The Use of Engineering Judgement in Dependent Failure Analysis

G. M. Ballard
UKAEA, Warrington, UK

1. Introduction

The recognition that dependent failures of engineering components and systems are a major contributor to the risk from nuclear power plant is now well established. The subject of common cause failure or common mode failure, to use two of the alternative titles in common use, had been treated by engineers as rather nebulous and perhaps a figment of the safety analyst's imagination. Fortunately, or perhaps unfortunately, incidents during NPP operation have demonstrated quite clearly (Ref 1) that dependent failures are real and significant. Thus, although there is still resistance in some quarters, both plant designers and operators, and safety analysts have had to find an acceptable method of incorporating this issue in plant safety cases.

This is not an easy problem as the considerable volume of recent papers on the subject has demonstrated. The subject starts with an air of unreality and is frequently continued by complex mathematical manipulations which seem to bear little relationship to the engineering characteristics of the plant. If real progress is to be made in improving plant defences against dependent failures there is an urgent need for dependent failure analysis (DFA) to be more systematic and understandable.

The recent Procedures Guide (Ref 2) published by the USNRC was a major step forward and one in which the UKAEA Safety and Reliability Directorate was very glad to collaborate. However, while this guide helps to systematise DFA particularly with regard to qualitative analysis, it does not manage to tie the quantitative analysis effectively to engineering design and operation; it still leaves it as a rather mathematical exercise.

SRD has been trying to bridge this gap between mathematics and engineering in DFA and this paper summarises some of the developments along that path.

2. Current Problems

Dependent failure analysis really began with the recognition that redundant configurations did not necessarily provide the level of reliability calculated using independent component failure rates. The response was to try to provide some numerical limit for the system reliability based on simple parametric models. The range of models used included

- a generic system reliability cut-off value
- the β factor model
- the Multiple Greek Letter (MGL) model
- the Binomial Failure Rate (BFR) model.

A characteristic of all these models is that very sparse generic date is used to support a simple extrapolation based on one or two parameters. Thus, the cut-off model (Ref 3) gives generic data for a few system configurations, the β factor model (Ref 4) extrapolates on the basis of an empirical correlation, with component failure rate, the MGL model (Ref 5) generalises the β factor model to several parameters and, finally, the BFR model tries to derive data driven values (Ref 6) for a statistical shock model. None of the models incorporates any engineering information concerning the design and operation of a specific plant, although some attempt has been made to derive model parameters for individual component types. The task of reflecting plant engineering has been transferred to the process of providing data for model parameter estimation.

The success or otherwise of this strategy can perhaps best be seen from the results of the European Benchmark exercise (Ref 7). In the first phase of that exercise, 10 different teams performed a qualitative and quantitative reliability study of an Auxiliary Feedwater System on a German PWR. The teams had the same information from the plant (including a system fault tree) but otherwise did not collaborate and used their own methods and data. The results are shown in Fig 1 and demonstrate a large variability of approximately 3 orders of magnitude. In qualitative terms, the teams had similar appreciations of the strengths and weaknesses of this system but their quantitative reflections of this qualitative picture were greatly different.

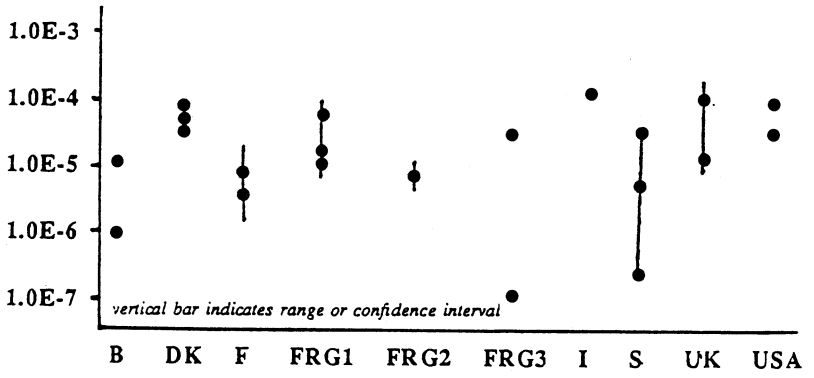

Fig 1 Quantitative results obtained in Phase I.

To demonstrate that this effect was not due to the specific model used or access to different amounts of data, further phases of the exercise compared these factors. The only remaining source of major variability was the interpretation that the teams placed on data in calculating the parameters of their model. Generally, the process of data screening was neither systematic nor in a proceduralised form which other people could see and understand.

This illustrates one of the fundamental problems of dependent failure analysis - the application of engineering judgement is the most significant factor influencing DFA but this application is not proceduralised. With widely differing perceptions of a rather nebulous phenomenon, it is not surprising that large variations in dependent failure assessment exist.

3. Possible Ways Forward

Two contributions to the CCF RBE did attempt to systematise to varying degrees the engineering judgement that has to be applied.

The US team applied the Impact Vector method (Ref 2). In summary, this method requires the analyst to review all data events within a database and

(a) decide if the event is applicable in any form to the plant being studied,

(b) decide whether the event is applicable to the reactor power state being studied,

(c) decide what impact (in terms of number of failed components) the event would have had if it had occurred on the plant under study.

(d) A β factor (or MGL parameters) is then calculated using the modified sub-set of events derived by the analyst.

This is a valuable procedure which ensures some level of visibility of the engineering judgement being applied. It is also possible to formulate some guidelines for this procedure (Ref 7) but these are rather unspecific. Thus, for example, when during the CCF RBE the same set of events were screened for applicability the US team eliminated 75 events while the UK team eliminated only 29 events. Such is the range of viewpoint!

The UK team applied a number of DFA models to the CCF RBE one of which was a so-called partial β factor approach (Ref 8). This approach was an early attempt to guide the application of engineering judgement. In summary the process, shown in Fig 2, involves the specific consideration of system design and operation characteristics which are considered to be (Ref 8) useful defences against dependent failures. These defences are shown in relation to a classification of common mode failure (CMF) causes. The analyst is asked to say how the various defensive issues apply to the particular system under study. In order to reflect these qualitative comments into quantitative statements, a table of partial β factors is provided. This table was generated by a wide ranging review of event data involving the assessment of the effectiveness of various defences. From this review the maximum potential effectiveness of each defence has been quantified (by a combination of calculation and judgement) on a scale of zero (eliminates all CCF) to unity (has no effect on CCF). The analyst is asked to assess the extent to which individual defences have been applied by assigning a value between the minimum value (fixed by the method) and unity (no application of the defences). The final result of this process is a β factor assembled from all the individual judgements required from the analyst.

Both the Impact Vector Method and the partial β factor approach attempt to make progress by asking specific questions of the analyst rather than leaving him to make global judgements. In effect, the analyst is guided to his final assessment in a number of small steps. However, neither of the methods provides the analyst with a clear engineering model of the structure and cause of dependent failure events in order to help him reach his judgements. In the case of the Impact Vector Method, this is necessary to help the analysis interpret the event descriptions and the applicability to different plant. In the case of the partial β factor method, such a model would help the analyst in assessing the degree of impact particular design and operation features may have in relation to defences against dependent failures.

4. A Dependent Failure Model

By definition, a dependent failure event is one in which there are failures, of multiple equipments or systems, which are not dependent. As a consequence, the probability of occurrence of such an event is not accurately reflected by the normal multiplication of individual failure probabilities and may, in practice, be of significantly higher probability that would be indicated by such a calculation which assumes failure independence.

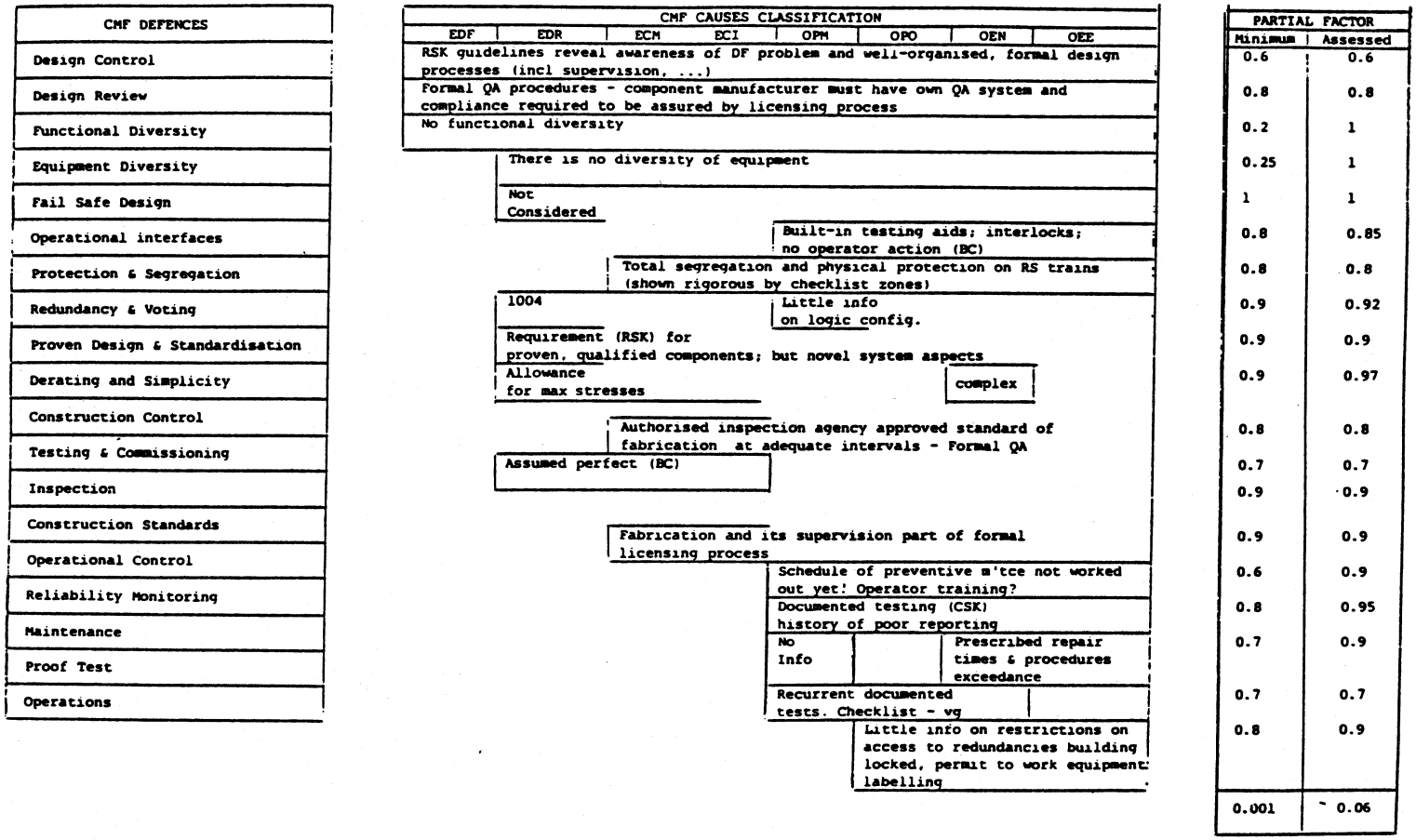

Fig 2 Assessment of β Factor

Take a typical example of an operational event.

Example 1

With the reactor at 20% power, two reactor coolant pumps (RCP) were shut down for testing. The reactor protection system (RPS) failed to see either pump trip. The two RCPs were restarted and the other two RCPs were tripped. Again, the RPS failed to see either pump trip.

Investigation of this incident, which involved the failure of 4 under power monitoring circuits to detect pump trip, revealed that the relays has been adjusted 2 days earlier in accordance with the relay manufacturer's specification. However, for this particular application, the relays had to be adjusted to operate at a specific pre-determined power level.

Analysis of this incident form a dependent failure point of view would indicate:

- the design involved redundancy of relays which were of the same type and same manufacture
- the relays were reset at the same time
- the relays were probably reset by the same staff using the same procedure in each case.

Failure of a relay due to setting/calibration errors is not an unexpected failure cause and one which would be included in the relay failure rate. However, in this case, all the relays failed by the same cause, thus generating a multiple dependent failure event because of the strong similarity between the design and operational characteristics of the relays.

This type of analysis of operational events which have involved dependent, multiple failures suggests that the anatomy of such events may be described as shown in Fig 3 in terms of a trigger, coupling mechanisms and defences.

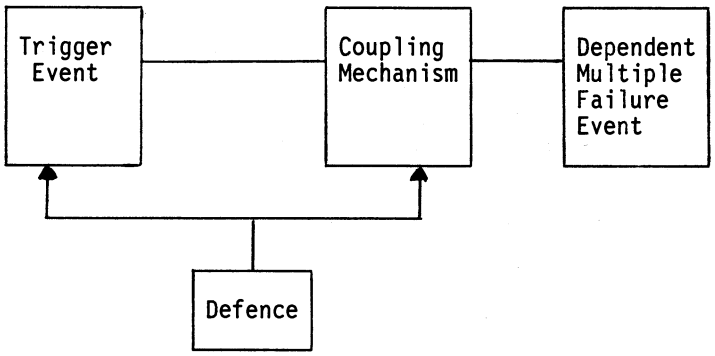

Fig 3 Essential anatomy of an event involving dependent failure of multiple components

Any multiple failure event must, obviously involve at least one equipment failure. The root cause of that equipment failure is always a potential trigger for the failure of other items of equipment. Given that a cause for one equipment failure exists, there has to be a reason why other equipment should fail in a dependent manner. Thus, the coupling mechanism is the link between one equipment failure and other equipment failures within the multiple failure event. In order for the trigger to lead to a dependent multiple failure event, there has to be a coupling mechanism. If there is no coupling

Table 1 represents a situation in which there is some application of dependent failure defences. Thus, it may be inferred that the widespread use of segregation for redundant components will have reduced the significance of the "same location" coupling mechanism below its potential strength. Nonetheless, Table 1 represents a useful baseline reflecting average current practice.

The analyst is now asked to identify features of the particular plant design and operation which contribute to diversity of the cutset components and for each of the coupling mechanisms. He is then asked to judge to what extent the identified diversity constitutes total diversity for that coupling mechanism. Thus, two different manufacturers of pumps do not comprise total diversity since there remains much in common between the pumps, including their operating principle and their design specification.

Judgements concerning this degree of difference are unfortunately a weakness of this approach, because there is little data available on the effectiveness of partial diversity. This, however, is the state of our knowledge and therefore the practical limit to providing definitive guidance of the application of engineering judgement. Nonetheless, considerable progress has been achieved because the uncertain judgement element has been severely constrained by the model. The analyst cannot arbitrarily reduce the quantitative parameters for the assessment; he has to justify a number of individual judgements, each of which has a limited effect because of the data-driven constraints.

The end result is, therefore, represented in Table 2 where for each coupling mechanisms the analyst assesses a factor γ between unity (little or no difference in cutset components) and zero (total effective diversity between cutset components). These γ factors multiply the previous partial β's to determine a new effective β for the specific plant under study.

Two important points to note are firstly that the procedure should ideally apply to each cutset of interest, although in practice many cutsets feature the same type of equipment and, therefore, can effectively be grouped together. Secondly, the general β value in equation (i) and the initial partial β's in equation (ii) will depend on the type of equipment being considered. However, the database is broadly adequate to give useful estimates for these parameters in a few broad classes of components.

6. Summary

The major points of the foregoing discussion are:

(i) Engineering judgement, which is essential at the current stage of dependent failure analysis, must be guided and limited by an engineering model and data.

(ii) The judgements required should be as limited as possible and be specific to engineering descriptions of the plant and its operation. The analyst is not asked for probabilistic judgements but for his knowledge of the design and operation of the plant.

(iii) The concepts of the TCM model are used to emphasise the different aspects of dependent failure defences; most notably that action on component failure rate is useful but not fundamental to the problem of dependent failures. The only fundamental defence is diversity.

(iv) There is sufficient data from operational events to provide useful input to a variety of parametric models but the information on the effectiveness of different degrees of diversity is still largely qualitative. This is a limitation on our current knowledge dictated by the very limited past use of diversity.

(v) Notwithstanding the limited data availability, the analyst is required to specifically support his quantitative judgements by identified differences between the cutset components. This makes the analysis open to independent consideration.

7. Conclusion

The USNRC guidance (Ref 2) has been an extremely valuable culmination of much development over the past years. It is, however, essential to avoid data screening judgements prejudicing these advances. There is still too frequently a view that fundamental problems of dependency can be avoided by relatively superficial changes in design or operation. This view is not supported by operational evidence and the structure for applying engineering judgement must, therefore, emphasise the fundamental aspects of dependent failure. The TCM model as interpreted in this paper appears to provide that structure, and will be capable of further refinement as more data to guide judgements becomes available.

References

1. Ballard, G M. (1985). An Analysis of Dependent Failures in the ORNL Precursor Study. Proceedings ANS/ENS Meeting on Probabilistic Safety Methods and Applications, San Francisco, pp 6-1.

2. Procedures for Treating CCF in Safety and Reliability Studies. NUREG/CR-4780.

3. Bourne, A J, Edwards, G T, Hunns, D M, Poulter, D R and Watson, I A. (1981). Defences Against Common-Mode Failure in Redundancy Systems; A Guide for Management, Designers and Operators. SRD R 196.

4. Fleming, K N et al. (1978). HTGR Accident Initiation and Progression Analysis. USDOE GA-A15000.

5. Fleming, K N and Kalinowski, A M. (1983). An Extension of the Beta Factor Method to Systems with High Level of Redundancy. PLG-0289.

6. Atwood, C L. Common Cause Fault Rates for Pumps. NUREG/CR-2098.

7. Poucet, A, Amendola, A and Cacciabue, C. (1986). Summary of the Common Cause Failure Benchmark Exercise. JRC Ispra, PER 113/86.

8. Johnston, B D and Humphreys, P. SRD Dependent Failures Procedures Guide, SRD R 418. To be published.

Table 1. Relative Frequencies of Active Coupling Mechanisms in Failure Events

Same Hardware (all aspects)		.47
Same staff	- operation	.08
	- test	.05
	- maintenance	.05
Same procedure	- operation	.06
	- test	.11
	- maintenance	.04
Same environment		.11
Same location		.03
		1.00

Table 2. Assessment of Strength of Coupling Mechanisms

Coupling Mechanism	Average Strength	Degree of Diversity	Specific Strength
		$\gamma = (1 \rightarrow 0)$	
1	β_1	γ_1	$\beta_1 \gamma_1$
2	β_2	γ_2	$\beta_2 \gamma_2$
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
η	β_η	γ_η	$\beta_\eta \gamma_\eta$
	1		≤ 1