Common Cause Failures in PSA Applications

Ola Bäckström[a], Xuhong He[a], Pavel Krcal[a], and Pengbo Wang[a]
[a] RiskSpectrum AB, Stockholm, Sweden, {Ola.Backstrom, Xuhong.He, Pavel.Krcal, Pengbo.Wang}@riskspectrum.com

Abstract: High redundancy contributes to availability of safety systems. It is essential for a realistic assessment of this contribution to take possibilities of common cause failures of symmetrical components into consideration. This failure mechanism breaks the independence assumption for basic events in fault trees, causing the quantification of some events to become conditional on the state of others. This dependency has implications for various applications of a Probabilistic Safety Assessment (PSA) model where different scenarios - each possibly altering the state of events - are evaluated.

In this context, we examine the expected results when using a PSA model within the Significance Determination Process, in online risk monitoring and in different scenarios and expectations when calculating the Risk Increase Factor (also known as Risk Achievement Worth) in a normal PSA calculation. In all these applications, some components are considered unavailable. When these components share common cause failures with other components then there are multiple options how to perform the conditional quantification of common cause failure events. We outline different real-life situations and develop formulas that reflect the common cause logic involved. Furthermore, we argue for an implementation that allows users to specify which of the formulas should be applied, based on their knowledge of the scenario at hand.

Additionally, we discuss the symmetry assumption of standard parametric common cause failure models. The Basic Parametric Model relaxes this assumption because it does not require the total basic event probability in the quantification. This allows us to model situations where a conservative modeling approach would otherwise be necessary if standard parametric models were used. We also describe the new implementation of this common cause failure model in RiskSpectrum PSA.

1. INTRODUCTION

Common cause failures make several redundant trains of a safety system unavailable by a single cause. Possibility of such events does not allow us to count the safety benefit of redundancy fully. It relativizes the assumption of independence between basic events – failures of individual components. We need to find a good middle way between the full credit for redundancy and ignoring its safety benefits altogether. The first one might not reveal relevant risks and by this will keep us ignorant and optimistic when it comes to the actual safety status. This decreases motivation to improve the plant design or to operate it in a safer manner.

The other extreme makes it impossible to assess real benefits of redundancy and to rationally prioritize investments in safety. By this, it also decreases motivation to improve either in design or in operation. A more realistic consideration of common cause failures requires a practically applicable mathematical model complemented by processed operational data that allows us to apply such model when needed. A lot of effort has been devoted to both. With this, common cause failure modeling became a standard, easy to use tool for including these dependencies in probabilistic models.

Average estimates give us a picture of the plant safety profile in the long run. It does not assume anything about the current state of the plant. This information is irrelevant from the long-term perspective. Apart from an average estimate, a probabilistic model can be used to evaluate a specific situation, real or hypothetical as in case of a maintenance plan. We might be interested in risk-informed

prioritization of operational decisions, risk-informed assessment of unexpected events, or evaluation of design choices based on their expected contribution to safety.

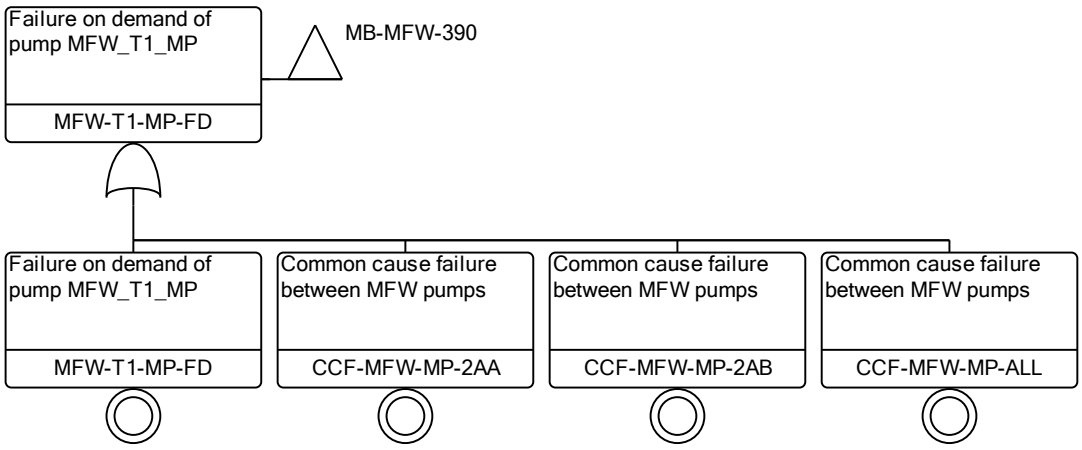
Quantification of common cause failures might be affected by switching from an average case to a specific situation. These cases have been recognized, and different solutions have been proposed. We argue for a flexible approach that allows analysts to determine the appropriate approach flexibly and with good granularity over the model. At the same time, quantification must remain transparent and easily verifiable. We describe how RiskSpectrum tools implement these choices.

Standard parametric models for common cause failures give an answer to the independence assumption, but they introduce a new one. Failures of components that share a common cause must be characterized by the same mathematical model and by the same data. Components within a common cause failure group must be symmetric. This assumption brings some inflexibility to modeling of asymmetric situations. Either we cannot use the established common cause failure framework or we abstract away the differences and model the situation as if it were symmetric. We present how one could trade a reasonably small bit of precision for flexibility that lifts this restriction of classical parametric common cause failure models.

2. COMMON CAUSE FAILURE PRELIMINARIES

Common cause failure modeling is a well-established way of treating dependencies between failures of components, typically of symmetrical ones in redundant trains. The standard modeling approach modifies the fault tree logic by replacing basic events by OR-gates with common cause failure events as inputs. Additionally, it applies parametric common cause failure models for quantification of common cause failure events. A simultaneous failure of several components due to the same root cause corresponds to a common cause failure event that occurs under the OR-gate of all these components. Figure 1 shows a fault tree fragment that replaces the basic event for the failure on demand of pump MFW-T1-MP.

Figure 1. An OR-gate modeling failure to start a pump. This failure can result from an independent cause or from a root cause affecting also other pumps.



Usual parametric common cause failure models partition the unavailability of the original basic event to an independent failure and common cause failures for all modeled combinations of simultaneous failures. Partitioning formulas rely on parameters that are obtained and periodically updated from operational data. The formula for the alpha factor model [1] uses parameters $\alpha_1, \ldots, \alpha_n$, where n is equal to or smaller than the number of components sharing the common cause failure. This number influences how many simultaneous failures we can model by a common cause failure event before we create the common cause failure event representing a simultaneous failure of all involved components. For the

example fault tree in Figure 1, we need three alpha parameters, α_1, α_2, and α_3. Since α_1 can be calculated from the other alpha parameters, we need to specify only α_2 and α_3. A general formula for the alpha factor model is in Equations 1 and 2. Let us by Q_k^m denote probability of a common cause failure event representing that *k* components from a common cause failure group with *m* components fail because of a common cause involving these *k* components.

$$Q_k^m = f_k^m \cdot Q_t \tag{1}$$

where

$$f_k^m = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} \tag{2}$$

and

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \tag{3}$$

Let us call the number f_k^m a *CCF-factor*.

3. PSA APPLICATIONS

A PSA model helps us to estimate frequencies of events that represent serious accidents with consequences for the population, environment, and capital investment. This adds traceable and transparent argument for granting an operating license by the respective national regulator. The complexity and resolution of the model allow us to utilize it additionally in other processes not necessarily directly connected to licensing.

3.1. Significance Determination Process

The Significance Determination Process which utilizes a PSA model to numerically assess the risk significance of an unexpected event or a performance deficiency discovered by an inspection [2]. Such evaluation takes place after the inspection, in the best case in the light of additional knowledge collected during the whole inspection. This creates a difference to Risk Monitoring presented in Subsection 3.2.

These deficiencies that occur during operation of a nuclear power plant are recorded for further evaluation, updates of operational data, and safety improvements. The risk level with the event or deficiency considered is compared to the base level. The increase in risk taken over the duration of the event determines how we classify the event.

If this deficiency or event affects a component which shares common cause failures with other symmetrical components then we need to consider this during the quantification. A common cause failure might be a part of the deficiency, its probability might increase because of the deficiency, or it might be independent of it.

3.2. Risk Monitoring

Risk Monitor software tools such as RiskSpectrum RiskWatcher or Phoenix Risk Monitor utilize PSA models for online evaluation of the plant risk level [3]. When coupled with the plant information system, a risk monitor tool automatically updates the model according to the plant state and runs a calculation that estimates the risk level at this time point. As a result, we get probabilistic support for operational decisions that complement deterministic ones in Technical Specifications.

Events registered in the Risk Monitor might be of different types, a change of plant configuration or a change of weather conditions, or unavailability of a component. In the last case, unexpected

unavailability detected on one train might affect the probability of failures with the same root cause in other trains.

3.3. Design and Configuration Assessment

Importance measures serve as an indicator for prioritization of design or operational decisions [4]. Fractional contribution indicates how much changes to component reliability affect the safety or reliability of the whole system. This makes it suitable for risk-informed evaluation of alternative design options. Risk increase factor (Risk achievement worth) estimates the effect on the overall safety or reliability if a component is unavailable. Results of this analysis help to assess different system configurations.

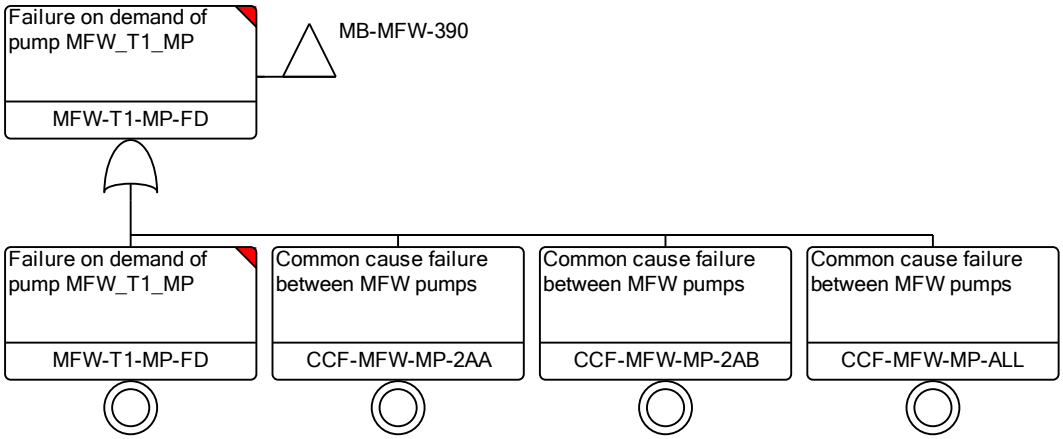
The latter importance measure sets a component or a component group unavailable and reassesses the risk. Like the Significance Determination Process and Risk Monitoring, the unavailability of a component included in a common cause failure group might affect (probability of) unavailability of other components.

4. UNAVAILABILITY OF COMMON CAUSE FAILURE EVENTS

In all cases described in the previous section, at least one component and with it also at least one basic event modeling its unavailability, obtained the failed state. This means that the corresponding basic events will be removed from the Boolean structure. If one of these events belongs to a common cause failure group, then it has been replaced by an OR-gate with common cause failure events as inputs. We have now different options.

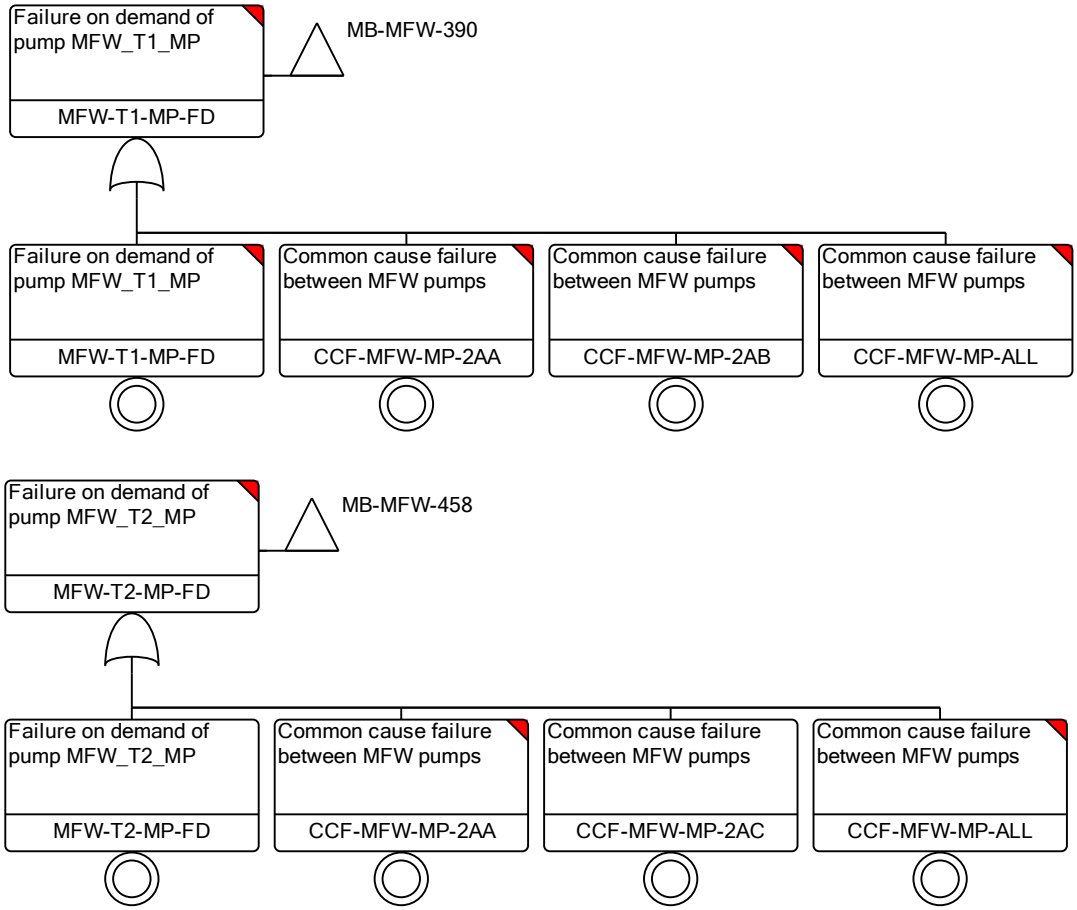
First, we can set only the common cause failure event that corresponds to the independent failure of the component to the failed state. Moreover, we leave the quantification of the other events unmodified. By this we say that this failure has occurred only on the component or group of components indicated. Other components sharing common cause failures are not affected by this. They might fail but these failures will be independent of this event, and they will be governed by the previously established mechanisms. Because the original basic event it replaced by an OR-gate, the failed state of the independent event propagates to the gate and acts as an unavailability of the original basic event for this component. Figure 2 depicts this situation in the Boolean structure. We call this option ‘No CCF’.

Figure 2. An unavailability of the pump in the first train modeled by setting the state of the independent event to ‘failed’. This state propagates to the OR-gate.



Another possibility acknowledges that the other components which share common cause failures with the unavailable one are affected and the modeling solution treats this purely in the Boolean structure by setting all common cause failure events that include the unavailable component to the failed state. This might be a conservative treatment if we do not know the actual state of the other components because we will consider them as certainly unavailable. On the other hand, the solution based on the Boolean logic provides a very simple treatment of common cause failure dependencies. Figure 3 contains the OR-gate for the unavailable component with all common cause failure events set to the failed state. These states propagate also through the Boolean structure of OR-gates for other components. Due to this, the OR-gates for symmetrical pumps in Train 2 and Train 3, which share common cause failures with the pump in Train 1, also becomes unavailable. This is clearly a conservative treatment. Let us denote this option as 'Full CCF'.

Figure 3. A conservative treatment of common cause failure dependencies. The top OR-gate models unavailable pump in Train 1, the bottom OR-gate models pump in Train 2.



The last option takes common cause dependencies into account, but it decreases the conservatism in the treatment. It modifies the Boolean structure in the same way as the 'No CCF' option in Figure 2. The common cause failures involving several components at the same time might occur, but they are not assumed to happen with certainty. The fact that one component is unavailable influences the quantification of these common cause failure events.

We quantify these events conditionally on the occurrence of the individual failure [5]. A common cause failure probability that several components are unavailable at the same time is then calculated given the

fact that one of these components is already unavailable. Derivation of these formulas based on minimal cut sets can be found in Appendix E of NUREG/CR-5485 [1]. Let us first look at a simple example of a common cause failure of two components A and B given that one of them, A, is unavailable. We do not know the cause of this unavailability, but it may also be the same cause that would make also B unavailable. The formula for the probability of the common cause failure of both components is then:

$$P(CCF_{AB}|A) = \frac{P(A|CCF_{AB}) \cdot P(CCF_{AB})}{P(A)} = \frac{f_2^m \cdot Q_t}{Q_t} = f_2^m \tag{4}$$

The general case for a common cause failure event of k components given a single unavailability is:

$$P(CCF_k|A) = \frac{P(A|CCF_k) \cdot P(CCF_k)}{P(A)} = \frac{f_k^m \cdot Q_t}{Q_t} = f_k^m \tag{5}$$

The conditional probability for multiple unavailability is given by $P(CCF_k|A_1 \cap \ldots \cap A_i)$, where $k>i$ and CCF_k contains $A_1, \ldots, A_i$. The simultaneous failure of i components that share common cause failures will be typically dominated by the common cause failure of all of them. Therefore, we can approximate the term above by $P(CCF_k|CCF_i)$. The formula is given by

$$\begin{aligned} &P(CCF_k|A_1 \cap \ldots \cap A_i) \approx P(CCF_k|CCF_i) = \\ &= \frac{P(CCF_i|CCF_k) \cdot P(CCF_k)}{P(CCF_i)} = \frac{f_k^m \cdot Q_t}{f_i^m \cdot Q_t} = \frac{f_k^m}{f_i^m} \end{aligned} \tag{6}$$

Note: if we know the cause of the deficiency, it might be overly conservative to consider the whole common cause failure event to be affected. A refined approach based on Causal Alpha Factor Model has been introduced [6, 7], where the alpha factor model partitions common cause failures by their causes. Data availability limits this approach in practice. Cause coding in the INL database is not sufficient to derive parameters for the Causal Alpha Factor Model. An alternative database ICDE [8] maintained by IAEA uses cause coding for qualitative usage, showing that common cause failures are caused to a big extent by operator/maintenance failures. In practice, the alpha factor model is used.

5. PRACTICAL TREATMENT OF UNAVAILABILITIES

As described in Section 3, PSA applications may encounter situations where the exact effect on a specific group of common cause failures must be considered. We describe some scenarios where different common cause failure treatments are appropriate. We discuss which features in software tools are important to cover these cases.

Significance Determination Process evaluates a specific scenario where an inspection finding alters the expected state of the plant. The finding can be unavailability of a piece of equipment. The evaluation relies on the information from inspectors whether this unavailability affected common cause failures or not. In case it does not, we can use the 'No CCF' approach for quantification. In case it does, the appropriate approach is the 'Conditional CCF' quantification. The evaluation is performed in hindsight. Therefore, we can assume that this information is available.

The higher risk value is integrated over time. The longer this unavailability lasts, the higher the risk becomes, which affects the categorization of this finding. This means that the timing of this

unavailability matters, too. If it is available (not only the time point of the finding, but also the time point when the component because unavailable) then we can evaluate the risk increase in a more precise way. In the best case, the 'Conditional CCF' method would also take into account the testing scheme for the components sharing the common cause failures. If a component that shares a common cause failure with the unavailable one has been successfully tested two weeks ago, we know that this common cause failure has a different probability than another one relating to a component tested two months ago.

Risk monitoring differs from the Significance Determination Process by the fact that the new risk level needs to be calculated as soon as possible after the event has been observed or reported by the plant information system. In this case, we need to rapidly estimate where the component failure happens and whether it is affecting common cause failures. Again, in case that it does not affect common cause failures, we can use the 'No CCF' quantification method, otherwise, it is the 'Conditional CCF'. The impact on calculation in the latter case might be very big, potentially prohibitive to further plant operation.

To encourage Risk Monitor users specifying 'Might affect CCF' every time when they cannot exclude a common cause failure, RiskSpectrum RiskWatcher offers a possibility to complement such a record by information about a successful test of related components. When they have been tested, a user can create a new record for this. In this case, we can exclude common cause failures and the 'No CCF' method is used. This, in turn, decreases the risk level caused by an unexpected event.

The timing aspect also plays a role in Risk Monitoring and full consideration of the testing scheme, e.g., staggered testing of symmetrical trains, would be desirable to account for all available information. This feature is not implemented in the current version of RiskSpectrum RiskWatcher and RiskSpectrum SDP. The current treatment is conservative, and it remains to be evaluated whether full timing information would contribute to significant quantitative improvements.

A simultaneous unavailability of multiple events from the same common cause failure group presents another challenge. The first question is whether these unavailabilities are caused by a common cause. In either case, are common cause failures of other related components possible or can they be excluded? Answers to both questions influence how we quantify other common cause failure events, e.g., by Equation 6 in case both answers are positive. Because such common cause failures are extremely rare, we do not offer this type of quantification in RiskSpectrum RiskWatcher or RiskSpectrum PSA.

Configuration assessment in a normal PSA model can benefit from all flexibility of the used PSA software. It is always possible to modify the original basic event probabilities or add new events to represent the analyzed configuration. This is a conceptually straightforward process, but it takes time and can therefore only be implemented for some specific configurations.

As an automatic alternative, PSA software tools typically offer calculation of the Risk Increase Factor importance measure for basic events and groups of basic events sharing some commonality. These groups of basic events can represent failure modes of a single component, a system composed of multiple components or sub-systems, events sharing a common property (an attribute), or a general event group.

The consideration of common cause failures might differ between these event groups. For a component, we might want to consider conditional quantification of common cause failures shared between symmetrical components per each failure mode. Attributes could be used to specify room information. Analyzing room events (e.g., a fire in the room) does not require treatment of common cause failures. When we evaluate the effect of unavailability of a whole system or of a group of components, we might want to set all common cause failure events as 'failed' (the 'Full CCF' treatment) to ensure that we really remove the whole system.

In order to establish a good tradeoff between the flexibility of calculations and a systematic and auditable specification, RiskSpectrum PSA allows users to select one of the pre-defined common cause failure quantification approaches, i.e., 'No CCF', 'Conditional CCF', and 'Full CCF', for each of these four categories of event groups. The same treatment will be applied to all event groups within the same category, but each category can have its own common cause failure treatment.

6. SYMMETRY IN PARAMETRIC MODELS

Equation 1 assumes that the total component unavailability Q_t is the same for all components that share common cause failures. This means that all components must have the same unavailability which is best achieved if these components are symmetrical. Their failures can be faithfully modeled by the same reliability model and by the same parameters.

There are situations where this symmetry assumption is not valid. Components might not be identical or they might be maintained or used differently. But we still want to model effects of common cause failures. In such situations, the value of Q_t in parametric models is not well-defined.

The Basic Parametric Model [1, 9] offers a solution by giving analysts a possibility to specify unavailability of common cause failure events that contain the same number of components directly.

6.1. Basic Parametric Model

Basic Parametric Model uses parameters $q_1, \dots, q_n$, where n is equal to or smaller than the number of components sharing the common cause failure. Similarly to the alpha factor model, this number influences how many simultaneous failures we can model by a common cause failure event before we create the common cause failure event representing a simultaneous failure of all involved components.

For the example fault tree in Figure 1, we need three parameters, q_1, q_2, and q_3. Since q_1 can be calculated as explained below, we need to specify only q_2 and q_3. A general formula for the Basic Parametric Model is in Equations 7 and 8. Recall that by Q_k^m we denote probability of a common cause failure event representing that k components from a common cause failure group with m components fail because of a common cause involving these k components. Equation 9 brings another degree of flexibility. With this equation replacing Equation 8, the independent failure of a component keeps the original total component unavailability.

$$Q_k^m = q_k^m, k > 1 \tag{7}$$

$$Q_1^i = Q_t^i - \sum_{k=2}^{m} \binom{m-1}{k-1} q_k^m \tag{8}$$

$$Q_1^i = Q_t^i \tag{9}$$

This is clearly a conservative treatment that does not partition the original total unavailability of the component. The sum of all common cause failure events that include this component will be greater than the original unavailability. But because it is typically common cause failure events that include a simultaneous failure of many components that dominate the results, this conservatism might be negligible.

An advantage that it brings is relaxation of another assumption in parametric common cause failure models, namely that each failure mode of a component can be included at most in one common cause failure group. For example, if we want to model dependencies between symmetrical components and

dependencies arising from a maintenance scheme that involves other components, we can use the Basic Parametric Model with Equation 9 for this purpose.

6.2. Implementation in RiskSpectrum

RiskSpectrum implements the Basic Parametric Model as a complementary common cause failure model besides the standard parametric ones from RiskSpectrum PSA 1.7.0. It offers a choice between both quantification methods for independent failure. The symmetry assumption does not apply to this model. Also, there is no theoretical constraint on including the same basic event in several common cause failure groups. However, this feature is not available in this version.

7. CONCLUSION

This paper presents different treatments of common cause failures in PSA applications, where unavailability of a component (or multiple components) is assumed. This can be motivated by an evaluation of inspection findings, events in an operating plant relevant for risk monitoring, or estimating effects of different situations leading to a risk increase. In all cases, the question of correct treatment of dependencies between components sharing common cause failures must be answered from the known context.

In this paper, we present practical implementation options for PSA application software tools that cover all important scenarios. In RiskSpectrum software suite, there are possibilities to record whether unavailability can be related to a common cause and to record that such possibility has been excluded by an additional test. Moreover, we have discussed Risk Increase Factor (Risk Achievement Worth) and proposed a flexible common cause failure treatment for different event groups. Finally, the symmetry assumption of parametric common cause failures can be relaxed in a newly implemented common cause failure model.

References

[1] A. Mosleh, D. M. Rasmuson and F. M. Marshall. "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment", NUREG/CR-5485, U.S. Nuclear Regulatory Commission, Washington, DC, (1998).

[2] U.S. Nuclear Regulatory Commission. "Basis for the Treatment of Potential Common-Cause Failure in the Significance Determination Process", NUREG-2225, Office of Nuclear Regulatory Research, Washington, DC, (2018).

[3] M. Zhang, Z. Zhang, A. Mosleh and S. Chen. "Common cause failure model updating for risk monitoring in nuclear power plants based on alpha factor model", Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(3), pp. 209-220, (2017).

[4] M. van der Borst and H. Schoonakker. "An overview of PSA importance measures", Reliability Engineering & System Safety, 72(3), pp. 241-245, (2001).

[5] D. L. Kelly and D. M. Rasmuson. "Common-Cause Failure Analysis in Event Assessment", Proceedings of the ANS PSA 2008 Topical Meeting, Knoxville, TN, American Nuclear Society, (2008).

[6] Z. Ma, J. K. Knudsen, J. A. Schroeder and C. L. Smith. "Feasibility Study of Developing Alternative Common-Cause Failure Model for Event Assessment", INL/EXT-21-33376, Idaho National Laboratory, Idaho Falls, ID, (2021).

[7] C. Hunter, C. Ng, M. Reisi Fard, Z. Ma and S. Zhang. "Research Activities Associated with the Treatment of Potential Common-Cause Failures in Event and Condition Assessments", Nuclear Technology, 209(11), pp. 1680-1687, (2023).

[8] OECD Nuclear Energy Agency. "International Common-Cause Failure Data Exchange (ICDE) Project", OECD/NEA, Paris, https://www.oecd-nea.org/jcms/pl_25090, (accessed 2026).

[9] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge and D. M. Rasmuson. "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780 (EPRI NP-5613), Vol. 2, U.S. Nuclear Regulatory Commission, Washington, DC, (1989).