Common-cause failure analysis

This item was submitted to Loughborough University’s Institutional Repository by the/an author.


Additional Information:

- This is a conference paper.

Metadata Record: [https://dspace.lboro.ac.uk/2134/3832](https://dspace.lboro.ac.uk/2134/3832)

Publisher: © T.R. Moss and J.D. Andrews

Please cite the published version.
This item was submitted to Loughborough's Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
http://creativecommons.org/licenses/by-nc-nd/2.5/
COMMON-CAUSE FAILURE ANALYSIS

T R Moss
Consultant
Abingdon

J D Andrews
Lecturer
Department of
Mathematical Sciences
Loughborough University
of Technology

Abstract

This paper describes a framework which can be used by reliability practitioners to incorporate common-cause failure events into reliability assessments. It describes the procedure by which early screening processes can be used to identify the most significant common-cause influences on the system performance. The paper then describes ways that the probability of occurrence of common-cause events can be quantified and through the use of a logic model (in this case fault tree analysis) the system performance can also be assessed.

1. INTRODUCTION

If a system consists of two identical components $A$ and $B$ in a parallel structure then the system will fail only if both components are in a failed state. The probability of this event, providing that the components fail independently of each other, is $p \times p = p^2$ where $p$ is the probability of an individual component failing.

This parallel system will be far more reliable than a system with a single component. However, if the components do not fail independently and can both fail under the same condition then the parallel system may only be slightly more reliable than each single component. A condition which can cause more than one component to fail is known as a common-cause.

A common-cause failure (CCF) has been defined [1] as the result of an event or events which, because of dependencies, cause a coincidence of failure states in two or more separate channels of a redundant system; leading to a defined system failing to perform its intended function. This paper describes a method employed by reliability practitioners to incorporate common-cause failure events into reliability assessments.
Strictly, a common-cause event is one whose occurrence causes the failure of more than one component with near certainty. An event which only increases the likelihood of components failing is a common influence event.

It is recognised that common-cause failures provide an important contribution to the failure of one or more elements of a redundant system. In fact they can dominate over random failures affecting only an individual item in the system. As such most comprehensive probabilistic risk or reliability assessments of potentially hazardous plant incorporate some way of dealing with this situation. There are two major difficulties in carrying out this type of assessment: (i) the number of potential common-cause events which can influence the functionality of one or more elements in a redundant system and (ii) the lack of available data to enable an accurate assessment of their likelihood of occurrence. A screening method is proposed to deal with the first of these problems. For the second difficulty the beta factor method can be employed. The method assumes that common-cause effects can be represented in the system reliability model as a proportion of the failure probability of a single channel of the multi-channel redundancy system. Where the channels have different levels of complexity the beta factor is applied to the predicted failure rate or failure probability of the highest reliability channel.

2 AREAS OF APPLICATION

The main area of application is in automatic protection system reliability studies where redundancy of protection channels will generally be incorporated into the design to reduce the probability of failure on demand. When quantifying the probability of failure it should be evident that a redundant sub-system will not always fail independently. A single common-cause may affect all channels at the same time.

3 COMMON-CAUSE ANALYSIS PROCEDURE

The analysis of the system performance taking account of potential common-cause events can be carried out by the following procedure:
Step 1: System Modelling

Step 2: Common-Cause Identification

Step 3: System Analysis

Each of these steps are now described in more detail.

System Modelling

This initial step in the process is very similar to that performed in modelling the reliability performance of a system whether or not common-cause events are to be considered. The stages carried out at this stage are:

1.1 Specification of the system failure modes of concern

1.2 System familiarisation

1.3 Development of the failure logic diagram

1.4 Component failure and repair data collection

The specification of the system failure modes of concern has generally been made prior to the analysis and is sometimes an obvious choice since the systems concerned perform some safety related tasks. Failure to act to provide protective or mitigating action usually being the event of concern.

System familiarisation has to be performed prior to constructing any form of logic model for the system behaviour. Each component in the system has to be identified, its potential failure modes considered and their effect on the system fully understood. As such, one mechanism for performing this task is to complete a failure mode and effects analysis (FMEA).

Failure logic models may take many forms, fault tree structures or networks (reliability block diagrams) being two of the most commonly used.
Data defining failure rates and repair rates or times for component failures which appear as basic events in the failure logic model are then collected. For dormant failures the test interval will also be required.

**Common-Cause Identification**

This second step identifies the characteristics that components have in common which would make them susceptible to a simultaneous failure. Components with the potential to fail due to a common-cause event are then grouped together. There may be many such groupings of components and if this is the case and it becomes impractical to analyze each common-cause event then an initial screening process must be carried out. The screening will identify the most significant common-cause events and these will then require a more detailed treatment. This second step therefore has the following stages.

2.1 Identify potential common cause events

2.1 For each common cause event indicate which component failure (basic events in the fault tree) are susceptible to this event.

2.3 Qualitatively screen out what are considered the least important common cause events.

2.4 Quantitatively screen out the least important common-cause events of those that remain.

The lower order failure combinations are generally the most significant contributors to the top event of a fault tree and it is these which it is required to eliminate to increase system reliability. However, if there is a common-mode failure influence on the system then higher order cut sets may also have comparable probabilities and contribute to the system failure in a significant way and cannot be neglected.

Potential common-mode failures can be caused by the following:

(a) components contain identical manufacturing faults
(b) components are maintained by the same maintenance engineer

(c) components are situated in the same location and are subject to the same environmental hazards such as impacts or vibration

(d) components are subject to the same operator.

Common-cause failures can generally be placed into one of the following three categories:

(1) Ageing

(2) Plant personnel

(3) System environment

A more detailed list of potential common-causes is given in Table 1.

The definition of common-cause failures by Edwards and Watson [1] aims to exclude situations which can be predicted from existing failure statistics such as loss of mains electricity supply. Common-cause failures generally fall within the areas shown in Figure 1, which Bourne et al [2], proposed for the classification of common-cause failures. These areas are also used by some analysts to estimate modifying factors which may be applied to the recommended mean value of beta.
<table>
<thead>
<tr>
<th>Source</th>
<th>Symbol</th>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>I</td>
<td>Impact</td>
<td>Pipe whip, water hammer, missiles, earthquake, structural failure.</td>
</tr>
<tr>
<td></td>
<td>V</td>
<td>Vibration</td>
<td>Machinery in motion, earthquake.</td>
</tr>
<tr>
<td></td>
<td>P</td>
<td>Pressure</td>
<td>Explosion, out-of-tolerance system changes (pump overspeed, flow blockage).</td>
</tr>
<tr>
<td></td>
<td>G</td>
<td>Grit</td>
<td>Airborne dust, metal fragments generated by moving parts with inadequate tolerances.</td>
</tr>
<tr>
<td></td>
<td>S</td>
<td>Stress</td>
<td>Thermal stress at welds of dissimilar metals, thermal stresses and bending moments caused by high conductivity and density.</td>
</tr>
<tr>
<td></td>
<td>T</td>
<td>Temperature</td>
<td>Fire, lightning, welding equipment, cooling system faults, electrical short circuits.</td>
</tr>
<tr>
<td></td>
<td>E</td>
<td>Loss of energy source</td>
<td>Common drive shaft, same power supply.</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>Calibration</td>
<td>Misprinted calibration instruction.</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>Manufacturer</td>
<td>Repeated fabrication error, such as neglect to properly coat relay contacts. Poor workmanship.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Damage during transportation.</td>
</tr>
<tr>
<td></td>
<td>IN</td>
<td>Installation</td>
<td>Same subcontractor or crew.</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>contractor</td>
<td>Incorrect procedure, inadequately trained personnel.</td>
</tr>
<tr>
<td></td>
<td>O</td>
<td>Maintenance</td>
<td>Operator disabled or overstressed, faulty operating procedures.</td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td>Operator or</td>
<td>Faculty test procedures which may affect all components normally tested together.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>operation Test</td>
<td>procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>procedure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>Ageing</td>
<td>Components of same materials</td>
</tr>
</tbody>
</table>

*Table 1. Categories and examples of common causes*
Figure 1. Classification of common-mode failures
Qualitative screening removes what are considered the least important common-cause events using the detailed knowledge of the plant and engineering judgement. This will involve some assessment of how susceptible groups of components are to the common-cause event and also the adequacy of any defence measures provided in the system design, operation or management to reduce the likelihood of simultaneous failure.

The quantified screening process, as suggested by Molesh [3], carries out a full analysis of the system building the common-cause events into the failure logic diagrams and assigning their occurrence probabilities by the beta factor method, described below, with beta set to a conservative value.

In assessing the results obtained in this step all common-cause events which may require a more detailed assessment are then identified and the third stage carried out.

**System Assessment**

For those common-cause events which remain following the screening process, more effort is expended in determining their likelihood of occurrence. This may be performed by producing a more refined value for the $\beta$ factor or by employing some other assessment method. Having revised the common-mode likelihood model the system logic model is reassessed.

**Common-Mode Cut Sets**

Once a fault tree has been constructed and the minimal cut sets obtained, then providing no common-mode failures exist in the system then these cut sets can be directly used in the reliability quantification process. If any of the possible common-mode causes are present for the system then a list of each common-cause should be made.

For each common-cause the groups of susceptible basic events are called **common-mode events**. If a basic event is unaffected by the common-cause then it is a **neutral event**. Where common-mode events exist in the minimal cut sets these can be replaced by a complex event representing the common-mode failure. The cut sets can now be re-minimised and by
providing a probability or frequency for the common-mode event the resulting cut sets can be analysed using conventional fault tree analysis programs.

For large fault trees, the list of minimal cut sets may be extremely large and it would be prohibitive for the common-mode events to be manipulated manually. Computer codes do, however, exist which will carry out the task of identifying common-cause events, replacing them in the cut sets with a single complex event and re-minimising the resulting cut set list ready for quantification.

Where common-causes provide an influence on a system it is not advisable that the qualitative analysis should be carried out using truncation or culling of the generated minimal cut sets based on cut set order. With a common-cause influence a cut set of order 4 may be more likely to occur than one with say only two events.

However in the example shown at the end of this paper the method used incorporates common-cause events into the fault tree structure. Thus removing the need for post-analysis manipulation of the minimal cut sets.

4 THE BETA FACTOR METHOD

The Beta Factor relates the CCF rate of redundant channels to the total failure rate of the highest reliability channel. If the total failure rate of the channel is \( \lambda \) and the independent and common-cause failure rates for that channel are \( \lambda_i \) and \( \lambda_{cc} \) then:

\[
\lambda = \lambda_i + \lambda_{cc}
\]

The \( \beta \) factor is defined as the ratio of the common cause failure rate to the total failure rate. Therefore

\[
\beta = \frac{\lambda_{cc}}{\lambda} \quad \text{or} \quad \lambda_{cc} = \beta \lambda
\]

(1)

and
\[ \lambda_t = \lambda - \lambda_{cc} = (1 - \beta)\lambda \]  

\textbf{Example}

A simple active-parallel redundant system is shown below

![Diagram of a simple active-parallel redundant system](image)

Considering only independent failures the reliability of the system \( R_s \) is given by:

\[ R_s = 1 - [(1 - R_i) \cdot (1 - R_i)] \]

where \( R_i \) = Probability of survival of a subsystem with Independent failures.

For a period of time \( t \)

\[ R_s(t) = [1 - [(1 - \exp[-\lambda_i t]) \cdot (1 - \exp[-\lambda_i t])] ] \]

\[ = 1 - (1 - 2\exp[-\lambda_i t] + \exp[-2\lambda_i t]) \]

\[ = 2\exp[-\lambda_i t] - \exp[-2\lambda_i t] \]  

(3)

With Common Cause failures included the system network is modified as follows:

![Diagram of a modified system with Common Cause](image)

The system reliability is then
\[ R'_i = R_s \cdot R_{cc} \]
\[ = (\text{probability of system survival with independent failures}) \times (\text{probability of survival with common cause failures}) \]

For a period of time \( t \)
\[ R'_i(t) = R_s(t) \cdot R_{cc}(t) \]
\[ = (2 \exp[-\lambda_i t] - \exp[-2\lambda_i t]) \cdot \exp[-\lambda_{cc} t] \]  \( (5) \)

substituting from equation 2 for \( \lambda_i \) and equation (1) for \( \lambda_{cc} \) gives
\[ R'_i(t) = (2 \exp[-(1-\beta)\lambda t] - \exp[-2(1-\beta)\lambda t]) \exp(-\beta \lambda t) \]
\[ = 2 \exp(-\lambda t) - \exp[-(2-\beta)\lambda t] \]

If \( \beta = 1 \) (ie ALL common-cause failures)
\[ R'_i(t) = 2 \exp(-\lambda t) - \exp[-(2-1)\lambda t] \]
\[ = 2 \exp(-\lambda t) - \exp(-\lambda t) \]
\[ = \exp(-\lambda t) \]
and, since \( \lambda = \lambda_{cc} \) in this case
\[ = \exp[-\lambda_{cc} t] \]  \( (6) \)

If \( \beta = 0 \) (ie NO common-cause failures)
\[ R'_i(t) = 2 \exp(-\lambda t) - \exp[-(2-0)\lambda t] \]  \( (7) \)
\[ = 2 \exp(-\lambda t) - \exp(-2\lambda t) \]
and, since \( \lambda = \lambda_i \) in this case
\[ = 2 \exp(-\lambda_i t) - \exp(-2\lambda_i t) \]

which is the same as equation 3.

Thus it can be seen that the \( \beta \) factor method gives consistent results in both cases. A base value of 0.2 for \( \beta \) has generally been assumed. The base value is then adjusted by modifying factors. It should be noted that modifying factors need to be based on engineering judgement since common-cause failures are relatively rare-events.
The analysis given above corresponds to the interpretation of Edwards and Watson [1], and is based on the original paper from the General Atomic Company in the USA [3].

Limiting values of failure probability are applied to account for the effect of common-cause failures particularly in reliability studies of protective instrumentation systems. The assumption is that, because of common-cause failures, the system reliability can never exceed an upper-limit determined by the configuration. The minimum failure probability levels proposed by Bourne [3] are:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Minimum Failure Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Instrument</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Redundant System</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Partially-Diverse System</td>
<td>$1 \times 10^{-4}$</td>
</tr>
<tr>
<td>Fully-Diverse System</td>
<td>$1 \times 10^{-5}$</td>
</tr>
<tr>
<td>Two Diverse Systems</td>
<td>$1 \times 10^{-6}$</td>
</tr>
</tbody>
</table>

These limiting values were employed by Martin and Wright [5] to modify the value of the recommended $\beta$ factor for different levels of redundancy and diversity.

Although alternative models for incorporating common-cause failure events into reliability analyses have been proposed they generally founder on the scarcity of common-cause failure data or because of problems in their application. The beta factor model scores because of its simplicity and its ability to cope with situations where failure rates and failure probabilities can both be involved.

5 FACTORS INFLUENCING BETA

The value of 0.2 for beta recommend by Edwards and Watson [1] was derived from a study of common-cause failures reported in a wide range of
industries from aircraft systems to large industrial plant. However, evidence from USA and UK studies show that the value of beta can vary significantly for different types of equipment. The beta values shown in Table 2 were derived from a comprehensive study of nuclear reactor operating experience in the USA [6]. Table 3, from a more limited study of UK experience at the nuclear chemical plant at Sellafield [7] show broad agreement with these figures. The indications are, therefore, that beta values can vary by at least a factor of 10.

Proposals for modifying the value of $\beta$ for specific situations have been made by a number of organisations. In this respect the most important factors which warrant consideration are redundancy and diversity, system complexity, the extent to which the design, operation and maintenance procedures provide defences against common-cause effects and the probability of the failure remaining unrevealed in normal operation.

Diversity

A partially-diverse system is defined as a system where the measured parameters (temperature, pressure, etc) are processed by channels employing different physical principles. Full diversity is when the measured parameters are also different and the diversity extends to full independence of power supplies, maintenance, etc. Increasingly the degree of diversity should reduce the probability of common-cause failure hence, the factor may be modified to reflect this.
<table>
<thead>
<tr>
<th>Component</th>
<th>Reactor Years</th>
<th>Number of Events Classified</th>
<th>Event Distribution</th>
<th>Estimated Beta Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Independent</td>
<td>Dependent</td>
</tr>
<tr>
<td>Reactor Trip Breakers</td>
<td>563</td>
<td>72</td>
<td>56</td>
<td>16</td>
</tr>
<tr>
<td>Diesel Generators</td>
<td>394</td>
<td>674</td>
<td>639</td>
<td>35</td>
</tr>
<tr>
<td>Motor-operated Valves</td>
<td>394</td>
<td>947</td>
<td>842</td>
<td>105</td>
</tr>
<tr>
<td>Safety/Relief Valves</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PWR</td>
<td>318</td>
<td>54</td>
<td>30</td>
<td>24</td>
</tr>
<tr>
<td>BWR</td>
<td>245</td>
<td>172</td>
<td>136</td>
<td>36</td>
</tr>
<tr>
<td>Pumps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Injection</td>
<td>394</td>
<td>112</td>
<td>77</td>
<td>35</td>
</tr>
<tr>
<td>RHR</td>
<td>394</td>
<td>117</td>
<td>67</td>
<td>50</td>
</tr>
<tr>
<td>Containment Spray</td>
<td>394</td>
<td>48</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>Auxiliary Feedwater</td>
<td>394</td>
<td>255</td>
<td>194</td>
<td>61</td>
</tr>
<tr>
<td>Service Water</td>
<td>394</td>
<td>203</td>
<td>159</td>
<td>44</td>
</tr>
<tr>
<td>Total</td>
<td>--</td>
<td>2,654</td>
<td>2,232</td>
<td>422</td>
</tr>
</tbody>
</table>

* Events classified include those having one or more actual or potential component failures or functionally unavailable states.
<table>
<thead>
<tr>
<th>SAMPLE NO.</th>
<th>DESCRIPTION</th>
<th>CCF/ TOTAL FAILURES</th>
<th>ESTIMATE $\beta$ FACTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Electrical distribution systems</td>
<td>$\frac{2}{23}$</td>
<td>$= 0.09$</td>
</tr>
<tr>
<td>2.</td>
<td>Ventilation fans (running failures)</td>
<td>$\frac{2}{166}$</td>
<td>$= 0.01$</td>
</tr>
<tr>
<td>3.</td>
<td>Ventilation fans (standby failures)</td>
<td>$\frac{2}{47}$</td>
<td>$= 0.04$</td>
</tr>
<tr>
<td>4.</td>
<td>Data loggers (processors)</td>
<td>$\frac{2}{66}$</td>
<td>$= 0.03$</td>
</tr>
<tr>
<td>5.</td>
<td>Data loggers (disk drives)</td>
<td>$\frac{2}{34}$</td>
<td>$= 0.06$</td>
</tr>
</tbody>
</table>

*Table 3. Estimates of beta factors from Sellafield data*

**System Complexity**

Much of the research into common-cause failures from which the recommended base value of $\beta$ was derived concentrated on complex control and protection systems. Less complex systems or individual components may not be prone to some of the potential causes of common-cause failures such as design and maintenance errors experienced by protective systems so lower values of $\beta$ may apply. On the other hand systems incorporating computers where software validation poses significant problems may attract higher $\beta$ factors.

**Defences Against CCF**

Edwards and Watson\(^1\) evaluated data from a number of different sources to estimate the proportion of common-cause failures attributable to the different areas shown in Figure 1. The results are shown in the last column of Table 4. From these data it can be seen that the defences against common-cause failure inherent in the design, and the maintenance and test procedures can have a significant impact on the probability of common-cause failure. If these defences are systematically evaluated during a
reliability assessment it may be appropriate to adopt a lower value for the $\beta$ factor.

Unrevealed Failures

Protective systems and equipment on standby duty will mainly experience unrevealed failures; that is, failures will only become evident when a demand or test is made on the system. When failure of one channel is revealed (for example, failure of the running pump in a pumping system) then action can frequently be taken to ensure that the system is quickly restored to its original operating state. Thus only simultaneous equipment failures will cause change of the operating state at system level and a lower value of $\beta$ may be adopted in the reliability assessment. Martin and Wright\(^5\) estimate that approximately one third of all failures would affect running systems simultaneously. The justification for this estimate can also be seen in Table 4.

6 MODIFICATION OF THE BETA FACTOR

In practice the most significant effect on common-cause failure frequency will be the degree of redundancy and diversity applied in the system design. Redundancy and diversity can, therefore, be expected to have the greatest effect on factors. The following modifying factors have been proposed\(^5\):

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Modifying Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant channel system</td>
<td>1.0</td>
</tr>
<tr>
<td>Partly-diverse system</td>
<td>0.1</td>
</tr>
<tr>
<td>Fully-diverse system</td>
<td>0.01</td>
</tr>
<tr>
<td>Two diverse systems</td>
<td>0.001</td>
</tr>
</tbody>
</table>
## CCF CAUSES

<table>
<thead>
<tr>
<th>Engineering (E)</th>
<th>Operations (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design (ED)</td>
<td>Procedural (OP)</td>
</tr>
<tr>
<td>Construction (EC)</td>
<td>Environmental (OE)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(EFD)</td>
<td>(EDR)</td>
<td>(ECM)</td>
<td>(ECI)</td>
<td>(OPM)</td>
<td>(OPO)</td>
<td>(OEN)</td>
<td>(OEE)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CCF Cause</th>
<th>Proportion of Failures on Dual Running Systems</th>
<th>Proportion of CCF failures in Each Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Simultaneous</td>
<td>Non-Simultaneous</td>
</tr>
<tr>
<td>EFD</td>
<td>1</td>
<td>0.026</td>
</tr>
<tr>
<td>EDR</td>
<td>0.5</td>
<td>0.145</td>
</tr>
<tr>
<td>ECM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ECI</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>OPM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>OPO</td>
<td>0.5</td>
<td>0.060</td>
</tr>
<tr>
<td>OEN</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>OEE</td>
<td>1</td>
<td>0.082</td>
</tr>
<tr>
<td>Total</td>
<td>3</td>
<td>0.322</td>
</tr>
<tr>
<td>Proportion of</td>
<td>0.375</td>
<td>0.35</td>
</tr>
</tbody>
</table>

Note: Each CCF cause has been assigned to the category of simultaneous or non-simultaneous failure (or split equally between them) or running (rather than standby) systems. It is seen that approximately 1/3 of failures would be expected to affect running systems simultaneously.

*Table 4. Classification of CCF (taken from reference 7)*
The other factors such as system complexity and the defences against CCF inherent in the design, operating and maintenance of the system will have less effect on the $\beta$ factor. This also applies to the unrevealed failure rates of dormant protective and standby equipment, however, their impact on common-cause failures should be systematically evaluated during the system reliability assessment and reductions in the beta factor applied where appropriate.

Proper consideration of redundancy, diversity and these other factors will generally lead to smaller beta factors and thus lower common-cause failure rates in system reliability studies. Unless realistic values are employed the common-cause failure probability is likely to be dominant so that the impact of specific combinations of independent failures may not be accorded the importance they actually warrant.

Data input to a fault tree needs careful consideration since it can influence the importance ranking of the minimal cut sets. Common-cause failure rates and thus the beta factor to be applied, need as much if not more consideration than the data for independent failures to ensure that realistic minimal cut set probabilities are generated by the analysis.

Beta factors should be applied to the most reliable channel, that is, the channel with the lowest independent failure probability.

7 EXAMPLE OF APPLICATIONS

Fault Tree Analysis with CCF

Figure 2 shows the preferred way to incorporate common-cause failures in fault trees. This fault tree illustrates how the four component failures A1, A2, B and C can combine to produce system failure. Both A1 and A2 have a common cause event CCFA. Boolean reduction is applied to this fault tree to obtain the minimal cut sets as follows:
\[ T = G_1 \cdot G_2 \]

Since \( G_1 = A_1 + CCFA \) and \( G_2 = B + G_3 \)
\[ T = (A_1 + CCFA) \cdot (B + G_3) \]
\[ = A_1 \cdot B + A_1 \cdot G_3 + CCFA \cdot B + CCFA \cdot G_3 \]

substituting for \( G_3 = G_4 \cdot C \)
\[ T = A_1 \cdot B + A_1 \cdot (G_4 \cdot C) + CCFA \cdot B + CCFAA \cdot (G_4 \cdot C) \]

Finally substitute \( G_4 = A_2 + CCFA \)
\[ T = A_1 \cdot B + A_1 \cdot C \cdot (A_2 + CCFA) + CCFA \cdot B + CCFA \cdot C \cdot (A_2 + CCFA) \]

expanding and reducing we get
\[ T = A_1 \cdot B + A_1 \cdot C \cdot A_2 + CCFA \cdot B + CCFA \cdot C \]

Minimal cut sets are then:

- B.A1
- B.CCFA
- C.CCFA
- C.A1.A2

If the basic events have the following probabilities:

- \( P(A_1) = P(A_2) = 0.1 \)
- \( P(B) = 0.2 \)
- \( P(C) = 0.3 \)
- \( \beta = 0.2 \) hence
- \( CCFA = \beta \cdot 0.1 = 0.02 \)

Using the Rare Event approximation to obtain the top event probability we get

\[ P(T) = (0.2 \times 0.1) + (0.2 \times 0.02) + (0.3 \times 0.02) + (0.3 \times 0.1 \times 0.1) \]
\[ = 0.02 + 0.004 + 0.006 + 0.003 \]
\[ = 0.033 \]
The effect of diversity on the top event probability for the fault tree in Figure 2 can be seen below for redundant, partially and fully diverse channels:

![Fault Tree Diagram]

*Figure 2. CCF incorporated at primary event level*

<table>
<thead>
<tr>
<th>MINIMAL CUT SETS</th>
<th>REDUNDANT $\beta=0.2$, $\text{CCFA}=0.02$</th>
<th>PARTLY DIVERSE $\beta=0.02$, $\text{CCFA}=0.002$</th>
<th>FULLY DIVERSE $\beta=0.002$, $\text{CCFA}=0.0002$</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.A1</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>B.CCFA</td>
<td>0.004</td>
<td>0.0004</td>
<td>0.00004</td>
</tr>
<tr>
<td>C.CCFA</td>
<td>0.006</td>
<td>0.0006</td>
<td>0.00006</td>
</tr>
<tr>
<td>C.A1.A2</td>
<td>0.003</td>
<td>0.003</td>
<td>0.003</td>
</tr>
<tr>
<td>TOP EVENT</td>
<td>0.033</td>
<td>0.024</td>
<td>0.0231</td>
</tr>
<tr>
<td>PROBABILITY</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The contribution from common cause failures might be further reduced if consideration had being given to the defences against CCF incorporated into design and operation. If failures were also revealed then the contribution to CCF could perhaps be a factor of 4 or 5 lower in all cases than the figures shown above. However, it can be seen that the major impact on the CCF contribution will be through the incorporation of diversity in the redundant channels.

8 ALTERNATIVE APPROACHES TO COMMON-CAUSE EVENT FREQUENCIES

This paper has concentrated on the Beta factor approach to obtain the probability of occurrence of the common-cause events. The Beta factor method is only one of the many approaches that can be used to calculate this probability. Some of the more popular alternatives are: the binomial failure rate method [9] and the multiple Greek letter method [10]. A brief description of these methods is given below.

Binomial Failure Rate Method

This model assumes that there are two types of failure which can affect the multiple channels of a redundant system: random type failures which will cause failure in a single channel, and lethal or non-lethal shocks which can affect any number of channels. For non-lethal shocks each channel is assumed to have an independent failure probability, for lethal shocks all channels fail simultaneously.

For a system of \( m \) channels of which \( k \) channels fail simultaneously, this model gives

\[
Q_k = \begin{cases} 
Q_i + \mu \rho (1-\rho)^{m-1} & k = 1 \\
\mu \rho^k (1-\rho)^{m-k} & 1 < k < m \\
\mu \rho^m + w & k = m 
\end{cases}
\]

where \( Q_k \) — the frequency of \( k \) out of the \( m \) channels failing

\( Q_i \) — the independent failure frequency for each component
\[ \mu \quad - \text{the frequency of occurrence of non-lethal shocks} \]

\[ \rho \quad - \text{the conditional probability of failure of each component given a non-lethal shock} \]

\[ w \quad - \text{the frequency of occurrence of lethal shocks} \]

This model is a four parameter model requiring values for \( Q, \mu, \rho \) and \( w \). Scarcity of good quality data can make it difficult to accurately estimate these parameters.

**Multiple Greek Letter Method**

This method is an extension of the Beta factor method to systems with more than two redundant channels. The specific form of the mathematical equation is dependent upon the number of channels but as a general illustration:

\[ Q_k = \frac{1}{(m-1)(k-1)} \prod_{i=1}^{k} F_i (1 - F_{k+1}) Q_i \]

\[ Q_k \quad = \text{the frequency of simultaneous failure of} k \text{ components} \]

\[ F_1 = 1 \]

\[ F_2 = \beta \quad = \text{the conditional probability that the common-cause of a component failure will be shared by one or more additional components} \]

\[ F_3 = \gamma \quad = \text{the conditional probability that the common-cause of a component failure that is shared by one or more components will also be shared by two or more components additional to the first} \]

\[ F_4 = \delta \quad = \text{the conditional probability that the common-cause of a component failure that is shared by two or more components will also be shared by three or more components, additional to the first} \]

\[ Q_t \quad - \text{the total failure frequency due to all independent common-cause events} \]
Again the difficulty in applying this model is the accurate estimation of the several parameters required.

9 OBSERVATIONS

Common-cause failure effects need to be considered in reliability studies. The factor model provides a practical means of incorporating these effects in fault trees. Currently the authors feel that the mean value of $\beta$ recommended by Edwards and Watson in 1979 is probably unduly pessimistic for power/process system safety studies. From the evidence of more recent surveys (Refs 6 and 7) a more representative estimate for the mean value of $\beta$ of 0.1 is probably the most realistic at the present time. However, lower (and higher) values have been experienced with certain equipment and wherever possible these should be adopted as best-estimates of the base value and incorporated into fault trees at the appropriate level after applying additional modifying factors.

The effect of diversity is particularly important in limiting the effect of CCF. Attention to defences against CCF during design, construction, operation and maintenance can also significantly reduce this effect.

Clearly there is a need to collect and analyse CCF data to improve the precision of common cause failure analysis.

10 REFERENCES


