also often the most expensive in computational requirements.

- The importance measures for non-repairable multi-phased missions have been extended to include the possibility of repair. Where systems are repairable, the Markov system state probabilities can be used to assess the importance of both individual components and minimal cut sets.

10.3 Further Work

The scope of this research leads to the possibility of further areas of investigation. Potential directions are discussed in the following sections.

10.3.1 Optimum BDD Ordering Schemes

The effect of basic event ordering schemes in single phase system BDDs has been subject to much research. Since the BDD approach can also be applied to non-repairable multi-phased missions, it would be useful to be able to obtain an optimal event ordering scheme to result in the most accurate and efficient phased mission BDD.

10.3.2 Dependency

The assumption that components are independent is not always practicable. In some situations it is possible that the failure of a component may depend on the state of another component, in which case this assumption no longer holds. The current research into dependencies within single phase systems could be extended for application to multi-phased missions.

10.3.3 Varying Failure Rates

The methods presented for solution to phased mission systems assume that the failure and repair rates of a component remain constant throughout the mission duration. It is possible that the requirements of a phase may cause an increase or decrease in the failure or repair rate of a component. Modifications of the current method can be made to allow for the possible change in failure or repair rate of a component between phases.

10.3.4 Phase Sequences

The research in this thesis has assumed that the phases in a mission occur in a set order. In reality, this may not be true. Depending on the outcome of a phase, the immediately succeeding phase may be different. An extension of the current methods could allow for any combination of phase patterns depending on the outcome of each phase.

10.3.5 Variable Phase Durations

The proposed methods for phased mission analysis assume that each phase is of a fixed time duration. In some cases it is possible that the interval over which a phase operates can be variable, for example if a phase transition will only occur due to the system reaching a particular state. It would be useful to extend the current techniques to allow for the possibility of variable phase durations.

10.3.6 Delayed Phase Transitions

The assumption that the transition between phases is instantaneous cannot always be made. It is possible that a delayed time period between phase boundaries can occur, for example due to the replacement of components. The current method could be modified to include the situations where phase transitions are not instantaneous.

10.3.7 Phase Consequences

The research in this thesis does not consider the consequence of each phase failure. In reality components would be more important in phases where failure has catastrophic consequences. Extensions could be made to this work to consider the consequence of each phase failure.

References

[1] J.D. Andrews, T.R. Moss, 'Reliability and Risk Assessment', 2nd Edition, Professional Engineering Publishing Limited, 2002.

[2] E.J. Henley, H. Kumamoto, 'Probabilistic Risk Assessment', IEEE Press, 1992.

[3] W.E. Vesely, 'A Time-Dependent Methodology for Fault Tree Evaluation', *Nuclear Design and Engineering*, vol. 13, 1970, pp 337-360.

[4] A. Rauzy, "New Algorithms for Fault Tree Analysis", *Reliability Engineering and System Safety*, vol 40, 1993, pp203-211.

[5] Z.W. Birnbaum, "On the Importance of Different Components in a Multicomponent System", *Multivariate Analysis II*, Academic Press, pp581-592, 1969.

[6] J.B. Fussell, "How to Hand Calculate System Reliability and Safety Characteristics", *IEEE Trans. Rel.*, vol. R-24, no. 3, pp. 169-174, Aug 1975.

[7] H.E. Lambert, "Measures of Importance of Events and Cut Sets in Fault Trees", In *Reliability and Fault Tree Analysis*, eds. R.E.Barlow, J.B. Fussell and N.D. Singpurwalla. SIAM Press, Philadelphia, 1975, pp. 77-100.

[8] S. Beeson, J.D. Andrews, "Importance Measures for Non-coherent System Analysis", *IEEE Trans. Rel.*, vol. 52, no. 3, pp. 301-310, Sept 2003.

[9] C. Dunglinson, H. Lambert, "Interval Reliability for Initiating and Enabling Events", *IEEE Trans. Rel.*, vol. R-32, no. 2, pp. 150-163, June 1983.

[10] R.M. Sinnamon, J.D. Andrews, "Improved Efficiency in Qualitative Fault Tree Analysis", *Quality and Reliability Engineering Int.*, vol 13, no. 5, 1997, pp 293-298.

[11] R.M. Sinnamon, J.D. Andrews, "Improved Accuracy in Quantitative Fault Tree Analysis", *Quality and Reliability Engineering Int.*, vol 13, no. 5, 1997, pp 285-292.

[12] J.D.Esary, H. Ziehms, "Reliability of Phased Missions", *Reliability and Fault-Tree Analysis*, Society for Industrial Applied Mathematics, Phila. 1975, pp 213-236, 1974 September.

[13] G.R Burdick, J.B.Fussell, D.M.Rasmuson, J.R.Wilson, "Phased Mission Analysis: A Review of New Developments and an Application", *IEEE Trans. Reliability,* vol R-26, 1977 Apr, pp 43-49.

[14] M. H. Veatch, "Reliability of Periodic, Coherent, Binary Systems", *IEEE Trans. Reliability,* vol R-35, 1986 Dec, pp 504-507.

[15] M. Vujosevic, D. Meade, "Reliability Evaluation and Optimization of Redundant Dynamic Systems", *IEEE Trans. Reliability*, vol. R-34, no. 2, June 1985, pp 171-174.

[16] Kang W. Lee, Jung S. Hong, "Reliability of a Phased Mission System with Time-Varying Redundancy and Failure", *Microelectronic Reliability,* vol 31, 1991, pp 955-961.

[17] D.F.Montague, J.B.Fussell, "A Methodology for Calculating the Expected Number of Failures of a System Undergoing a Phased Mission", *Nuclear Science and Engineering,* vol 74, 1980, pp 199-209.

[18] Xue Dazhi, Wang Xiaozhong, "A Practical Approach for Phased Mission Analysis", *Reliability Engineering and System Safety,* vol 25, 1989, pp 333-347.

[19] T.Kohda, M. Wada, K. Inoue, "A Simple Method for Phased Mission Analysis", *Reliability Engineering and System Safety*, vol 45, 1994, pp 299-309.

[20] A.K.Somani, K.S.Trivedi, "Boolean Algebraic Methods for Phased-Mission System Analysis", in *Proceedings of Sigmetrics*, 1994 May, pp 98-107.

[21] Y.Ma, K.S.Trivedi, "An algorithm for reliability of phased-mission systems", *Reliability Engineering and System Safety*, vol 66, 1999, pp 157-170.

[22] Xinyu Zang, Hairong Sun, Kishor S. Trivedi "A Bdd-Based Algorithm for Reliability Analysis of Phased-Mission Systems", *IEEE Trans. Reliability,* vol 48, 1999 March, pp 50-60.

[23] J. Bechta Dugan, L. Xing, "Comments on PMS BDD Generation in 'A BDD-Based Algorithm for Reliability Analysis of Phased-Mission Systems' [2]", *IEEE Trans. Reliability*, vol 53, no. 2, June 2004, pp 169-173.

[24] J. Dugan, L. Xing, "Analysis of Generalised Phased-Mission System Reliability, Performance, and Sensitivity" *IEEE Trans. Reliability,* vol 51, no. 2, June 2002, pp199-211

[25] J. Bechta Dugan, L. Xing, "A Seperable Ternary Decision Diagram Based Analysis of Phased-Mission Reliability", *IEEE Trans. Reliability*, vol 53, no. 2, June 2004, pp 174-184.

[26] Joanne Bechta Dugan, "Automated Analysis of Phased Mission Reliability", *IEEE Trans. Reliability,* vol. 40, 1991 Apr, pp 45-52.

[27] Y. Ou, J. Bechta Dugan, "Modular Solution of Dynamic Multi-Phase Systems", *IEEE Trans. Reliability*, vol. 53, no.4, Dec 2004, pp 499-508.

[28] Arun Somani, "Simplified Phased Mission Analysis for Systems with Independent Component Repairs", *Int. J. Reliability Quality Safety Eng.*, vol 4, 1997, pp 167-191.

[29] J. K. Vaurio, "Fault Tree Analysis of Phased Mission Systems with Repairable and Non-Repairable Components", *Reliability Engineering and System Safety,* 2001, pp 169-180.

[30] C.A.Clarotti, S.Contini, R.Somma, "Repairable Multiphase Systems - Markov and Fault-Tree Approaches for Reliability Evaluation", in Apostolakis, Garribba, Volta (eds.), *Synthesis and Analysis Methods for Safety and Reliability Studies*, Plenum Press, 1980, pp 45-58.

[31] J.N.P.Gray, "Continuous-Time Markov Methods in the Solution of Practical Reliability Problems", *Reliability Engineering*, vol. 11, 1985, pp 233-252.

[32] C.E. Wells, J.L. Bryant, "Reliability Characteristics of a Markov System with a Mission of Random Duration", *IEEE Trans. Reliability*, vol. R-34, no. 4, Oct 1985, pp393-396.

[33] Mansoor Alam, Ubaid M. Al-Saggaf, "Quantitative Reliability Evaluation of Repairable Phased Mission Systems Using Markov Approach", *IEEE Trans. Reliability*, vol. R-35, 1986 Dec, pp 498-503.

[34] K. Kim, K.S. Park, "Phased-Mission System Reliability under Markov Environment", *IEEE Trans. Reliability*, vol. 43, no. 2, June 1994, pp 301-308.

[35] A.K. Somani, J. A. Ritcey, S.H.L. Au, "Computationally Efficient Phased-Mission Reliability Analysis for Systems with Variable Configurations", *IEEE Trans. Reliability*, vol. 41, No. 4, Dec 1992, pp 504-511.

[36] I. Mura, A. Bondavalli, "Hierarchical Modeling & Evaluation of Phased-Mission Systems", *IEEE Trans. Reliability*, vol. 48, no. 4, Dec 1999, pp 360-368.

[37] I. Mura, A. Bondavalli, X. Zang, K.S. Trivedi, "Dependability Modeling and Evaluation of Phased Mission Systems: a DSPN Approach", in *IEEE Computer Society Press*, 1999, pp 299-318.

[38] M.K. Smotherman, K. Zemoudeh, "A Non-Homogeneous Markov Model for Phased-Mission Reliability Analysis", *IEEE Trans. Reliability*, vol. 38, Dec 1989, pp 585-590.

[39] M.K. Smotherman, Robert M. Geist, "Phased Effectiveness using a Nonhomogeneous Markov Reward Model", *Reliability Engineering and System Safety*, vol. 27, 1990, pp 241-255.

[40] G. Becker, L. Camarinopoulos, G, Zioutas, "An Inhomogeneous state graph model and application for a phased mission and tolerable downtime problem", *Reliability Engineering and System Safety*, vol. 49, Jan 1995, pp 51-57.

[41] R. La Band, J.D.Andrews, "Phased Mission Modelling using Fault Tree Analysis", *Proceedings of the I MECH E Part E Journal of Process Mechanical Engineering*, vol. 218, no. 2, June 2004, pp 83-91.

[42] K. Reay, J.D.Andrews, "A Fault Tree Analysis Strategy using Binary Decision Diagrams", *Reliability Engineering and System Safety*, vol. 78, 2002, pp 45-56.

Appendix A Unconditional Phase Failure Intensity Example

Phase 1

The phase 1 prime implicant sets are: $\varepsilon_1 = \{A_1\}$

$\varepsilon_2 = \{B_1\}$

The phase 1 failure intensity can be expressed in equation (A.1),

$$w_1\, dt = w_1^{(1)}\, dt - w_1^{(2)} dt \qquad \text{(A.1)}$$

The first term on the right hand side of equation (A.1) represents the contribution from the occurrence of at least one prime implicant set in phase 1, and can be expressed in equation (A.2).

$$\begin{aligned} w_1^{\,1} &= P(\varepsilon_1) + P(\varepsilon_2) - P(\varepsilon_1 \cap \varepsilon_2) \\ &= P(\varepsilon_1) + P(\varepsilon_2) \quad \text{since there are no common events} \end{aligned} \qquad \text{(A.2)}$$

Each term of equation (A.2) may be obtained as follows to give $w_1^{\,1}$ in equation (A.3).

$$P(\varepsilon_1) = P(\text{Prime implicant set } \varepsilon_1 \text{ occurs during phase 1}) \text{ x } \lambda_{MISS}$$

$$P(\varepsilon_1) = \lambda_{MISS} \int_0^{t_1} f_A(t)dt = \lambda_{MISS}(1 - e^{-\lambda_A t_1})$$

$$P(\varepsilon_2) = P(\text{Prime implicant set } \varepsilon_2 \text{ occurs during phase 1}) \text{ x } \lambda_{MISS}$$

$$P(\varepsilon_2) = \lambda_{MISS} \int_0^{t_1} f_B(t)dt = \lambda_{MISS}(1 - e^{-\lambda_B t_1})$$

$$w_1^{\,1} = \lambda_{MISS}(1 - e^{-\lambda_A t_1} + 1 - e^{-\lambda_B t_1}) = \lambda_{MISS}(2 - e^{-\lambda_A t_1} - e^{-\lambda_B t_1}) \qquad \text{(A.3)}$$

The second term of equation (A.1) represents the contribution of prime implicant sets occurring while other prime implicant sets already exist in phase 1 (i.e. the system has already failed). This can be expressed in equation (A.4).

$$w_1^{\,2} = P(\varepsilon_1, \overline{A}) + P(\varepsilon_2, \overline{A}) - P(\varepsilon_1, \varepsilon_2, \overline{A}) \qquad \text{(A.4)}$$

The first term of equation (A.4) represents the probability that prime implicant set ε_1 occurs in phase 1 while any other prime implicant sets already exists. This is expanded in equation (A.5).

$$\begin{aligned}
&P(\varepsilon_1,\overline{A}) = P(\varepsilon_1,\overline{u_1}) + P(\varepsilon_1,\overline{u_2}) - P(\varepsilon_1,\overline{u_1},\overline{u_2}) \\
&P(\varepsilon_1,\overline{A}) = P(\varepsilon_1,\overline{u_2}) \qquad \text{since a prime implicant cannot exist and occur} \qquad \text{(A.5)}
\end{aligned}$$

The probability that prime implicant set ε_1 occurs while prime implicant set ε_2 already exists is the probability that component A fails in phase 1 when component B is already failed. This can be represented diagrammatically in Figure A.1.

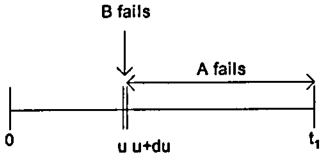


Figure A.1 Component B Fails Followed by Component A in Phase 1

The situation demonstrated in Figure A.1 can be represented algebraically and is derived in equation (A.6).

$$\begin{aligned}
P(\varepsilon_1,\overline{u_2}) &= \lambda_{MISS} \int_0^{t_1} f_B(u)\left(\int_u^{t_1} f_A(t)dt\right) du \\
&= \lambda_{MISS} \int_0^{t_1} f_B(u)\left(\left[-e^{-\lambda_A t}\right]_u^{t_1}\right) du \\
&= \lambda_{MISS} \int_0^{t_1} f_B(u)\left(-e^{-\lambda_A t_1} + e^{-\lambda_A u}\right) du \\
&= \lambda_{MISS} \int_0^{t_1} \lambda_B e^{-\lambda_B u}\left(-e^{-\lambda_A t_1} + e^{-\lambda_A u}\right) du \\
&= \lambda_{MISS} \int_0^{t_1} -\lambda_B e^{-\lambda_A t_1 - \lambda_B u} + \lambda_B e^{-(\lambda_A+\lambda_B)u} du \\
&= \lambda_{MISS} \left[e^{-\lambda_A t_1 - \lambda_B u} - \frac{\lambda_B}{\lambda_A+\lambda_B} e^{-(\lambda_A+\lambda_B)u} \right]_0^{t_1} \\
&= \lambda_{MISS} \left(e^{-(\lambda_A+\lambda_B)t_1} - \frac{\lambda_B}{\lambda_A+\lambda_B} e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B} \right) \\
&= \lambda_{MISS} \left(e^{-(\lambda_A+\lambda_B)t_1}\left(1 - \frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B} \right) \qquad \text{(A.6)}
\end{aligned}$$

Similarly, the second term of equation (A.4) may be expanded as,

$$P(\varepsilon_2,\overline{A}) = P(\varepsilon_2,\overline{u_1}) + P(\varepsilon_2,\overline{u_2}) - P(\varepsilon_2,\overline{u_1},\overline{u_2}) = P(\varepsilon_2,\overline{u_1})$$

This is the probability that prime implicant set ε_1 exists when prime implicant set ε_2 occurs, and is calculated in equation (A.7).

$$\begin{aligned} P(\varepsilon_1,\overline{u_2}) &= \lambda_{MISS}\int_0^{t_1} f_A(u)\left(\int_u^{t_1} f_B(t)\,dt\right)du \\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_1}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_1} + \frac{\lambda_A}{\lambda_A+\lambda_B}\right) \qquad \text{(A.7)} \end{aligned}$$

The third term of equation (A.4) becomes zero since the prime implicant sets contain no common events and so cannot both occur at the same instant of time,

$$P(\varepsilon_1,\varepsilon_2,\overline{A}) = P(\varepsilon_1,\varepsilon_2,\overline{u_1}) + P(\varepsilon_1,\varepsilon_2,\overline{u_2}) - P(\varepsilon_1,\varepsilon_2,\overline{u_1},\overline{u_2}) = 0$$

The second term of equation (A.1) is then obtained as the sum of equations (A.6) and (A.7) in equation (A.8).

$$\begin{aligned} w_1^{\,2} &= P(\varepsilon_1,\overline{A}) + P(\varepsilon_2,\overline{A}) - P(\varepsilon_1,\varepsilon_2,\overline{A}) \\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_1}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B} + e^{-(\lambda_A+\lambda_B)t_1}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_1} + \frac{\lambda_A}{\lambda_A+\lambda_B}\right) \\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_1}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}+1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_1} - e^{-\lambda_B t_1} + \frac{\lambda_A}{\lambda_A+\lambda_B} + \frac{\lambda_B}{\lambda_A+\lambda_B}\right) \\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_1} - e^{-\lambda_B t_1} + 1\right) \qquad \text{(A.8)} \end{aligned}$$

The phase 1 unconditional failure intensity is calculated using equations (A.3) and (A.8) in equation (A.9).

$$\begin{aligned} w_1 &= w_1^{\,1} - w_1^{\,2} \\ w_1 &= \lambda_{MISS}(2 - e^{-\lambda_A t_1} - e^{-\lambda_B t_1} - e^{-(\lambda_A+\lambda_B)t_1} + e^{-\lambda_A t_1} + e^{-\lambda_B t_1} - 1) \\ w_1 &= \lambda_{MISS}(1 - e^{-(\lambda_A+\lambda_B)t_1}) \qquad \text{(A.9)} \end{aligned}$$

Phase 2

The prime implicant sets for phase 2 are:

$$\varepsilon_1 = \{A_2B_2\}$$

$$\varepsilon_2 = \{A_2\overline{B_1}C_1\}.$$

$$\varepsilon_3 = \{A_2\overline{B_1}C_2\}.$$

Using equation (4.23), the unconditional failure intensity of phase 1 can be found by equation (A.10).

$$w_2 = w_2^{\ 1} - w_2^{\ 2} \tag{A.10}$$

The first term on the right hand side of equation (A.10) represents the contribution from the occurrence of at least one prime implicant set in phase 2, and can be expressed as,

$$w_2^{\ 1} = P(\varepsilon_1) + P(\varepsilon_2) + P(\varepsilon_3) - P(\varepsilon_1 \cap \varepsilon_2) - P(\varepsilon_1 \cap \varepsilon_3) - P(\varepsilon_2 \cap \varepsilon_3) + P(\varepsilon_1 \cap \varepsilon_2 \cap \varepsilon_3)$$

It is not possible for prime implicant sets ε_2 and ε_3 to both occur since component C cannot fail in both phases 1 and 2. The occurrence of at least one prime implicant set becomes as given in equation (A.11).

$$w_2^{\ 1} = P(\varepsilon_1) + P(\varepsilon_2) + P(\varepsilon_3) - P(\varepsilon_1 \cap \varepsilon_2) - P(\varepsilon_1 \cap \varepsilon_3) \tag{A.11}$$

The first term on the right hand side of equation (A.4) represents the probability of occurrence of minimal cut set ε_1. For ε_1 to occur, components A and B must both fail in phase 2 in any order. The two possible failure orderings are represented diagrammatically in Figure A.2.

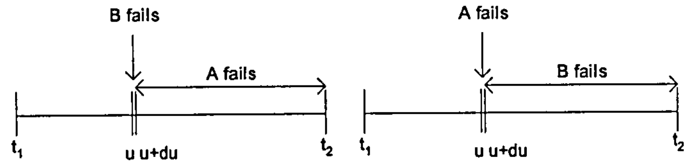


Figure A.2 Failure Orderings for Occurrence of Prime Implicant Set ε_1

The probability of occurrence of minimal cut set ε_1 is expressed as the sum of the probabilities of either A failing followed by B in phase 2, or B failing followed by A in phase 2. This is derived and given in equation (A.12).

$$P(\varepsilon_1) = \lambda_{MISS}\left\{\int_{t_1}^{t_2} f_B(u)\left(\int_u^{t_2} f_A(t)dt\right)du + \int_{t_1}^{t_2} f_A(u)\left(\int_u^{t_2} f_B(t)dt\right)du\right\}$$

$$\text{where} \quad \int_u^{t_2} f_A(t)dt = \left[-e^{-\lambda_A t}\right]_u^{t_2} = e^{-\lambda_A u} - e^{-\lambda_A t_2}$$

$$\int_u^{t_2} f_B(t)dt = \left[-e^{-\lambda_B t}\right]_u^{t_2} = e^{-\lambda_B u} - e^{-\lambda_B t_2}$$

$$\begin{aligned}
P(\varepsilon_1) &= \lambda_{MISS}\left\{\int_{t_1}^{t_2} \lambda_B e^{-\lambda_B u}(e^{-\lambda_A u} - e^{-\lambda_A t_2})du + \int_{t_1}^{t_2} \lambda_A e^{-\lambda_A u}(e^{-\lambda_B u} - e^{-\lambda_B t_2})du\right\} \\
&= \lambda_{MISS}\int_{t_1}^{t_2} \lambda_B e^{-(\lambda_B+\lambda_A)u} - \lambda_B e^{-\lambda_A t_2 - \lambda_B u} + \lambda_A e^{-(\lambda_B+\lambda_A)u} - \lambda_A e^{-\lambda_B t_2 - \lambda_A u}du \\
&= \lambda_{MISS}\left[-\frac{\lambda_B}{(\lambda_A+\lambda_B)}e^{-(\lambda_B+\lambda_A)u} + e^{-\lambda_A t_2 - \lambda_B u} - \frac{\lambda_A}{(\lambda_A+\lambda_B)}e^{-(\lambda_B+\lambda_A)u} + e^{-\lambda_B t_2 - \lambda_A u}\right]_{t_1}^{t_2} \\
&\doteq \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_2}\left(1 - \frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_2 - \lambda_B t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right. \\
&\qquad \left. + e^{-(\lambda_A+\lambda_B)t_2}\left(1 - \frac{\lambda_A}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_2 - \lambda_A t_1} + \frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right) \\
&= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_2} + e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-\lambda_B t_2 - \lambda_A t_1}\right) \qquad \text{(A.12)}
\end{aligned}$$

The probability of occurrence of prime implicant set ε_2 is the probability that component B works through phase 1, component C fails in phase 1, and then component A fails during phase 2. This is derived algebraically and is given in equation (A.13).

$$\begin{aligned}
P(\varepsilon_2) &= \lambda_{MISS}\left\{q_{C_1}(1 - q_{B_1})\int_{t_1}^{t_2} f_A(t)dt\right\} \\
&= \lambda_{MISS}\left\{(1 - e^{-\lambda_C t_1})e^{-\lambda_B t_1}\int_{t_1}^{t_2} f_A(t)dt\right\} \\
&= \lambda_{MISS}\left\{(1 - e^{-\lambda_C t_1})e^{-\lambda_B t_1}(e^{-\lambda_A t_1} - e^{-\lambda_A t_2})\right\} \\
&= \lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2 - \lambda_B t_1} - e^{-(\lambda_A+\lambda_B+\lambda_C)t_1} + e^{-(\lambda_B+\lambda_C)t_1 - \lambda_A t_2}\right\} \qquad \text{(A.13)}
\end{aligned}$$

ε_3 will occur if component B works through phase 1, and components A and C both fail in phase 2 in any order. Since only dynamic failure relationships are considered in phase 2, the probability that component B works through phase 1 is treated separately. The probability of occurrence of prime implicant set ε_3 is expressed in equation (A.14).

$$P(\varepsilon_3) = \lambda_{MISS}(1-q_{B_1})\left\{\int_{t_1}^{t_2} f_C(u)\left(\int_u^{t_2} f_A(t)dt\right)du + \int_{t_1}^{t_2} f_A(u)\left(\int_u^{t_2} f_C(t)dt\right)du\right\} \qquad \text{(A.14)}$$

Using the derivation method presented in equation (A.12), the probability of occurrence of prime implicant set ε_3 is derived and expressed in equation (A.15).

$$\begin{aligned} P(\varepsilon_3) &= \lambda_{MISS} e^{-\lambda_B t_1}\left(e^{-(\lambda_A+\lambda_C)t_2} + e^{-(\lambda_A+\lambda_C)t_1} - e^{-\lambda_A t_2-\lambda_C t_1} - e^{-\lambda_C t_2-\lambda_A t_1}\right) \\ P(\varepsilon_3) &= \lambda_{MISS}\left(e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2} + e^{-(\lambda_A+\lambda_B+\lambda_C)t_1} - e^{-\lambda_A t_2-(\lambda_B+\lambda_C)t_1} - e^{-\lambda_C t_2-(\lambda_A+\lambda_B)t_1}\right) \end{aligned} \qquad \text{(A.15)}$$

Minimal cut set ε_1 and prime implicant set ε_2 can both occur at the same instant of time if C fails in phase 1, B fails in phase 2, and A fails after B in phase 2. Component A must be the last to fail since the failure of A in phase 2 is the only common event between the two sets. If the event of component C failure in phase 1 is treated separately, the probability of occurrence of ε_1 AND ε_2 can be expressed in equation (A.16).

$$P(\varepsilon_1 \cap \varepsilon_2) = \lambda_{MISS}(1-e^{-\lambda_C t_1})\left\{\int_{t_1}^{t_2} f_B(u)\left(\int_u^{t_2} f_A(t)\,dt\right)du\right\} \qquad \text{(A.16)}$$

The probability that component B fails followed by component A in phase 2 can be derived using equation (A.12), and the probability of occurrence of ε_1 AND ε_2 is calculated in equation (A.17).

$$\begin{aligned} P(\varepsilon_1 \cap \varepsilon_2) &= \lambda_{MISS}(1-e^{-\lambda_C t_1})\left(e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_2-\lambda_B t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right) \\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_A t_2-\lambda_B t_1} + \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right. \\ &\quad \left. - e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) + e^{-(\lambda_C+\lambda_B)t_1-\lambda_A t_2} - \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\right) \end{aligned} \qquad \text{(A.17)}$$

Minimal cut set ε_1 and prime implicant set ε_3 can both occur at the same instant of time if C and B fail in phase 2, and A fails last in phase 2. Component A must be the last to fail in phase 2 since component A failure in phase 2 is the only common event between the sets. There are two possible failure orderings, $C_2 \rightarrow B_2 \rightarrow A_2$ or $B_2 \rightarrow C_2 \rightarrow A_2$, given in Figure A.3.

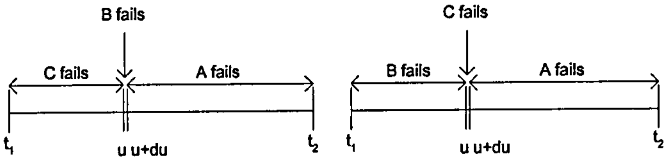


Figure A.3 Failure Orderings for Occurrence of Prime Implicant Sets ε_1 and ε_3

The probability of occurrence of ε_1 AND ε_3 can be derived and is given in equation (A.18).

$$P(\varepsilon_1 \cap \varepsilon_3) = \lambda_{MISS}\left\{\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_C(t')dt'\right) f_B(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du + \int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_B(t')dt'\right) f_C(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du\right\}$$

where $\int_{t_1}^{u} f_C(t')dt' = \int_{t_1}^{u} \lambda_C e^{-\lambda_C t'}dt' = e^{-\lambda_C t_1} - e^{-\lambda_C u}$

$$\int_{u}^{t_2} f_A(t)dt = \int_{u}^{t_2} \lambda_A e^{-\lambda_A t}dt = e^{-\lambda_A u} - e^{-\lambda_A t_2}$$

$$\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_C(t')dt'\right) f_B(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du$$

$$= \int_{t_1}^{t_2}\left(e^{-\lambda_C t_1} - e^{-\lambda_C u}\right)\lambda_B e^{-\lambda_B u}\left(e^{-\lambda_A u} - e^{-\lambda_A t_2}\right)du$$

$$= \int_{t_1}^{t_2}\left(\lambda_B e^{-\lambda_C t_1 - (\lambda_A + \lambda_B)u} - \lambda_B e^{-(\lambda_A + \lambda_B + \lambda_C)u} - \lambda_B e^{-\lambda_C t_1 - \lambda_A t_2 - \lambda_B u} + \lambda_B e^{-\lambda_A t_2 - (\lambda_B + \lambda_C)u}\right)du$$

$$= \left[-\frac{\lambda_B}{\lambda_A + \lambda_B} e^{-\lambda_C t_1 - (\lambda_A + \lambda_B)u} + \frac{\lambda_B}{\lambda_A + \lambda_B + \lambda_C} e^{-(\lambda_A + \lambda_B + \lambda_C)u} + e^{-\lambda_C t_1 - \lambda_A t_2 - \lambda_B u} - \frac{\lambda_B}{\lambda_B + \lambda_C} e^{-\lambda_A t_2 - (\lambda_B + \lambda_C)u}\right]_{t_1}^{t_2}$$

$$= -\frac{\lambda_B}{\lambda_A + \lambda_B} e^{-\lambda_C t_1 - (\lambda_A + \lambda_B)t_2} + \frac{\lambda_B}{\lambda_A + \lambda_B + \lambda_C} e^{-(\lambda_A + \lambda_B + \lambda_C)t_2} + e^{-\lambda_C t_1 - (\lambda_A + \lambda_B)t_2} - \frac{\lambda_B}{\lambda_B + \lambda_C} e^{-(\lambda_A + \lambda_B + \lambda_C)t_2}$$

$$+ \frac{\lambda_B}{\lambda_A + \lambda_B} e^{-(\lambda_A + \lambda_B + \lambda_C)t_1} - \frac{\lambda_B}{\lambda_A + \lambda_B + \lambda_C} e^{-(\lambda_A + \lambda_B + \lambda_C)t_1} - e^{-(\lambda_B + \lambda_C)t_1 - \lambda_A t_2} + \frac{\lambda_B}{\lambda_B + \lambda_C} e^{-(\lambda_B + \lambda_C)t_1 - \lambda_A t_2}$$

$$= e^{-(\lambda_A + \lambda_B + \lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_A + \lambda_B} - \frac{\lambda_B}{\lambda_A + \lambda_B + \lambda_C}\right) + e^{-(\lambda_A + \lambda_B + \lambda_C)t_2}\left(\frac{\lambda_B}{\lambda_A + \lambda_B + \lambda_C} - \frac{\lambda_B}{\lambda_B + \lambda_C}\right)$$
$$+ e^{-(\lambda_B + \lambda_C)t_1 - \lambda_A t_2}\left(\frac{\lambda_B}{\lambda_B + \lambda_C} - 1\right) + e^{-\lambda_C t_1 - (\lambda_A + \lambda_B)t_2}\left(1 - \frac{\lambda_B}{\lambda_A + \lambda_B}\right)$$

Similarly, $\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_B(t')dt'\right) f_C(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du$

$$= e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_C}{\lambda_A+\lambda_C}-\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-\frac{\lambda_C}{\lambda_B+\lambda_C}\right)$$

$$+e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2}\left(\frac{\lambda_C}{\lambda_B+\lambda_C}-1\right)+e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_A+\lambda_C}\right)$$

Therefore,

$$P(\varepsilon_1 \cap \varepsilon_3) = \lambda_{MISS}\left\{\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_C(t')dt'\right) f_B(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du + \int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_B(t')dt'\right) f_C(u)\left(\int_{u}^{t_2} f_A(t)dt\right)du\right\}$$

$$= \lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_A+\lambda_B}-\frac{\lambda_B}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B}{\lambda_A+\lambda_B+\lambda_C}-\frac{\lambda_B}{\lambda_B+\lambda_C}\right)\right.$$

$$+e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2}\left(\frac{\lambda_B}{\lambda_B+\lambda_C}-1\right)+e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right)$$

$$+e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_C}{\lambda_A+\lambda_C}-\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-\frac{\lambda_C}{\lambda_B+\lambda_C}\right)$$

$$\left.+e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2}\left(\frac{\lambda_C}{\lambda_B+\lambda_C}-1\right)+e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_A+\lambda_C}\right)\right\}$$

$$= \lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_A+\lambda_B}+\frac{\lambda_C}{\lambda_A+\lambda_C}-\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-1\right)\right.$$

$$\left.-e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2}+e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right)+e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_A+\lambda_C}\right)\right\} \qquad \text{(A.18)}$$

The contribution from the occurrence of at least one prime implicant set in phase 2 can be expressed using equations (A.12), (A.13), (A.15), (A.17) and (A.18) and is given in equation (A.19).

$$w_2{}^1 = P(\varepsilon_1) + P(\varepsilon_2) + P(\varepsilon_3) - P(\varepsilon_1 \cap \varepsilon_2) - P(\varepsilon_1 \cap \varepsilon_3)$$

$$= \lambda_{MISS}\Big\{e^{-(\lambda_A+\lambda_B)t_2} + e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2-\lambda_B t_1} - e^{-\lambda_B t_2-\lambda_A t_1} + e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2-\lambda_B t_1} - e^{-(\lambda_A+\lambda_B+\lambda_C)t_1} + e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2}$$

$$+ e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2} + e^{-(\lambda_A+\lambda_B+\lambda_C)t_1} - e^{-\lambda_A t_2-(\lambda_B+\lambda_C)t_1} - e^{-\lambda_C t_2-(\lambda_A+\lambda_B)t_1} - e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right)$$

$$+ e^{-\lambda_A t_2-\lambda_B t_1} - \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1} + e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-(\lambda_C+\lambda_B)t_1-\lambda_A t_2} + \frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}$$

$$- e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_A+\lambda_B} + \frac{\lambda_C}{\lambda_A+\lambda_C} - \frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right) - e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C} - 1\right)$$

$$+ e^{-(\lambda_B+\lambda_C)t_1-\lambda_A t_2} - e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_A+\lambda_C}\right)\Big\}$$

$$= \lambda_{MISS}\Big\{\frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_2} + e^{-(\lambda_A+\lambda_B)t_1}\left(2-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_2-\lambda_A t_1} - e^{-\lambda_A t_2-\lambda_B t_1} - e^{-\lambda_C t_2-(\lambda_A+\lambda_B)t_1}$$

$$+ \frac{\lambda_C}{\lambda_A+\lambda_C}e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2} - e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C} - 1\right) - e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_C}{\lambda_A+\lambda_C} - \frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)\Big\} \tag{A.19}$$

The second term of equation (A.10) represents the contribution of prime implicant sets occurring while other prime implicant sets already exist in phase 2 (i.e. the system has already failed). This can be expressed in equation (A.20).

$$w_2{}^2 = P(\varepsilon_1, \overline{A}) + P(\varepsilon_2, \overline{A}) + P(\varepsilon_3, \overline{A}) - P(\varepsilon_1, \varepsilon_2, \overline{A}) - P(\varepsilon_1, \varepsilon_3, \overline{A}) - P(\varepsilon_2, \varepsilon_3, \overline{A}) + P(\varepsilon_1, \varepsilon_2, \varepsilon_3, \overline{A}) \tag{A.20}$$

Each term of equation (A.20) can be further expanded. The first term on the right hand side of equation (A.20) is the probability that minimal cut set ε_1 occurs while any other minimal cut sets or prime implicant sets exist. This is expanded as,

$$P(\varepsilon_1, \overline{A}) = P(\varepsilon_1, \overline{u_1}) + P(\varepsilon_1, \overline{u_2}) + P(\varepsilon_1, \overline{u_3}) - P(\varepsilon_1, \overline{u_1}, \overline{u_2}) - P(\varepsilon_1, \overline{u_1}, \overline{u_3}) - P(\varepsilon_1, \overline{u_2}, \overline{u_3}) + P(\varepsilon_1, \overline{u_1}, \overline{u_2}, \overline{u_3})$$

Since it is not possible for a minimal cut set to both occur and exist, and also prime implicant sets ε_2 and ε_3 cannot both exist together, many of the terms are eliminated.

The probability that minimal cut set ε_1 occurs while any other prime implicant set exists becomes as given in equation (A.21).

$$P(\varepsilon_1,\overline{A}) = P(\varepsilon_1,\overline{u_2}) + P(\varepsilon_1,\overline{u_3}) \tag{A.21}$$

The probability that prime implicant set ε_2 exists requires C to fail in phase 1, B to work through phase 1, and finally A to fail in phase 2. Since A is already failed in phase 2, for minimal cut set ε_1 to occur, B must then fail in phase 2. The probability that minimal cut set ε_1 occurs while prime implicant set ε_2 exists is the probability that C fails in phase 1, A fails in phase 2, and B fails last in phase 2. This is represented algebraically in equation (A.22).

$$P(\varepsilon_1,\overline{u_2}) = \lambda_{MISS}(1-e^{-\lambda_C t_1})\left\{\int_{t_1}^{t_2} f_A(u)\left(\int_u^{t_2} f_B(t)dt\right)du\right\} \tag{A.22}$$

Using the derivation in equation (A.12), equation (A.22) can be calculated and is given in equation (A.23).

$$\begin{aligned}P(\varepsilon_1,\overline{u_2}) &= \lambda_{MISS}(1-e^{-\lambda_C t_1})\left(e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)-e^{-\lambda_B t_2-\lambda_A t_1}+\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right)\\ &= \lambda_{MISS}\left(e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)-e^{-\lambda_B t_2-\lambda_A t_1}+\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right.\\ &\qquad \left.-e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)+e^{-(\lambda_C+\lambda_A)t_1-\lambda_B t_2}-\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\right)\end{aligned} \tag{A.23}$$

The probability that minimal cut set ε_1 occurs while prime implicant set ε_3 exists is the probability that C fails in phase 2, A fails in phase 2, and B fails last in phase 2. Components A and C can fail in any order, but component B must fail last for minimal cut set ε_1 to occur. This is represented in equation (A.24).

$$P(\varepsilon_1,\overline{u_3}) = \lambda_{MISS}\left\{\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_C(t')dt'\right)f_A(u)\left(\int_u^{t_2} f_B(t)dt\right)du+\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_A(t')dt'\right)f_C(u)\left(\int_u^{t_2} f_B(t)dt\right)du\right\} \tag{A.24}$$

Using the derivations in equation (A.18), this may be obtained in equation (A.25).

$$\begin{aligned}P(\varepsilon_1,\overline{u_3}) = \lambda_{MISS}\Bigg\{ & e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_B}-\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}-\frac{\lambda_A}{\lambda_A+\lambda_C}\right)\\ & +e^{-(\lambda_A+\lambda_C)t_1-\lambda_B t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_C}-1\right)+e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)\\ & +e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_C}{\lambda_B+\lambda_C}-\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-\frac{\lambda_C}{\lambda_A+\lambda_C}\right)\\ & +e^{-(\lambda_A+\lambda_C)t_1-\lambda_B t_2}\left(\frac{\lambda_C}{\lambda_A+\lambda_C}-1\right)+e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_B+\lambda_C}\right)\Bigg\}\end{aligned}$$

$$\begin{aligned}= \lambda_{MISS}\Bigg\{ & e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_B}+\frac{\lambda_C}{\lambda_B+\lambda_C}-\frac{\lambda_A+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-1\right)\\ & -e^{-(\lambda_A+\lambda_C)t_1-\lambda_B t_2}+e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)+e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_B+\lambda_C}\right)\Bigg\}\end{aligned}$$

(A.25)

Prime implicant set ε_2 can not occur while any other minimal cut sets or prime implicant sets exist. The existence of any other prime implicant sets would require component A to be failed in phase 2. Since the last component of ε_2 to fail is component A in phase 2, it is not possible for ε_2 to be the last prime implicant set to occur,

$$P(\varepsilon_2,\overline{A}) = P(\varepsilon_2,\overline{u_1})+P(\varepsilon_2,\overline{u_2})+P(\varepsilon_2,\overline{u_3})-P(\varepsilon_2,\overline{u_1},\overline{u_2})-P(\varepsilon_2,\overline{u_1},\overline{u_3})-P(\varepsilon_2,\overline{u_2},\overline{u_3})+P(\varepsilon_2,\overline{u_1},\overline{u_2},\overline{u_3})$$

$P(\varepsilon_2,\overline{A})=0$ since prime implicant set ε_2 cant be the last to occur

The probability that prime implicant set ε_3 occurs while any other minimal cut sets or prime implicant sets exist is expanded as,

$$P(\varepsilon_3,\overline{A}) = P(\varepsilon_3,\overline{u_1})+P(\varepsilon_3,\overline{u_2})+P(\varepsilon_3,\overline{u_3})-P(\varepsilon_3,\overline{u_1},\overline{u_2})-P(\varepsilon_3,\overline{u_1},\overline{u_3})-P(\varepsilon_3,\overline{u_2},\overline{u_3})+P(\varepsilon_3,\overline{u_1},\overline{u_2},\overline{u_3})$$

Since it is not possible for a prime implicant set to both occur and exist, and prime implicant set ε_3 cannot occur if ε_2 already exists since component C is already failed in phase 1, many of the terms are eliminated. The probability that prime implicant set ε_3 occurs while any other prime implicant set exists becomes as given in equation (A.26).

$$P(\varepsilon_3, \overline{A}) = P(\varepsilon_3, \overline{u_1}) \tag{A.26}$$

The probability that minimal cut set ε_1 exists requires A and B to both fail in phase 2. Since A is already failed in phase 2 and component B must have worked through phase 1, for prime implicant set ε_3 to occur, C must fail last in phase 2. The probability that prime implicant set ε_3 occurs while minimal cut set ε_1 exists is the probability that A and B fail in phase 2 in any order, and C fails last in phase 2. This is represented algebraically in equation (A.27).

$$P(\varepsilon_3, \overline{u_1}) = \lambda_{MISS}\left\{\int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_A(t')dt'\right) f_B(u)\left(\int_{u}^{t_2} f_C(t)dt\right)du + \int_{t_1}^{t_2}\left(\int_{t_1}^{u} f_B(t')dt'\right) f_A(u)\left(\int_{u}^{t_2} f_C(t)dt\right)du\right\} \tag{A.27}$$

Using the derivations in equation (A.18), this may be obtained in equation (A.28).

$$\begin{aligned}
P(\varepsilon_3, \overline{u_1}) = \lambda_{MISS}\Bigg\{ & e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_B+\lambda_C} - \frac{\lambda_B}{\lambda_A+\lambda_B+\lambda_C}\right) + e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B}{\lambda_A+\lambda_B+\lambda_C} - \frac{\lambda_B}{\lambda_A+\lambda_B}\right) \\
& + e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2}\left(\frac{\lambda_B}{\lambda_A+\lambda_B} - 1\right) + e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1 - \frac{\lambda_B}{\lambda_B+\lambda_C}\right) \\
& + e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_C} - \frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}\right) + e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C} - \frac{\lambda_A}{\lambda_A+\lambda_B}\right) \\
& + e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_B} - 1\right) + e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1 - \frac{\lambda_A}{\lambda_A+\lambda_C}\right)\Bigg\}
\end{aligned}$$

$$\begin{aligned}
= \lambda_{MISS}\Bigg\{ & e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_B+\lambda_C} + \frac{\lambda_A}{\lambda_A+\lambda_C} - \frac{\lambda_A+\lambda_B}{\lambda_A+\lambda_B+\lambda_C}\right) + e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A+\lambda_B}{\lambda_A+\lambda_B+\lambda_C} - 1\right) \\
& - e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2} + e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1 - \frac{\lambda_B}{\lambda_B+\lambda_C}\right) + e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1 - \frac{\lambda_A}{\lambda_A+\lambda_C}\right)\Bigg\}
\end{aligned} \tag{A.28}$$

It is not possible for minimal cut set ε_1 and prime implicant set ε_2 to both occur while any other minimal cut sets or prime implicant sets exist and so,

$$\begin{aligned}
P(\varepsilon_1, \varepsilon_2, \overline{A}) = {} & P(\varepsilon_1, \varepsilon_2, \overline{u_1}) + P(\varepsilon_1, \varepsilon_2, \overline{u_2}) + P(\varepsilon_1, \varepsilon_2, \overline{u_3}) \\
& - P(\varepsilon_1, \varepsilon_2, \overline{u_1}, \overline{u_2}) - P(\varepsilon_1, \varepsilon_2, \overline{u_1}, \overline{u_3}) - P(\varepsilon_1, \varepsilon_2, \overline{u_2}, \overline{u_3}) + P(\varepsilon_1, \varepsilon_2, \overline{u_1}, \overline{u_2}, \overline{u_3}) = 0
\end{aligned}$$

Similarly, it is not possible for minimal cut set ε_1 and prime implicant set ε_3 to both occur while any other minimal cut sets or prime implicant sets exist,

$$P(\varepsilon_1,\varepsilon_3,\overline{A})=P(\varepsilon_1,\varepsilon_3,\overline{u_1})+P(\varepsilon_1,\varepsilon_3,\overline{u_2})+P(\varepsilon_1,\varepsilon_3,\overline{u_3})-P(\varepsilon_1,\varepsilon_3,\overline{u_1},\overline{u_2})-P(\varepsilon_1,\varepsilon_3,\overline{u_1},\overline{u_3})-P(\varepsilon_1,\varepsilon_3,\overline{u_2},\overline{u_3})+P(\varepsilon_1,\varepsilon_3,\overline{u_1},\overline{u_2},\overline{u_3})=0$$

Also, it is not possible for prime implicant sets ε_2 and ε_3 to both occur at the same time and so,

$$P(\varepsilon_2,\varepsilon_3,\overline{A})=P(\varepsilon_2,\varepsilon_3,\overline{u_1})+P(\varepsilon_2,\varepsilon_3,\overline{u_2})+P(\varepsilon_2,\varepsilon_3,\overline{u_3})-P(\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_2})-P(\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_3})-P(\varepsilon_2,\varepsilon_3,\overline{u_2},\overline{u_3})+P(\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_2},\overline{u_3})=0$$

$$\begin{aligned}P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{A})&=P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_1})+P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_2})+P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_3})\\&\quad-P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_2})-P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_3})-P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_2},\overline{u_3})+P(\varepsilon_1,\varepsilon_2,\varepsilon_3,\overline{u_1},\overline{u_2},\overline{u_3})=0\end{aligned}$$

The contribution of prime implicant sets occurring while other prime implicant sets already exist in phase 2 can be expressed using equations (A.23), (A.25), and (A.28), and is given in equation (A.29).

$$\begin{aligned}w_2{}^2&=P(\varepsilon_1,\overline{u_2})+P(\varepsilon_1,\overline{u_3})+P(\varepsilon_3,\overline{u_1})\\
&=\lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)-e^{-\lambda_B t_2-\lambda_A t_1}+\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}\right.\\
&\quad-e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)+e^{-(\lambda_C+\lambda_A)t_1-\lambda_B t_2}-\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\\
&\quad+e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_B}+\frac{\lambda_C}{\lambda_B+\lambda_C}-\frac{\lambda_A+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-1\right)\\
&\quad-e^{-(\lambda_A+\lambda_C)t_1-\lambda_B t_2}+e^{-\lambda_C t_1-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)+e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1-\frac{\lambda_C}{\lambda_B+\lambda_C}\right)\\
&\quad+e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_B}{\lambda_B+\lambda_C}+\frac{\lambda_A}{\lambda_A+\lambda_C}-\frac{\lambda_A+\lambda_B}{\lambda_A+\lambda_B+\lambda_C}\right)+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A+\lambda_B}{\lambda_A+\lambda_B+\lambda_C}-1\right)\\
&\quad\left.-e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2}+e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\left(1-\frac{\lambda_B}{\lambda_B+\lambda_C}\right)+e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_C}\right)\right\}\end{aligned}$$

$$\begin{aligned}&=\lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right)-e^{-\lambda_B t_2-\lambda_A t_1}+\frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1}+e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_C}-\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}\right)\right.\\
&\quad\left.+e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}-1\right)+e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}-e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2}+e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_C}\right)\right\}\end{aligned}$$

(A.29)

The unconditional failure intensity of phase 2 as defined in equation (A.10) can be obtained using equations (A.19) and (A.29) and is given in equation (A.30).

$$w_2 = w_2{}^1 - w_2{}^2$$

$$w_2 = \lambda_{MISS}\left\{\frac{\lambda_B}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_2} + e^{-(\lambda_A+\lambda_B)t_1}\left(2-\frac{\lambda_B}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_2-\lambda_A t_1} - e^{-\lambda_A t_2-\lambda_B t_1} - e^{-\lambda_C t_2-(\lambda_A+\lambda_B)t_1}\right.$$

$$\left. + \frac{\lambda_C}{\lambda_A+\lambda_C}e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2} - e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}-1\right) - e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_C}{\lambda_A+\lambda_C}-\frac{\lambda_B+\lambda_C}{\lambda_A+\lambda_B+\lambda_C}\right)\right\}$$

$$-\lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_B}\right) - e^{-\lambda_B t_2-\lambda_A t_1} + \frac{\lambda_A}{\lambda_A+\lambda_B}e^{-(\lambda_A+\lambda_B)t_1} + e^{-(\lambda_A+\lambda_B+\lambda_C)t_1}\left(\frac{\lambda_A}{\lambda_A+\lambda_C}-\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}\right)\right.$$

$$\left. + e^{-(\lambda_A+\lambda_B+\lambda_C)t_2}\left(\frac{\lambda_A}{\lambda_A+\lambda_B+\lambda_C}-1\right) + e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2} - e^{-(\lambda_A+\lambda_B)t_1-\lambda_C t_2} + e^{-\lambda_B t_1-(\lambda_A+\lambda_C)t_2}\left(1-\frac{\lambda_A}{\lambda_A+\lambda_C}\right)\right\}$$

$$w_2 = \lambda_{MISS}\left\{e^{-(\lambda_A+\lambda_B)t_1} - e^{-\lambda_A t_2-\lambda_B t_1} + e^{-(\lambda_A+\lambda_B+\lambda_C)t_2} - e^{-\lambda_A t_1-(\lambda_B+\lambda_C)t_2}\right\} \quad (A.30)$$

Appendix B Criticality Function Example

B.1 Critical States

In tabular form, the arbitrary components X, Y, and Z are assigned for each component as given in Table B.1.

	X	Y	Z
Component B	A	C	D
Component C	A	B	D
Component D	A	B	C

Table B.1 Component Representation

The critical states for components B, C, and D are shown for phase 1, 2, and 3 in Tables B.2, B.3, and B.4 respectively

Other Component States	Probability	Critical State		
		B	C	D
$(.,\overline{X_1},\overline{Y_1},\overline{Z_1})$	$(1-q_{X_1})(1-q_{Y_1})(1-q_{Z_1})$	Yes	Yes	No
$(.,\overline{X_1},\overline{Y_1},Z_1)$	$(1-q_{X_1})(1-q_{Y_1})q_{Z_1}$	Yes	Yes	No
$(.,\overline{X_1},Y_1,\overline{Z_1})$	$(1-q_{X_1})q_{Y_1}(1-q_{Z_1})$	No	No	No
$(.,\overline{X_1},Y_1,Z_1)$	$(1-q_{X_1})q_{Y_1}q_{Z_1}$	No	No	No
$(.,X_1,\overline{Y_1},\overline{Z_1})$	$q_{X_1}(1-q_{Y_1})(1-q_{Z_1})$	No	No	No
$(.,X_1,\overline{Y_1},Z_1)$	$q_{X_1}(1-q_{Y_1})q_{Z_1}$	No	No	No
$(.,X_1,Y_1,\overline{Z_1})$	$q_{X_1}q_{Y_1}(1-q_{Z_1})$	No	No	No
$(.,X_1,Y_1,Z_1)$	$q_{X_1}q_{Y_1}q_{Z_1}$	No	No	No

Table B.2 Critical States in Phase 1

Other Component States	Probability	Phase 1 Fail	Critical for B	Phase 1 Fail	Critical for C	Phase 1 Fail	Critical for D
$(.,\overline{X_{12}},\overline{Y_{12}},\overline{Z_{12}})$	$(1-q_{X_{12}})(1-q_{Y_{12}})(1-q_{Z_{12}})$	No	No	No	No	No	No
$(.,X_1,\overline{Y_{12}},\overline{Z_{12}})$	$q_{X_1}(1-q_{Y_{12}})(1-q_{Z_{12}})$	Yes	-	Yes	-	Yes	-
$(.,X_2,\overline{Y_{12}},\overline{Z_{12}})$	$q_{X_2}(1-q_{Y_{12}})(1-q_{Z_{12}})$	No	No	No	No	No	Yes
$(.,\overline{X_{12}},Y_1,\overline{Z_{12}})$	$(1-q_{X_{12}})q_{Y_1}(1-q_{Z_{12}})$	Yes	-	Yes	-	Yes	-
$(.,\overline{X_{12}},Y_2,\overline{Z_{12}})$	$(1-q_{X_{12}})q_{Y_2}(1-q_{Z_{12}})$	No	No	No	No	No	Yes
$(.,\overline{X_{12}},\overline{Y_{12}},Z_1)$	$(1-q_{X_{12}})(1-q_{Y_{12}})q_{Z_1}$	No	Yes	No	No	Yes	-
$(.,\overline{X_{12}},\overline{Y_{12}},Z_2)$	$(1-q_{X_{12}})(1-q_{Y_{12}})q_{Z_2}$	No	Yes	No	No	No	No
$(.,X_1,Y_1,\overline{Z_{12}})$	$q_{X_1}q_{Y_1}(1-q_{Z_{12}})$	Yes	-	Yes	-	Yes	-
$(.,X_1,Y_2,\overline{Z_{12}})$	$q_{X_1}q_{Y_2}(1-q_{Z_{12}})$	Yes	-	Yes	-	Yes	-
$(.,X_2,Y_1,\overline{Z_{12}})$	$q_{X_2}q_{Y_1}(1-q_{Z_{12}})$	Yes	-	Yes	-	Yes	-
$(.,X_2,Y_2,\overline{Z_{12}})$	$q_{X_2}q_{Y_2}(1-q_{Z_{12}})$	No	No	No	No	No	Yes
$(.,X_1,\overline{Y_{12}},Z_1)$	$q_{X_1}(1-q_{Y_{12}})q_{Z_1}$	Yes	-	Yes	-	Yes	-
$(.,X_1,\overline{Y_{12}},Z_2)$	$q_{X_1}(1-q_{Y_{12}})q_{Z_2}$	Yes	-	Yes	-	Yes	-
$(.,X_2,\overline{Y_{12}},Z_1)$	$q_{X_2}(1-q_{Y_{12}})q_{Z_1}$	No	No	No	No	Yes	-
$(.,X_2,\overline{Y_{12}},Z_2)$	$q_{X_2}(1-q_{Y_{12}})q_{Z_2}$	No	No	No	No	No	Yes
$(.,\overline{X_{12}},Y_1,Z_1)$	$(1-q_{X_{12}})q_{Y_1}q_{Z_1}$	Yes	-	Yes	-	Yes	-
$(.,\overline{X_{12}},Y_1,Z_2)$	$(1-q_{X_{12}})q_{Y_1}q_{Z_2}$	Yes	-	Yes	-	Yes	-
$(.,\overline{X_{12}},Y_2,Z_1)$	$(1-q_{X_{12}})q_{Y_2}q_{Z_1}$	No	Yes	No	No	Yes	-
$(.,\overline{X_{12}},Y_2,Z_2)$	$(1-q_{X_{12}})q_{Y_2}q_{Z_2}$	No	Yes	No	No	No	Yes
$(.,X_1,Y_1,Z_1)$	$q_{X_1}q_{Y_1}q_{Z_1}$	Yes	-	Yes	-	Yes	-
$(.,X_1,Y_1,Z_2)$	$q_{X_1}q_{Y_1}q_{Z_2}$	Yes	-	Yes	-	Yes	-
$(.,X_1,Y_2,Z_1)$	$q_{X_1}q_{Y_2}q_{Z_1}$	Yes	-	Yes	-	Yes	-
$(.,X_1,Y_2,Z_2)$	$q_{X_1}q_{Y_2}q_{Z_2}$	Yes	-	Yes	-	Yes	-
$(.,X_2,Y_1,Z_1)$	$q_{X_2}q_{Y_1}q_{Z_1}$	Yes	-	Yes	-	Yes	-
$(.,X_2,Y_1,Z_2)$	$q_{X_2}q_{Y_1}q_{Z_2}$	Yes	-	Yes	-	Yes	-
$(.,X_2,Y_2,Z_1)$	$q_{X_2}q_{Y_2}q_{Z_1}$	No	No	No	No	Yes	-
$(.,X_2,Y_2,Z_2)$	$q_{X_2}q_{Y_2}q_{Z_2}$	No	No	No	No	No	Yes

Table B.3 Critical States in Phase 2

Other Component States	Probability	Phase 1 Fail	Phase 2 Fail	Critical for B	Phase 1 Fail	Phase 2 Fail	Critical for C	Phase 1 Fail	Phase 2 Fail	Critical for D
$(.,\overline{X_{123}},\overline{Y_{123}},\overline{Z_{123}})$	$(1-q_{X_{123}})(1-q_{Y_{123}})(1-q_{Z_{123}})$	No	No	No	No	No	No	No	No	No
$(.,X_1,\overline{Y_{123}},\overline{Z_{123}})$	$q_{X_1}(1-q_{Y_{123}})(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,\overline{Y_{123}},\overline{Z_{123}})$	$q_{X_2}(1-q_{Y_{123}})(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,\overline{Y_{123}},\overline{Z_{123}})$	$q_{X_3}(1-q_{Y_{123}})(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,\overline{X_{123}},Y_1,\overline{Z_{123}})$	$(1-q_{X_{123}})q_{Y_1}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,\overline{X_{123}},Y_2,\overline{Z_{123}})$	$(1-q_{X_{123}})q_{Y_2}(1-q_{Z_{123}})$	No	No	No	No	No	No	No	No	No
$(.,\overline{X_{123}},Y_3,\overline{Z_{123}})$	$(1-q_{X_{123}})q_{Y_3}(1-q_{Z_{123}})$	No	No	No	No	No	No	No	No	No
$(.,\overline{X_{123}},\overline{Y_{123}},Z_1)$	$(1-q_{X_{123}})(1-q_{Y_{123}})q_{Z_1}$	No	No	No	No	No	No	No	No	No
$(.,\overline{X_{123}},\overline{Y_{123}},Z_2)$	$(1-q_{X_{123}})(1-q_{Y_{123}})q_{Z_2}$	No	No	No	No	No	No	No	No	No
$(.,\overline{X_{123}},\overline{Y_{123}},Z_3)$	$(1-q_{X_{123}})(1-q_{Y_{123}})q_{Z_3}$	No	No	No	No	No	No	No	No	No
$(.,X_1,Y_1,\overline{Z_{123}})$	$q_{X_1}q_{Y_1}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_2,\overline{Z_{123}})$	$q_{X_1}q_{Y_2}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_3,\overline{Z_{123}})$	$q_{X_1}q_{Y_3}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_1,\overline{Z_{123}})$	$q_{X_2}q_{Y_1}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_2,\overline{Z_{123}})$	$q_{X_2}q_{Y_2}(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,X_2,Y_3,\overline{Z_{123}})$	$q_{X_2}q_{Y_3}(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,Y_1,\overline{Z_{123}})$	$q_{X_3}q_{Y_1}(1-q_{Z_{123}})$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_3,Y_2,\overline{Z_{123}})$	$q_{X_3}q_{Y_2}(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,Y_3,\overline{Z_{123}})$	$q_{X_3}q_{Y_3}(1-q_{Z_{123}})$	No	No	No	No	No	Yes	No	No	No
$(.,X_1,\overline{Y_{123}},Z_1)$	$q_{X_1}(1-q_{Y_{123}})q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,\overline{Y_{123}},Z_2)$	$q_{X_1}(1-q_{Y_{123}})q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,\overline{Y_{123}},Z_3)$	$q_{X_1}(1-q_{Y_{123}})q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,\overline{Y_{123}},Z_1)$	$q_{X_2}(1-q_{Y_{123}})q_{Z_1}$	No	Yes	-	No	Yes	-	Yes	-	-
$(.,X_2,\overline{Y_{123}},Z_2)$	$q_{X_2}(1-q_{Y_{123}})q_{Z_2}$	No	Yes	-	No	Yes	-	No	No	No
$(.,X_2,\overline{Y_{123}},Z_3)$	$q_{X_2}(1-q_{Y_{123}})q_{Z_3}$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,\overline{Y_{123}},Z_1)$	$q_{X_3}(1-q_{Y_{123}})q_{Z_1}$	No	No	No	No	No	Yes	Yes	-	-
$(.,X_3,\overline{Y_{123}},Z_2)$	$q_{X_3}(1-q_{Y_{123}})q_{Z_2}$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,\overline{Y_{123}},Z_3)$	$q_{X_3}(1-q_{Y_{123}})q_{Z_3}$	No	No	No	No	No	Yes	No	No	No
$(\overline{X_{123}},Y_1,Z_1,.)$	$(1-q_{X_{123}})q_{Y_1}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(\overline{X_{123}},Y_1,Z_2,.)$	$(1-q_{X_{123}})q_{Y_1}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(\overline{X_{123}},Y_1,Z_3,.)$	$(1-q_{X_{123}})q_{Y_1}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-

Other Component States	Probability	Phase 1 Fail	Phase 2 Fail	Critical for B	Phase 1 Fail	Phase 2 Fail	Critical for C	Phase 1 Fail	Phase 2 Fail	Critical for D
$(\overline{X_{123}},Y_2,Z_1,)$	$(1-q_{X_{123}})q_{Y_2}q_{Z_1}$	No	No	No	No	Yes	-	Yes	-	-
$(\overline{X_{123}},Y_2,Z_2,)$	$(1-q_{X_{123}})q_{Y_2}q_{Z_2}$	No	No	No	No	Yes	-	No	No	No
$(\overline{X_{123}},Y_2,Z_3,)$	$(1-q_{X_{123}})q_{Y_2}q_{Z_3}$	No	No	No	No	No	No	No	No	No
$(\overline{X_{123}},Y_3,Z_1,)$	$(1-q_{X_{123}})q_{Y_3}q_{Z_1}$	No	No	No	No	No	No	Yes	-	-
$(\overline{X_{123}},Y_3,Z_2,)$	$(1-q_{X_{123}})q_{Y_3}q_{Z_2}$	No	No	No	No	No	No	No	No	No
$(\overline{X_{123}},Y_3,Z_3,)$	$(1-q_{X_{123}})q_{Y_3}q_{Z_3}$	No	No	No	No	No	No	No	No	No
$(.,X_1,Y_1,Z_1)$	$q_{X_1}q_{Y_1}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_1,Z_2)$	$q_{X_1}q_{Y_1}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_1,Z_3)$	$q_{X_1}q_{Y_1}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_2,Z_1)$	$q_{X_1}q_{Y_2}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_2,Z_2)$	$q_{X_1}q_{Y_2}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_2,Z_3)$	$q_{X_1}q_{Y_2}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_3,Z_1)$	$q_{X_1}q_{Y_3}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_3,Z_2)$	$q_{X_1}q_{Y_3}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_1,Y_3,Z_3)$	$q_{X_1}q_{Y_3}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_1,Z_1)$	$q_{X_2}q_{Y_1}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_1,Z_2)$	$q_{X_2}q_{Y_1}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_1,Z_3)$	$q_{X_2}q_{Y_1}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_2,Y_2,Z_1)$	$q_{X_2}q_{Y_2}q_{Z_1}$	No	Yes	-	No	Yes	-	Yes	-	-
$(.,X_2,Y_2,Z_2)$	$q_{X_2}q_{Y_2}q_{Z_2}$	No	Yes	-	No	Yes	-	No	No	No
$(.,X_2,Y_2,Z_3)$	$q_{X_2}q_{Y_2}q_{Z_3}$	No	No	No	No	No	Yes	No	No	No
$(.,X_2,Y_3,Z_1)$	$q_{X_2}q_{Y_3}q_{Z_1}$	No	Yes	-	No	Yes	-	Yes	-	-
$(.,X_2,Y_3,Z_2)$	$q_{X_2}q_{Y_3}q_{Z_2}$	No	Yes	-	No	Yes	-	No	No	No
$(.,X_2,Y_3,Z_3)$	$q_{X_2}q_{Y_3}q_{Z_3}$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,Y_1,Z_1)$	$q_{X_3}q_{Y_1}q_{Z_1}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_3,Y_1,Z_2)$	$q_{X_3}q_{Y_1}q_{Z_2}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_3,Y_1,Z_3)$	$q_{X_3}q_{Y_1}q_{Z_3}$	Yes	-	-	Yes	-	-	Yes	-	-
$(.,X_3,Y_2,Z_1)$	$q_{X_3}q_{Y_2}q_{Z_1}$	No	No	No	No	Yes	-	Yes	-	-
$(.,X_3,Y_2,Z_2)$	$q_{X_3}q_{Y_2}q_{Z_2}$	No	No	No	No	Yes	-	No	No	No
$(.,X_3,Y_2,Z_3)$	$q_{X_3}q_{Y_2}q_{Z_3}$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,Y_3,Z_1)$	$q_{X_3}q_{Y_3}q_{Z_1}$	No	No	No	No	No	Yes	Yes	-	-
$(.,X_3,Y_3,Z_2)$	$q_{X_3}q_{Y_3}q_{Z_2}$	No	No	No	No	No	Yes	No	No	No
$(.,X_3,Y_3,Z_3)$	$q_{X_3}q_{Y_3}q_{Z_3}$	No	No	No	No	No	Yes	No	No	No

Table B.4 Critical States in Phase 3

B.2 Phase Criticality Function

The criticality function for components B, C, and D calculated by the sum of the probabilities of occurrence of the critical states and also by differentiation of the phase unavailability are given in Table B.5.

Sum of Probability of Occurrence	Partial Differential
<u>Component B</u> *Q(critical in phase 1)* $=(1-q_{A_1})(1-q_{C_1})(1-q_{D_1})+(1-q_{A_1})(1-q_{C_1})q_{D_1}$ $=(1-q_{A_1})(1-q_{C_1})$ *Q(no failure in phase1 & critical in phase 2)* $=(1-q_{A_{12}})(1-q_{C_{12}})q_{D_1}+(1-q_{A_{12}})(1-q_{C_{12}})q_{D_2}+(1-q_{A_{12}})q_{C_2}q_{D_1}+(1-q_{A_{12}})q_{C_2}q_{D_2}$ $=(1-q_{A_{12}})(1-q_{C_{12}})(q_{D_1}+q_{D_2})+(1-q_{A_{12}})q_{C_2}(q_{D_1}+q_{D_2})$ $=(1-q_{A_{12}})(1-q_{C_{12}})q_{D_{12}}+(1-q_{A_{12}})q_{C_2}q_{D_{12}}$ $=(1-q_{A_{12}})q_{D_{12}}(1-q_{C_{12}}+q_{C_2})$ $=(1-q_{A_{12}})q_{D_{12}}(1-q_{C_1}-q_{C_2}+q_{C_2})$ $=(1-q_{A_{12}})q_{D_{12}}(1-q_{C_1})$ $=(1-q_{A_{12}})q_{D_{12}}(1-q_{C_1})$ *Q(no failure in phases 1 and 2 & critical in phase 3)*=0	$\frac{\partial Q_1}{\partial q_{B_1}}=1-q_{A_1}-q_{C_1}+q_{A_1}q_{C_1}$ $=(1-q_{A_1})(1-q_{C_1})$ $\frac{\partial Q_2}{\partial q_{B_2}}=(1-q_{A_1})(1-q_{C_1})q_{D_{12}}-q_{A_2}(1-q_{C_1})q_{D_{12}}$ $=(1-q_{C_1})q_{D_{12}}(1-q_{A_1}-q_{A_2})$ $=(1-q_{C_1})q_{D_{12}}(1-q_{A_{12}})$ $\frac{\partial Q_3}{\partial q_{D_1}}=0$
<u>Component C</u> *Q(critical in phase 1)* $=(1-q_{A_1})(1-q_{B_1})(1-q_{D_1})+(1-q_{A_1})(1-q_{B_1})q_{D_1}$ $=(1-q_{A_1})(1-q_{B_1})$ *Q(no failure in phase1 & critical in phase 2)*=0	$\frac{\partial Q_1}{\partial q_{C_1}}=1-q_{A_1}-q_{B_1}+q_{A_1}q_{B_1}$ $=(1-q_{A_1})(1-q_{B_1})$ $\frac{\partial Q_2}{\partial q_{C_2}}=0$

Sum of Probability of Occurrence	Partial Differential
Q(no failure in phases 1 and 2 & critical in phase 3) $=q_{A_2}(1-q_{B_{123}})(1-q_{D_{123}})+q_{A_3}(1-q_{B_{123}})(1-q_{D_{123}})$ $+q_{A_2}q_{B_2}(1-q_{D_{123}})+q_{A_2}q_{B_3}(1-q_{D_{123}})+q_{A_3}q_{B_2}(1-q_{D_{123}})+q_{A_3}q_{B_3}(1-q_{D_{123}})$ $+q_{A_2}(1-q_{B_{123}})q_{D_3}+q_{A_3}(1-q_{B_{123}})q_{D_1}+q_{A_3}(1-q_{B_{123}})q_{D_2}+q_{A_3}(1-q_{B_{123}})q_{D_3}$ $+q_{A_2}q_{B_2}q_{D_3}+q_{A_2}q_{B_3}q_{D_3}+q_{A_3}q_{B_2}q_{D_3}+q_{A_3}q_{B_3}q_{D_1}+q_{A_3}q_{B_3}q_{D_2}+q_{A_3}q_{B_3}q_{D_3}$ $=(q_{A_2}+q_{A_3})(1-q_{B_{123}})(1-q_{D_{123}})$ $+(q_{A_2}q_{B_2}+q_{A_2}q_{B_3}+q_{A_3}q_{B_2}+q_{A_3}q_{B_3})(1-q_{D_{123}})$ $+q_{A_2}(1-q_{B_{123}})q_{D_3}+q_{A_3}(1-q_{B_{123}})(q_{D_1}+q_{D_2}+q_{D_3})$ $+q_{A_2}(q_{B_2}+q_{B_3})q_{D_3}+q_{A_3}q_{B_2}q_{D_3}+q_{A_3}q_{B_3}(q_{D_1}+q_{D_2}+q_{D_3})$ $=q_{A_{23}}(1-q_{B_{123}})(1-q_{D_{123}})+q_{A_{23}}q_{B_{23}}(1-q_{D_{123}})+q_{A_2}(1-q_{B_{123}})q_{D_3}+q_{A_3}(1-q_{B_{123}})q_{D_{123}}$ $+q_{A_2}q_{B_{23}}q_{D_3}+q_{A_3}q_{B_2}q_{D_3}+q_{A_3}q_{B_3}q_{D_{123}}$ $=q_{A_{23}}(1-q_{B_{123}}+q_{B_{23}})(1-q_{D_{123}})+q_{A_2}(1-q_{B_{123}}+q_{B_{23}})q_{D_3}+q_{A_3}(1-q_{B_{123}}+q_{B_3})q_{D_{123}}+q_{A_3}q_{B_2}q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}})+q_{A_2}(1-q_{B_1})q_{D_3}+q_{A_3}(1-q_{B_{12}})q_{D_{123}}+q_{A_3}q_{B_2}q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}})+q_{A_2}(1-q_{B_1})q_{D_3}+q_{A_3}(1-q_{B_{12}})q_{D_{12}}+q_{A_3}(1-q_{B_{12}}+q_{B_2})q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}})+q_{A_2}(1-q_{B_1})q_{D_3}+q_{A_3}(1-q_{B_{12}})q_{D_{12}}+q_{A_3}(1-q_{B_1})q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}})+(q_{A_2}+q_{A_3})(1-q_{B_1})q_{D_3}+q_{A_3}(1-q_{B_{12}})q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}})+q_{A_{23}}(1-q_{B_1})q_{D_3}+q_{A_3}(1-q_{B_{12}})q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{123}}+q_{D_3})+q_{A_3}(1-q_{B_{12}})q_{D_3}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{D_3}$	$\frac{\partial Q_3}{\partial q_{C_3}}=q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{D_{12}}$ $=q_{A_{23}}(1-q_{B_1})(1-q_{D_{12}})+q_{A_3}(1-q_{B_{12}})q_{D_{12}}$
Component D *Q(critical in phase 1)* =0 *Q(no failure in phase1 & critical in phase 2)* $=q_{A_2}(1-q_{B_{12}})(1-q_{C_{12}})+(1-q_{A_{12}})q_{B_2}(1-q_{C_{12}})+q_{A_2}q_{B_2}(1-q_{C_{12}})+q_{A_2}(1-q_{B_{12}})q_{C_2}+(1-q_{A_{12}})q_{B_2}q_{C_2}+q_{A_2}q_{B_2}q_{C_2}$ $=q_{A_2}(1-q_{B_1}-q_{B_2}+q_{B_2})(1-q_{C_{12}})+(1-q_{A_{12}})q_{B_2}(1-q_{C_1}-q_{C_2}+q_{C_2})+q_{A_2}(1-q_{B_1}-q_{B_2}+q_{B_2})q_{C_2}$ $=q_{A_2}(1-q_{B_1})(1-q_{C_{12}})+(1-q_{A_{12}})q_{B_2}(1-q_{C_1})+q_{A_2}(1-q_{B_1})q_{C_2}$ $=q_{A_2}(1-q_{B_1})(1-q_{C_1}-q_{C_2}+q_{C_2})+(1-q_{A_{12}})q_{B_2}(1-q_{C_1})$ $=q_{A_2}(1-q_{B_1})(1-q_{C_1})+(1-q_{A_{12}})q_{B_2}(1-q_{C_1})$ *Q(no failure in phases 1 and 2 & critical in phase 3)*=0	$\frac{\partial Q_2}{\partial q_{D_1}}=0$ $\frac{\partial Q_2}{\partial q_{D_2}}=q_{A_2}(1-q_{B_{12}})(1-q_{C_1})+(1-q_{A_1})q_{B_2}(1-q_{C_1})$ $=q_{A_2}(1-q_{B_1})(1-q_{C_1})-q_{A_2}q_{B_2}(1-q_{C_1})+(1-q_{A_1})q_{B_2}(1-q_{C_1})$ $=q_{A_2}(1-q_{B_1})(1-q_{C_1})+(1-q_{A_{12}})q_{B_2}(1-q_{C_1})$ $\frac{\partial Q_2}{\partial q_{D_3}}=0$

Table B.5 Criticality Function for Components B, C, and D