COMMON CAUSE FAILURE MODELLING IN CANDU DESIGN PSA

Warren Vesik
Atomic Energy of Canada, Ltd.
2251 Speakman Drive
Mississauga, Ontario, Canada L5K 1B2
(905) 823-9040

ABSTRACT

At AECL, an increasing focus is being placed on using probabilistic safety assessment as part of the development of the established CANDU 6 and new CANDU 9 nuclear power plant designs. Fault tree/event tree analysis is being used to provide insight into the dominant contributors to plant risk. An important part of this process is the evaluation of dependent failures, and in particular, common cause failures which can have a significant impact on system reliabilities. This paper describes the common cause failure analysis method employed by AECL, its usefulness as a design audit tool, and the effects of common cause failure on CANDU system reliabilities.

I. INTRODUCTION

Common cause failures (CCFs) which render multiple redundant components unavailable generally occur much less frequently than individual component failures. Nonetheless, their impact on system reliability can be quite significant, depending on the characteristics of a given design. This combined importance and rarity of CCF events makes the selection of a method of evaluation difficult, particularly given the abundance of CCF modelling techniques and the judgmental nature of CCF analysis.

One of the fundamental problems in performing CCF analyses for CANDU is that the reliability data collection has generally been focused on calculating total failure rates of components. No distinction has been made between single and multiple component failures. Therefore there are no data that would allow straightforward evaluation of CCF failure rates based on a simple number of events per demand calculation.

For this reason, it is necessary to use a parametric model that allows calculation of CCF rates with a minimal amount of data input. To address this problem, AECL has adopted the Unified Partial Method[1] (UPM) to perform common cause failure analyses.

At present, the UPM is being applied to AECL's CANDU 6 and CANDU 9 reactor designs. CANDU 6 is a single unit, 700 MWe reactor that is in operation in a number of countries and for which the design continues to evolve. A probabilistic safety assessment has previously been performed in-house for this reactor type.[2] In contrast, the detailed design of the 900 MWe CANDU 9 is ongoing, and system reliability models are being developed in conjunction with this effort.

For CANDU 6, the reliability analyses ensure that any proposed enhancements to the plant take into account the impact of CCFs on risk. In this way design changes can be optimized in terms of the amount of redundancy, diversity and inter-component separation that is incorporated within the constraints of the existing plant layout.

For CANDU 9, there is even greater opportunity to make design decisions based on insights from reliability analysis. Particular care is being taken to identify any non-obvious dependent failure mechanisms which can adversely affect system reliability, and the CCF analysis is an important part of this process. Feedback to the designers will ensure that reliability targets are met by reducing the

vulnerability of critical components to CCFs and adding redundancy and diversity to systems where appropriate.

A description of the CCF analyses performed at AECL is presented in the following sections, highlighting the advantages and limitations of the UPM. Results for selected systems and components are also described.

II. METHODOLOGY

The UPM is a single parameter model for common cause failures in the sense that the final result of the analysis is a beta factor. The beta factor multiplied by the total component failure rate produces a CCF rate for a given multiple component group.

The evaluation of a beta factor for a particular group of redundant components is made by a series of judgments relating to eight topics which are expected to have an impact on redundant component vulnerabilities to CCF. The analyst is required to assess a "partial" beta-factor for each of these topics. To determine each partial beta-factor, the UPM requires the analyst to choose one of five generic system definitions which most closely matches the system under review. The partial beta-factors are then combined together to obtain an overall beta-factor. The eight partial beta-factors considered in the UPM are:

- redundancy/diversity of components
- separation between components
- level of understanding of the system/components (e.g. years of system operation, system complexity)
- prior analysis of the system (e.g. fault trees/FMEA)
- man-machine interface
- plant safety culture
- control of components' operating environments
- environmental testing of components

The method has been calibrated with weightings on each of these sub-factors to generate beta-factors which lie within a range of values typically observed in the nuclear industry.

The system fault trees at AECL have been developed with a high degree of detail. In general, control and instrumentation (C&I) failures have been modelled separately from the mechanical failures of the components being actuated. Therefore, fuses, relays, handswitches and the like all make separate contributions to the system unreliability. This complicates the CCF analysis because it greatly increases the number of component groups for which a beta factor must be evaluated. Therefore, an approach similar to that used in a previous plant-specific CANDU PSA[3] has been adopted to simplify the analysis.

First, the component boundaries are expanded to encompass both the mechanical components and their controlling C&I logic. The combined failure probability of these grouped components is calculated, and a "screening" beta factor is applied to this total value. New CCF basic events are incorporated in the fault tree model as appropriate. After obtaining the minimal cutsets of the fault tree, it is a simple matter to determine which CCF events make a significant contribution (e.g. more than 1%) to the total unreliability. The UPM is then applied to these component groups to refine the analysis results.

A. Advantages and Use of the UPM for CANDU Reliability Analysis

Generic CCF data are available in many references for components typically found in nuclear power plants.[4,5,6] However, there is no clear basis for applying generic beta factors to CANDU, since the data on which they are based may include some failures which are not possible in a CANDU plant. On the other hand, there may be particular features in a CANDU plant that make CCFs more likely in certain areas. It is thought that careful application of the UPM resolves this issue to some extent, and in addition provides CCF rate estimates for component types for which the generic data may be sparse or unavailable.

The other advantage of using the UPM as seen by AECL is that it allows the analyst to take credit for good design practices when making judgments regarding the most suitable partial beta factors. Conversely, poor design practice is penalized by the method. Therefore, if it is found that CCF of a particular group of components dominates the system unreliability, there is a good indication that the system would

be improved with increased redundancy, better component layout or greater diversity. It is hoped that if the designers are made aware of the potential quantitative impact of their decisions, then the means by which dependent failures may be defended against will be considered starting from the initial design concept through the final design.

One example of the implementation of a design for which particular care has been taken to guard against dependent failures is the CANDU 9 ventilation isolation system. The design process has also benefited from feedback from the system reliability and CCF analyses.

The system consists of two sub-systems, each designed to independently isolate the main ventilation lines penetrating the reactor building. A single sub-system consists of isolation dampers and instrumentation for the two parameters which can initiate containment isolation - high radiation or high pressure within the containment. The equipment for each subsystem will be procured from different manufacturers, and located as far away as is practically possible from the redundant sub-system.

Separation is achieved by locating the sub-systems on opposite sides of the reactor building wall, so that the operating environments are different. An exception is the redundant sets of sensors used to detect high pressure in the building, which have been located at opposite sides of the containment. In addition to a good degree of separation, the radiation monitors of each sub-system have diverse operating principles, to minimize the possibility of CCF. Human errors during maintenance or calibration tasks that might incapacitate both sub-systems are greatly reduced since they will be performed by different personnel, with separate procedures.

The reliability analysis of the combined system revealed a CCF occurring in one sub-system which could potentially impair the operation of the second sub-system. In order to meet the overall reliability target, a design change introducing a third initiation parameter (low ventilation flow) to each sub-system was identified. This demonstrates the value of integrating the reliability and CCF analyses into the design process.

B. Limitations of UPM

One of the limitations of UPM that has been identified in the course of AECL's CCF analysis is the treatment of highly redundant systems. Lower failure rates are obtained for component groups with a one out of eight success criteria than for components groups with simple one out of two or two out of three redundancy. However, it is not clear how to assess the more general m out of n success criteria. Since redundancy represents only one of the eight partial beta factors, inevitably the other seven factors quickly become dominant as the redundancy is improved. Therefore there is a rather inflexible cut-off value below which the CCF rate may not be reduced. Since inevitably the beta factor is applied across the entire component group, the fault tree evaluation produces a minimal cutset that represents failure of all the items in the group. Thus one arrives at the anti-intuitive result that the probability of failure of two adjacent valves in a one out of two arrangement is quite close to the probability of failure of nine out of sixteen valves in a widely spaced arrangement. Whether or not this leads to unacceptably conservative results relative to other methods is currently under investigation.

The other potential concern with the UPM is the fact that it does not distinguish between component types. There is some difference in the treatment of mechanical and electrical components, but, for the most part, given a certain standard of design, the calculated beta factors for valves, pumps, fans, instrumentation and numerous other items will be similar. This is also true of the particular failure modes considered, since the method does not distinguish between running and starting failures. Therefore it is useful to compare generic beta factors with some sample results of the UPM to see if there are any significant discrepancies.

III. CCF Analysis Results

Table 1 compares some generic beta factors obtained from the literature[4,5,6] for selected equipment with some of the results obtained with the UPM. It is apparent that although the absolute values of the generic and UPM beta factors are different, the relative values of the various equipment types do have a similar trend. For example, diesel generators have the lowest beta factors in both cases. It can also be stated that the values are generally within a factor of two, with the exception of the diesel generator failure to start result. On this basis, the UPM results are acceptable for design PSA purposes. Whether the predicted CCF rate for a given set of components is reasonable or not can only be judged from accumulated plant-specific data. If the design PSA becomes the starting point for a "living" PSA, the CCF rates or beta factors can be updated as operating experience is gained.

The effect of CCF on selected CANDU system reliabilities is shown in Table 2. The results have been found to be highly system dependent. As might be expected, the lower the system reliability assuming that failures are independent, the greater the impact of CCFs. Therefore for power systems with one out of two redundancy, the effect of CCF is to increase the system reliabilities by about 35% or less. The effect of CCFs is limited since there are independent failure combinations of equal magnitude in these systems.

EQUIPMENT	FAILURE MODE	UPM BETA FACTOR	GENERIC BETA FACTOR
pneumatic valve	fails to operate	0.12	0.17
safety/relief valve	fails to open	0.053	0.095
diesel generator	fails to start	0.045	0.011
diesel generator	fails to run	0.045	0.027
EWS pump	fails to start	0.11	0.2*
EWS pump	fails to run	0.11	0.098*

*Note: values are for auxiliary feedwater pumps that supply water at higher pressure than CANDU EWS pumps

Table 1 - CANDU UPM Beta Factors vs. Generic Data

SYSTEM	UNAVAILABILITY WITHOUT CCF	UNAVAILABILTY / UNRELIABILITY INCREASE
CANDU 6 Emergency Power Supply	1.6E-2	28 %
CANDU 6 Emergency Water Supply	1.7E-2	7-9 % (depending on operating mode)
CANDU 6 Steam Generator Crash Cooldown (one sub-system)	3.6E-5	20 times
CANDU 6 Class III Power System	2.9E-2	35%
CANDU 9 Shutdown System #2	3.3E-5 to 5.6E-4 (depending on trip parameter)	1.7 to 9 times (depending on trip parameter)
CANDU 9 Ventilation Isolation System	1.0E-4	9 times

TABLE 2 - Effect of CCF on Reliability of Selected CANDU Systems

In contrast, the CANDU 6 steam generator crash cooldown system reliability changes by a factor of twenty, and the CANDU 9 system reliabilities increase by up to nine times. In all such cases, the results are dominated by CCFs, reflecting the lack of any inherently unreliable components or single failures in the systems.

In particular, the crash cooldown result is attributable to the success criteria of the system, in which seven out of sixteen safety valves are required to open. If only independent failures are considered, then combinations of valve failures result in a very low value for the system unavailability. Once the CCF dependency is introduced, the frequency of all of the valves failing increases markedly. These valves are of considerable importance not just in terms of the reliability of this particular system, but also in terms of their significance to the overall plant risk. Therefore a model which is better geared to high levels of redundancy should be applied to this system in future, to increase the level of confidence in the predicted system unavailability.

IV. SUMMARY

The Unified Partial Method has been applied to a number of generic CANDU 6 and CANDU 9 systems to estimate common cause failure rates. The beta factors for a variety of component types

have been calculated and judged to be acceptable in comparison with available generic data. During this early phase of its use, the method has also proven to be of value as a design audit tool. Overall, the effect of CCF on various CANDU systems has been found to be highly variable. In general, the percentage change in reliability when CCF events are added to the system model is larger for more reliable systems.

REFERENCES

1. V.P. Brand, "UPM 3.1: A Pragmatic Approach to Dependent Failures Assessment for Standard Systems", *SRDA-R13*, SRD Association, Cheshire, UK (1996).

2. H.S. Shapiro et al., "Overview of the CANDU 6 Wolsong NPP 2/3/4 Probabilistic Safety Assessment", *Proc. International Conference on Probabilistic Safety Assessment Methodology and Applications (PSA '95)*, Vol. 1, pp. 495-500, KAERI, Taejon, Korea, (1995).

3. Joon-Eon Yang et al., "Analysis of Common Cause Failure in Wolsong 2/3/4 NPPS PSA", *Proc. Fifth International Topical Meeting on Nuclear Thermal Hydraulics, Operations and Safety (NUTHOS-5)*, I5, pp. 1-6, Beijing, China, (1997).

4. J.A. Steverson and C.L. Atwood, "Common Cause Fault Rates for Valves: Estimated Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants 1976-1980", *NUREG/CR-2770*, NRC (1983).

5. C.L. Atwood, "Common Cause Fault Rates for Pumps: Estimates Based on Licensee Event Reports at U.S. Commercial Nuclear Power Plants, January 1, 1972 through September 30, 1980", *NUREG/CR-2098*, NRC (1983).

6. K.N. Fleming et al., "On the Analysis of Dependent Failures in Risk Assessment and Reliability Evaluation", *Nuclear Safety*, Vol. 24, No. 5 (1983).