CHAPTER-III

CONCEPT OF COMMON CAUSE FAILURES AND RELATED MODELS

3.1 INTRODUCTION

This chapter unfolds the concept of common cause failures which are identified to be one of the most dominant causes of failure in many real line applications. In the first two chapters discussed in this thesis contain the quantitative, combinatorial, network modelling and Markov models. In most of these methods and techniques the basic assumption is that the failure of the components is independent of the failure of the other. Further, it is assumed that there could be only one component (event) failure due to any cause in an infinitesimally small duration of time. And it would mean that the probability of failure of two or more orders of magnitude happening is almost zero.

Thus most of the techniques and methods that are
considered in the literature of reliability would belong to this category. However, in practice, it was found that the probability of failure of one, two or more orders of magnitude is predicted. The more obvious examples come from Nuclear Industry. For instance, a single fire accident in a nuclear reactor plant would cause the failure of both the cooling water systems viz., normal cooling water system and emergency cooling water system because both of them are housed in the same pumping room. Yet another example is that the crash of a light air-craft would cause in failure of a two-circuit transmission lines because both of them are mounted on the same tower.

Thus one must say that the reliability analyst has failed to recognise the dominant causes of system failures which appear in many real oriented applications. This would understand that, in reliability analysis, more optimistic prediction is considered rather than what exactly is there in

Therefore, one of the most important modes of failure which severely degrades the actual operating reliability of the system is identified and known as 'common-cause failures', which find a place in reliability literature most recently [16,61,62,63]. This is also sometimes referred as 'common-mode failures'.

3.2 WHAT IS COMMON-CAUSE FAILURE?

In many real applications, common-cause failures are identified to be one of the most dominant cause of failure of components of the systems. This type of failures cause the simultaneous failure of two or more components owing to a single external common-cause. Considerable attention was given to this type of failures in the recent years in order to properly define them and to devise the methods to study their effect on the systems. Some of the organizations and reliability analysts who contributed
in this work include US Atomic Energy Commission (USAEC)[62], Task Force on IEEE APM Sub-Committee [61], russell and Burdick [31], Epler [27], Wagner [64], Edward and Watson [26], Gangloff [33], Billinton and Allan [16], Atwood [7-10], etc.

The common-cause failures as defined by Task Force of the IEEE APM Sub-Committee is the cause that must be a single external event which produces multiple effects. Essentially this means that more than one component fails. The definition would mean that common-cause is purely external one which produces more than one component failure in the system instead of the internal system event causing the failure of one or more other components in the system. Of course, the latter type of event would refer to dependent failures, which can be tackled using conditional probability approach.

The components of a system always need not necessarily fail independently of each other. The
failures may be synchronized for instance, by an extreme environment. Thus the common-cause failures will greatly reduce the reliability of the system and one is interested in the quantification of common-cause failure rates.

To emphasise on the concept of common-cause failures we discuss some more physical examples which would convince the more practicability of such type of failures. The concept of common-cause failures are mostly identified with more intensity in Nuclear Power Industry, Atwood [7-10], Epler [27], Fussell [31].

However, the common-cause failures are not restricted to nuclear industry alone. A few years ago, there was a widely publicized event that an improper installation of 'O-Rings' has resulted in failure of all four engines of a commercial airliner over the Atlantic Ocean. Yet another example is that during one of the space-shuttle flight, two-
computers that are installed in it were repeatedly and simultaneously inoperative due to jarring in the space shuttle while in operation. There are number of other contexts in which such type of causes were observed which attract less public attention.

These examples would obviously suggest the justification of common-cause failure models. The common-cause shocks would further be classified into two categories depending on the intensity of the shock.

1) Non-lethal common-cause shock failures (NCS)

2) Lethal common-cause shock failures (LCS)

Non-lethal common-cause shock is one, the occurrence of which would produce a random number of components to simultaneously outage, which follow a probability law viz., Binomial distribution. On the
other hand, a lethal common-cause failure is one, occurrence of which result in simultaneous outage of all components in the system. Therefore, a lethal shock is more powerful than non-lethal shocks.

3.3 COMMON-CAUSE FAILURES - REVIEW OF LITERATURE

In what follows from Section (3.1), the occurrence of common-cause failures, the practicability of such type of failures in many real situations, the nature of the common-cause failures will however justify the need and awareness of such type of failures, while considering the mathematical formulation to study the system performance measures on the more realistic conditions. Thus one is inclined to study the effect of common-cause shock failures on the systems.

Thus in this direction a significant work has come from Vesely [63] who applied the MVED (Multivariate Exponential Distribution) to estimate the
common-cause failure probabilities. The model suggested is a particular case of Marshall and Olkins [48] multivariate exponential distribution. This approach is also known as Marshall-Olkin specialization method.

Vesely model considers the 'common-cause shock failures' (Non-lethal common-cause shock failures) in addition to individual and independent failures. This we refer as 'Basic model' in this thesis. The details of this model and other aspects of this were separately discussed in Section (3.4) of this chapter.

Apart from Vesely's Basic BFR (BINOMIAL FAILURE RATE) model certain other common-cause models were also attempted by Flemming [29,30], Kelley et al [41]. Vesely's BFR model was applied to various sets of data by Atwood and Steverson [60], Meachum and Atwood [49]. In all the above applications an important additional information was often found. To account for this additional information in the data
Atwood [10] had considered the extension of the BFR Model by accounting the lethal common-cause shocks as provided by the data.

The details of this model were discussed in the Section (3.5) of this chapter. Billinton and Allan [16] have briefly discussed some of the basic models and evaluation techniques which are based on Markov approach in the context of common-cause failures. The models however take into consideration three types of failures repair processes. The effect of common-cause failures is discussed and it is established that even the small percentage of common-cause/mode failures increase very significantly the probability of the system being in down-state. This substantiates the need for common-cause failures to be inducted in the reliability analysis.

Chae and Clark [23] presented a method for calculating the reliability of the system with identically distributed components in the presence of common-
cause failures. The model assumes that the components are subjected to failure by Poisson failure processes that govern simultaneous failure of a specific subset of components. The model also compares the reliability with common-cause failures with that of individual failures and it establishes the effect of common-cause shock failures on the reliability when compared to 'individual failures'.

Billinton and Kumar [21] have developed a general purpose graphical approach to study the steady-state availability and frequency expression from a flow graph based on Markov approach. A set of examples that commonly encountered in practice are presented as a part of their study. The study also includes common-cause failures for non-identical components. The formulae are presented in each case.

Billinton et al [19], considered a study of application of common-cause outage models in composite system reliability evaluation. Billinton et al [20],
considered a study of spare component management in reliability and availability measures of the system.

In common-cause shock models that were presented by Vesely [63], Steverson and Atwood [60], Meachum and Atwood [49], mainly the objective is to estimate the rate of common-cause failures. The models are concentrated only to show how the quantities of interest in the model (discussed in Sections 3.4 and 3.5) of this chapter), in the presence of common-cause failures be estimated. This highlights on the statistical and computational parts of the methods.

3.4 BASIC COMMON-CAUSE MODEL - SOME DETAILS

Vesely's original BFR model is referred in this thesis as Basic common-cause model, which is a particular case of Marshall and Olkin's [48] MVED model. Some details of the model is presented here.
Assumptions of the Vesely's Model

1. The system consists of finite (say m) number of components.

2. The components all are identical and each of the component fail independently at random times.

3. The components have the same failure rate and such failures will be termed as 'individual failures'.

4. In addition to the individual failures, the system also encountered with common-cause (non-lethal common-cause) shocks, occurring with rate $\lambda$. For instance, the shocks here might be considered as human intervention such as overzealous torquing of several valves, extreme environment conditions such as unusual temperature or vibration, hardware failure outside the system such as pipe leak, etc.

5. The model also assumes that when the system is
affected by a non-lethal common-cause shock, each component is assumed to fail independently of the other with probability \( p \).

6. If a system is encountered with a common-cause shock the number of failed components is random, governing a Binomial law with parameters \((m, p)\). Thus the model is named as Binomial Failure Rate Model.

7. (a) The time between failures of any component in the absence of shocks, is exponentially distributed.

(b) Also time between shocks is exponentially distributed.

(c) Shocks and individual failures occur independent of each other.

(d) The failures are discovered and repaired immediately (with negligible time). In consequence, the number of individual failures in any time period is Poisson variable and so is the number of shocks.
Under the above assumptions the objective of the Vesely's model is to estimate the common-cause failure rates and probabilities in reliability and risk analysis.

3.5 EXTENSION OF BASIC BFR MODEL

Atwood and Steverson [60], Meachum and Atwood [49] have applied the basic BFR model to various sets of data. In what follows, the data exhibited an additional feature and a second kind of common-cause failures, were brought out. Thus Atwood [10] extended the basic Vesely's BFR model by including the lethal common-cause failures and discussed more details of BFR model. The practical examples of such types of shock failures are:

1) A closed suction valve, which is common to all three pumping systems in Nuclear Plant, will result in no flow through any of the pumps.
ii) An improper installation of 'O-Rings' in an airliner result in failure of all engines simultaneously.

The additional assumptions in the extended BFR common-cause failures are:

1. The system is affected by lethal common-cause shocks in addition to non-lethal common-cause shocks.

2. Lethal and non-lethal shocks are assumed to occur independently of each other and the time between lethal shocks is governed by exponential law with pdf

\[ f(t, \omega) = \omega \exp(-\omega t), \quad \omega > 0, \ t \geq 0 \]

\[ = 0 \quad \text{otherwise} \]

where \( \omega \) is the rate of lethal common-cause failures.

To use this model, the following information is
to be known exclusively.

(a) The number of components in the system.
(b) The total observation time of the system.
(c) The number of failures in the system.
(d) The number of failed components for any failure involving more than one component.
(e) Failure of several components was a coincidence or due to a non-lethal or due to a lethal shock.

The last point enlightens that, during a periodic inspection if failed components are found, it must be possible to decide whether they failed individually or whether the failures were synchronized by external factors. If all the components failed because of common-cause shock it is quite possible that we decide whether it is non-lethal shock resulted in all components fail or it is lethal shock that causes all components to fail by its very
Therefore, it is also possible to distinguish between potential common-cause shock and an individual failure. Some of the quantities in which one is interested in BFR model with lethal shock is shown in Table 3.1 (Atwood [10], Technometrics, 28, p.141).

<table>
<thead>
<tr>
<th>TABLE 3.1 Some Quantities of Interest in Atwood BFR Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantity</td>
</tr>
<tr>
<td>( \lambda )</td>
</tr>
<tr>
<td>( \beta )</td>
</tr>
<tr>
<td>( p = 1-q )</td>
</tr>
<tr>
<td>( \omega )</td>
</tr>
<tr>
<td>Quantity</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>$\lambda_+ = \beta(1 - q^m)$</td>
</tr>
<tr>
<td>$r_1 = \lambda + \omega$</td>
</tr>
<tr>
<td>$r_k = \beta p^k + \omega, \ k \geq 2$</td>
</tr>
<tr>
<td>$r_{1/m} = m\lambda + \lambda + \omega$</td>
</tr>
<tr>
<td>$r_{k/m} = \beta \sum_{i=k}^{m} m_{ci} p^i q^{m-i} + \omega \quad (\forall \ k \geq 2)$</td>
</tr>
</tbody>
</table>

Thus the basic parameters of the above model are $\lambda$, $\beta$, $\omega$, $p$. Atwood [10] considered the point and interval estimation methods. The model assumes that the individual and shock failures will be identified.
3.6 OVERVIEW OF THE PRESENT WORK

Having seen in many real applications, the practicability of the common-cause shock failures one must be aware of such type of failures in order to study the effect of them on the performance of the system. However, if we avoid the consideration of such type of failures for the analysis, it will give rise to approximate values of reliability characteristics which is always an over estimate of the situation. Thus on more practical grounds, one must look upon the analysis by accounting the common-cause shocks if any, in the model. Thus the models that are discussed with common-cause shocks will reflect the precision and accuracy in the real contexts.

However, the common-cause models so far discussed will emphasise only the estimation of failure rates and the probability connected in the common-cause failures. But, however, no discussion is made regarding the influence of common-cause failures
considering both lethal and non-lethal shock failures on the performance of the system, namely, reliability, availability (time dependent and steady-state), MTTF, coefficient of efficiency of renewal etc.

Therefore, in this thesis, the author discussed the methods and results of the above mentioned measures of effectiveness of the system, under the influence of common-cause shock failures, given that the information on failure rates is available. The formulae are developed, of the above mentioned measures of effectiveness of the system considering the 2-component system for both types viz., series and parallel configurations.

However, the methods and techniques with common-cause shock failures have a limitation on the data to be taken into consideration. The relevant data will virtually come from actual operating experience only rather than from controlled tests.

Under the present setup, firstly the author
developed formulae of reliability, availability (time dependent), steady-state availability \([4]\), MTTF when the common-cause failures are acting on the system with certain probability \([6]\). The effect of common-cause shock failures over the individual failures is discussed.

Secondly, the author also considered a Markov model with non-lethal common-cause failures in addition to individual failures and studied the impact of non-lethal shock failures when compared to individual failures.

Thirdly, in this thesis also considered the influence of lethal common-cause shock failures in addition to individual as well as non-lethal common-cause failures. The details of the formulae, examples supporting the results, illustrations and relevant numerical values are presented in the chapters IV and V.