Time Dependent Analysis with Common Cause Failure Events in RiskSpectrum

Pavel Krcal[a,b] and Ola Bäckström[a]
[a] Lloyd's Register Consulting, Stockholm, Sweden
[b] Uppsala University, Uppsala, Sweden

Abstract: Testing of components with common cause failures presents a challenge to a realistic analysis of failure probabilities. In reality, the most commonly used testing scheme is staggered testing. Common Cause Failure (CCF) models in Probabilistic Safety Assessment (PSA) studies often assume a sequential testing scheme. This might be overly conservative if the actual testing scheme is staggered. Some software tools, e.g., RiskSpectrum, offer time dependent analysis where one can model testing of components in time explicitly. This paper deals with effects of different testing schemes on the quantification of CCF events in time dependent analysis.

Determining which formulae shall be used by software tools in time dependent analysis requires an in-depth understanding of how to model effects of tests on the common cause parts of failures. We analyze assumptions which lie behind different ways of modeling tests of common cause failure events.

Keywords: PSA, Time Dependent Analysis, Common Cause Failures.

1. INTRODUCTION

Testing of components with common cause failures presents a challenge to a realistic analysis of failure probabilities. In reality, the most commonly used testing scheme is staggered testing. Common Cause Failure (CCF) models in Probabilistic Safety Assessment (PSA) studies often assume a sequential testing scheme. This might be overly conservative if the actual testing scheme is staggered. Some software tools, e.g., RiskSpectrum, offer a mean probability calculation and also time dependent analysis where one can model testing of components in time explicitly.

Quantification of common cause failure events depends on the chosen testing scheme, both in mean probability calculations and in a time dependent analysis. We focus mainly on the alpha model for common cause failure events in this paper. NUREG/CR-5485 [2] presents formulae for mean value quantification of common cause failure events with the alpha model under assumption of both sequential and staggered testing schemes. We discuss the following issue: How does an explicit modeling of a testing scheme in a time dependent analysis relate to the mean value estimates obtained by formulae from NUREG/CR-5485? This requires an in-depth understanding of how to model effects of tests on the common cause parts of failures.

This leads to more detailed questions about the analysis algorithm. Which formulae shall be used by software tools in a time dependent analysis? Under which assumptions are they correct? It is of great importance to understand the underlying assumptions when interpreting the numerical results in order to avoid taking an unjustified credit for top frequency decrease with staggered testing [3].

The main topic of this paper can be generalized to the following issue. The simplified models for staggering only consider staggering within one CCF group, but this is still a significant simplification since testing of important systems is often also staggered. Time dependent analyses provide a better solution, since these can also take staggering between different systems into account.

The paper is organized as follows. First, we present the background for common cause failure modeling and tested basic events. Then we formulate the main problem in Section 3. Section 4 shows the relation between time dependent analysis and mean value calculations. Section 5 discusses assumptions on which both methods are based. Finally, we conclude the paper.

2. BACKGROUND

The classical approach in PSAs assumes that basic failures modeled by basic events are independent of each other. Dependent failures are then either modeled explicitly by adding the root cause into the model as a new basic event or by defining so called common cause failures. Since its introduction in the sixties, common cause failure analysis became an integral part of PSA studies, with a mature methodology described in many standards and procedures [1,2,5].

2.1 Parametric models

Common cause failures are defined by parametric models. This means that we identify groups of basic events that might fail together as a result of a common cause. Then we choose a model and assign values to model parameters. The model together with the parameter values already define how to complete the fault tree model by so-called common cause failure events, and also defines how to quantify them. Fault tree analysis results will then reflect the contribution of common cause failures to the top failure. In fact, common cause failures often significantly contribute to core damage frequency.

Basic events included in the same common cause failure group have to be identical. In this paper, we assume that they have the same reliability model with the same reliability parameters.

Parametric models for common cause failure modeling divide into shock and non-shock models. Shock models assume that common cause failures result from the impact of an external shock which occurs with a given frequency. Non-shock models do not have any such assumption and directly determine probabilities of common cause failure events.

The most commonly used non-shock parametric models include the Beta Factor, the Alpha Factor, and the Multiple Greek Letters (MGL) model. The Beta Factor model is the simplest one, distinguishing only between independent failures and a common failure of all basic events from the common cause failure group. This model requires only one parameter value. The Alpha Factor and MGL models offer an extension of this model to all combinations of common cause failures. An advantage of the Alpha Factor model over the MGL model is that its parameters can be directly estimated from the failure data obtained from tests. This paper focuses on the Alpha Factor model, since it is recommended in, e.g., [2,5], and since other models can be transformed to it.

2.2 Alpha Factor model

The Alpha Factor model [7] for a group of *m* basic events is determined by *m* parameters denoted by $\boldsymbol{\alpha_1}$, $\boldsymbol{\alpha_2}$, …, $\boldsymbol{\alpha_m}$. Each parameter $\boldsymbol{\alpha_k}$ is the fraction of failures that occur together in groups of *k* components in total failures. In other words, it is a "probability that when a common cause basic event occurs in a common cause group of size *m*, it involves failure of *k* components" [2]. Let us by $\boldsymbol{Q_k^m}$ 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. Since components in a common cause failure group are assumed to be equivalent, this probability is well-defined. Now we can define $\boldsymbol{\alpha_k}$ formally by

$$\boldsymbol{\alpha_k = \frac{\binom{m}{k} Q_k^m}{\sum_{k=1}^{m} \binom{m}{k} Q_k^m}} \tag{1}$$

We assume that the common cause failure events are mutually exclusive to each other (i.e., a common cause failure of components A and B models a situation where A and B fail together and components

C and D from the same common cause failure group function correctly) and that they add up together with independent failures to the original failure probabilities of the basic events included in the common cause failure group. Formally,

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^m \tag{2}$$

Quantification of common cause failure events based on the alpha parameters and the independent basic event probability is derived from the two basic equations above. The probability of Q_k^m is determined by

$$Q_k^m = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \tag{3}$$

where

$$\alpha_t = \sum_{k=1}^{m} k\alpha_k \tag{4}$$

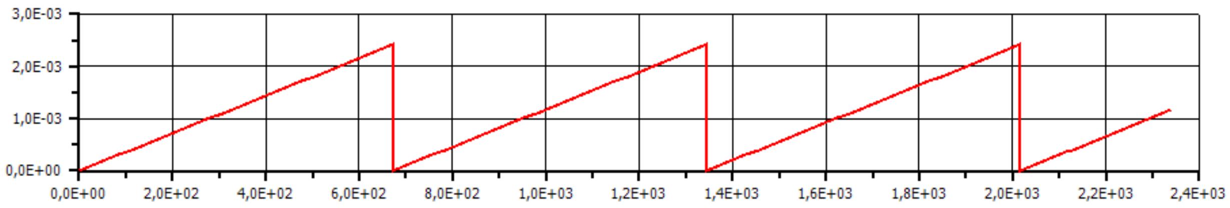
Complete derivation is described in, e.g., [2], Appendix A.

So far, we did not consider any time dependent behavior of basic events. Equation 3 above is valid for mean value calculations. Now, let us consider basic events representing stand-by components which are periodically tested. Such basic events are defined in [4] by the following reliability model. This model assumes an exponential distribution for the failure process (constant failure rate λ), a constant fixed test interval (*TI*) with optional different time to first test (*TF*). To simplify the understanding of this model, we will first present it with only the failure rate and test interval parameters. The unavailability in this case is given by:

$$Q(t) = 1 - e^{-\lambda(t-T_i)} \qquad T_i = 0, TI, 2TI, \dots \tag{5}$$

This model results in the classical saw-tooth curve for the unavailability (Figure 1). If a *TF* (time to first test) parameter is given, the model is identical except that the time points for the tests are "offset" by the value *TF*, i.e. the test time points are $T_i = 0, TF, TF + TI, TF + 2TI, \dots$

Figure 1. Graph of the unavailability over time of a tested basic event.



The mean unavailability Q_{mean} is obtained by integrating the unavailability *Q(t)* over a complete test cycle:

$$Q_{mean} = \frac{1}{TI} \int_0^{TI} Q(t)dt = 1 - \frac{1}{\lambda TI}\left(1 - e^{-\lambda TI}\right) \tag{6}$$

We assume that a repair occurs directly after a test if the component is failed at the test. The unavailability of the component immediately before a test, *Q(TI),* is, in other words, the probability that a repair is needed after the test.

Clearly, testing influences the mean failure probability of such basic events. If these basic events form a common cause failure group then they are implicitly divided into several other basic events modeling common cause failures. Testing of such events is determined by testing of all components which are included in this common cause failure. As long as all components are tested synchronously at the same time points, this does not alter assumptions for the mean value formula above. When we test components at different time points then, from the logic of common cause failure modeling, each successful test also demonstrates that there is no common cause failure involving the tested component. This means that testing one component affects other components.

Testing components from one common cause failure group at different time points evenly spread over the testing calendar is called *staggered testing*. The test procedure works as follows. If a tested component functions normally then we wait until the next test time point where another component is tested. If a failure is observed during a test of one component then all other components from the same common cause failure group are tested as well. All malfunctioning components are repaired.

Our aim is to describe different ways of taking staggered testing into account both in mean value and time dependent analysis.

3. PROBLEM STATEMENT

We present a formula from [2] for the Alpha Factor model that takes staggered testing into account. Then we introduce a way to perform time dependent analysis. Finally, we state the problem as establishing a relation between the two approaches.

3.1. Mean Value Calculation with Staggered Testing

Equation 3 does not explicitly depend on a testing scheme, because we did not need to make any assumptions about it in Equations 1 and 2. However, values of alpha parameters and the total basic event probability might depend on the actual testing scheme. [2] presents a formula for the Alpha Factor model with staggered testing:

$$\boldsymbol{Q_k^m = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t} \tag{7}$$

To obtain this, we have to use the relation between estimators for Q_k^m in both schemes. We have that

$$\boldsymbol{Q_k^{m\,[NS]} = k \cdot Q_k^{m\,[S]}} \tag{8}$$

and if we replace the values from non-staggered testing by the right hand side in the Equation 1 and leave Equation 2 then we obtain Formula 7. Since this derivation is not a part of [2], we show it here. Recall a simple relation between binomial coefficients.

$$\boldsymbol{\binom{m}{k} = \frac{m}{k}\binom{m-1}{k-1}} \tag{9}$$

Applying Equation 8 on Equation 1 together with Equation 9 gives us

$$\boldsymbol{\alpha_k = \frac{\binom{m}{k} k Q_k^m}{\sum_{k=1}^m \binom{m}{k} k Q_k^m} = \frac{\binom{m-1}{k-1} m Q_k^m}{\sum_{k=1}^m \binom{m-1}{k-1} m Q_k^m} = \frac{\binom{m-1}{k-1} Q_k^m}{\sum_{k=1}^m \binom{m-1}{k-1} Q_k^m}} \tag{10}$$

Now we can substitute the denominator according to Equation 2.

$$\alpha_k = \frac{\binom{m-1}{k-1} Q_k^m}{Q_t} \tag{11}$$

From here we obtain Formula 7.

3.2. Time dependent Analysis

Time dependent analysis in RiskSpectrum is based on an assumption that alpha factors are the same over time. Component failure probabilities are established according to Formula 5 and it is always the latest tested component that determines probabilities of common cause failure events containing this component.

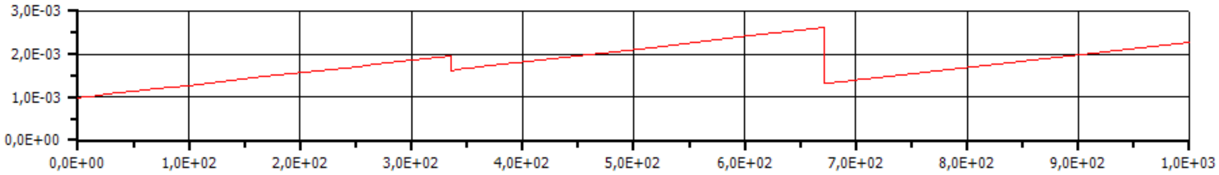
Common cause failure modeling works in the following way. We split the original event(s) into several new ones. Each new event:

- Represents failure of one or more events from the common cause failure group.
- Contains reliability parameters from the original event.
- Has its failure probability (unavailability) at a given time multiplied by a factor obtained from alpha parameters depending on its multiplicity according to Formula 3.

After this, each new event represents a clearly defined physical event (e.g., components A and B fail simultaneously because of a common cause failure) and behaves as an independent event. Its failure probability at a given time is independent of the probability of other common cause failure events at this time point. It is determined only by its parameters, alpha parameters, and the time point, which in turn determines the time point of the last test. An event representing a simultaneous failure of several components is tested each time one of these components is tested. If this tested component works then it means that the simultaneous failure of these components has not happened and therefore its probability is equal to zero.

The mean value of top event unavailability is obtained by calculating unavailability at different time points (Figure 2), integrating it over time numerically and dividing it by the interval length.

Figure 2. A graph of unavailability over time for an example emergency feed water system.



3.3. Final Problem Statement

We shall deal with the following questions in the rest of the paper:

- Which assumptions lie behind the time dependent analysis in RiskSpectrum?
- How does this time dependent analysis relate to the staggered mean value formula from NUREG/CR-5485?
- What are the advantages and disadvantages of either approach?

4. RELATING TIME DEPENDENT ANALYSIS AND MEAN VALUE FORMULAE

Recall that failure probability of a common cause failure event at a given time is determined only by its parameters, alpha parameters, and the last time point when a component included in this event was tested. We call this a *perfect testing assumption*. Each test excludes the possibility of all common cause failure events including the tested component, leaving other common cause failure event probabilities unaffected.

One consequence of this is that probabilities of common cause failure events at a random time point might not satisfy Equation 2 for $\boldsymbol{Q_t}$. First, values $\boldsymbol{Q_k^m}$ are not well-defined anymore. They can be different for different common cause failure events with the same multiplicity. Secondly, if we, at a specific time point, sum up values of all common cause events including failure of the original component then we might get a value smaller than the original value $\boldsymbol{Q_t}$. For example, in a group with two components A and B, if we test B at a time point *t* then the total failure probability of A decreases, because the probability of a common cause failure of A and B is set to zero.

The mean probability value of a common cause failure event in time dependent analysis with staggered testing might be up to k times, where k is the event's multiplicity, smaller than its mean value with non-staggered testing. There are two reasons why it is not always *k* times smaller:

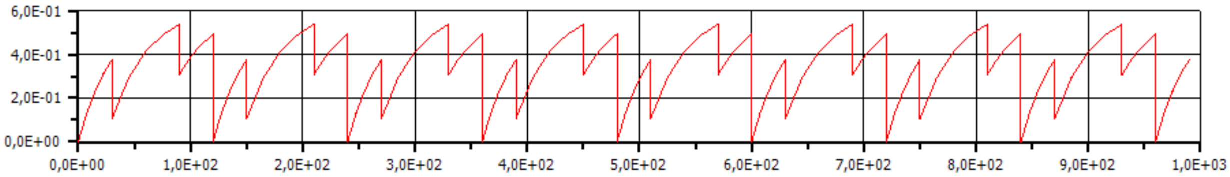
- Tests of this common cause failure might not be evenly distributed over the test interval.
- For larger lambda values, the probability function over time deviates significantly from a linear function. See Figure 3 for an example of both phenomena.

Since the mean value formula does not take exact test time points into account, and the effects of the two items above are small if we have small lambda values, we can say that this decrease of mean probability for common cause failure events corresponds to dividing the mean value by *k*. This decreases the mean total probability of the component failure (modeled by the original basic event) by a factor of α_t. If we denote the mean failure probability of the component in question under assumption of staggered testing by $Q_t^{[S]}$ and under assumption of non-staggered testing by $Q_t^{[NS]}$ then we have that

$$\boldsymbol{Q_t^{[S]} = Q_t^{[NS]}/\alpha_t} \tag{12}$$

All these considerations assume that we use Formula 3 (non-staggered testing) to calculate probabilities in the time dependent analysis. On the other hand, using $Q_t^{[S]}$ or Formula 7 (staggered testing) for the time dependent analysis, i.e., to obtain event probabilities at a certain time point, would be applying staggered testing on data obtained from staggered testing and it would result in an unjustified decrease of failure probability.

Figure 3. Uneven staggered testing of components with failure rate equal to 0.02



5. DISCUSSION

In this section we discuss advantages and problems with time dependent analysis of the background of Formula 7.

5.1 Perfect Testing Assumption

Time dependent analysis in RiskSpectrum works under the *perfect testing assumption*. As a result, the component failure probability obtained from the time dependent analysis is somewhat lower than the original one. For realistic alpha parameters where α_1 (the independent failure) dominates the other parameters, the difference rather small. See Table 1 for some examples of alpha parameters taken from [6].

Table 1: Decrease of Component Failure Probability in Time dependent Analysis with Staggered Testing

α_1	α_2	α_3	α_4	Decrease (%)
0.9771	1.38E-2	8.09E-3	5.59E-3	4.9
0.9766	1.49E-2	6.81E-3	1.67E-3	3.3
0.9636	1.34E-2	1.11E-2	1.13E-2	6.5
0.9612	2.42E-2	1.07E-2	3.89E-3	5.5
0.8395	8.33E-2	2.68E-2	4.75E-2	21.7

Time dependent analysis offers multiple advantages over mean value calculations. It gives complete flexibility for modeling of staggered testing. We can model different testing schemes, e.g., a two-train system with two redundant components in each train where testing of trains is staggered. We test both redundant components in a train in one test episode and the other two redundant components from the second train in the next test episode. Here, using the Formula 7 for a CCF group of size four might lead to underestimating the actual failure probabilities.

The mean probability model for staggering only considers staggering within one CCF group, but this is still a significant simplification since testing of important systems is often also staggered. Time dependent analyses provide a better solution, since these can also take staggering between different systems into account. Therefore, time dependent analysis can serve as a verification tool for designing a test scheme. Additionally, it makes time dependent analysis a natural method for on-line risk monitors.

Finally, can we use some of the equations above to obtain the same result also in mean value calculations? Formula 7 is derived from the unmodified Equation 2 which states that all common cause failure probabilities sum up to the original component failure probability. To reconcile this with the perfect testing assumption, we have to replace the original component probability by the staggered one from Equation 12. This means that we consciously distinguish between mean failure probability of a component with non-staggered and with staggered testing and we accept that this probability is lower under staggered testing. Formula 7 then gives us the same mean probability values for common cause failure events as the time dependent analysis (this follows directly from a comparison between Formula 3 and Formula 7 after application of Equation 12).

5.2 Failure Probability Preservation Assumption

In spite of the arguments above, one might argue that the perfect testing assumption is giving us an unreasonable risk decrease bonus. By a successful test of a component A, we can exclude the possibility that components A and B from the same common cause failure group fail together. If we were now in the position to partition the total failure probability for the whole component, maybe we would simply assign a bit more to other common cause failure events instead of the currently excluded event AB. By this, we would preserve the original total probability also under the staggered testing scheme. The effect of this testing scheme would be a different probability partitioning in favor of common cause failure events with lower multiplicities. This corresponds to a modification of the alpha parameters.

This is a conservative way of accounting for staggered testing. It is skeptical to our knowledge about common cause failures and does not want to take the full credit for testing of common cause failure events. Probability of a common cause failure event modeling a dependent failure of k components with staggered testing will be higher than the probability of the same event with non-staggered testing divided by *k*. This approach might still lead to a decrease of the top event probability/frequency, because it decreases failure probability of common cause failure events with higher multiplicities. These events are usually greater contributors to the top event probability/frequency than the independent component failures.

A disadvantage of the failure probability preservation assumption is that it is not clear how to perform the time dependent analysis leading to the same quantitative results.

6. CONCLUSIONS

We have discussed advantages and disadvantages of time dependent analysis of a system with common cause failures in comparison to mean value calculation according to formulae from NUREG/CR-5485. The main advantage of the time dependent analysis is the great flexibility which it offers for modeling of staggered testing, not only between components from one common cause failure group, but also between different common cause failure groups and whole systems. We have formulated two assumptions for staggered testing which lie behind either the time dependent analysis or the mean value calculation. We leave it for further discussion under which circumstances these assumptions are reasonable.

References

[1] A. Mosleh et al., “*Procedures for Treating Common Cause Failure in Safety and Reliability Studies*”, NUREG/CR-4780, 1988.

[2] A. Mosleh et al., “*Procedures and Guidelines in Modeling Common Cause Failures in Probabilistic Risk Assessment*”, NUREG/CR-5485, 1998.

[3] J. E. Stott et al., “*Common Cause Failure Modeling: Aerospace vs. Nuclear*”, In Proc. of PSAM10, Seattle, 2010.

[4] RiskSpectrum Analysis Tools Theory Manual, Lloyd's Register Consulting, 2012.

[5] International Atomic Energy Agency, “*Procedures for conducting common cause failure analysis in probabilistic safety assessment*”, IAEA-TECDOC-648, 1992.

[6] F. M. Marshall et al., “*Common-Cause Failure Parameter Estimations*”,NUREG/CR-5497, 1998

[7] A. Mosleh and N Siu, , “*A Multi-Parameter Common Cause Failure Model*”, In proc. of the 9th International Conference on Structural Mechanics in Reactor Technology, Lausanne, 1987.