On the Calculation of Unit Trip Frequency

James C. Lin
ABSG Consulting Inc., Irvine, USA

Abstract: The development of the fault tree models for evaluating unit trip frequency is similar to the fault trees constructed for the calculation of the support system failure frequencies. Since these models need to accommodate the different failure sequences with different initial failures of the normally operating equipment, the fault trees can be very complicated if constructed manually. A calculation approach has been developed to derive the system failure frequency directly from the minimum cutsets generated from the fault tree models developed for calculating the system failure probability. Each of these minimum cutsets may be further defined into more than one failure sequence, with each failure sequence involving an initial failure of a normally operating component and a number of subsequent failures. The initial failure is characterized by an annual failure frequency. The probability of each of the subsequent failures in the same failure sequence can be evaluated using a failure exposure time equal to the time for repair/restoration of the component involved in the initial failure. The system fails when the required subsequent failures occur before the component involved in the initial failure is restored and returned to service. This calculation process can also be implemented in the traditional probabilistic risk assessment (PRA) software to permit the direct calculation of the support system failure frequencies as part of the integrated fault tree model since all of the support components are already linked directly to the equipment supported.

Keywords: Trip Frequency, Support System Failure Initiating Event Frequency, Fault Tree Model, PRA, Minimum Cutsets.

1. INTRODUCTION

The computerized, online trip monitor is a computer tool that quantifies the trip monitor model to calculate the unit trip frequency based on the actual configuration of the plant at the time of the evaluation; i.e., selected pieces of equipment may be unavailable due to failures or maintenance. The trip monitor model includes combinations of equipment failures and unavailability, organized in fault trees, which can lead to a nuclear plant trip. Similar to the risk monitor, the risk metric used for the trip monitor is the frequency of unit trips. The software platform of an online trip monitor includes user interfaces that are user-friendly to facilitate the specification/input of the actual plant configuration. This is a tool that can be used to avoid unintentional entry into high trip-risk configurations resulting from planned maintenance activities.

The U.S. nuclear power industry started the development of the trip monitor methodology back in the late 1990s and early 2000s [1, 2, 3, 4]. However, due to the insufficient drivers, the development and implementation of the trip monitor in the U.S. did not progress very far at that time. The methodology used to calculate the trip frequency is the same as the calculation of the loss of support system initiating event frequencies, which nowadays are typically evaluated using fault tree models. The fault tree method can be used conveniently to model the failure probability of mitigation functions/systems. To model the frequency of failures of systems/functions, the fault tree model developed for these systems/functions must be expanded to account for the order in which the failures occur because the frequency is evaluated as the product of the frequency of the initial failure and the probability of the subsequent failures.

EPRI Report 1016741 “Support System Initiating Events Identification and Quantification Guide” [5] discusses the major concepts and issues applicable to using fault tree modeling techniques for the development of initiating event frequencies for loss of a support system. However, no explicit and rigorous approach was ever proposed for the automated evaluation of the fault tree model developed for the system failure probability to derive the system failure frequency. As such, to this date, with the exception of the RISKMAN™ PRA models, the frequency of support system failure initiating events modeled using the fault tree approach has been developed manually by explicitly enumerating all of the combinations of failure sequences.

In this paper, an approach that can be used for the computerized evaluation of the unit trip frequency and the system failure frequency (for the modeling of the frequencies of the support system failure initiating events) using the fault trees developed for the system failure probability is discussed. The rigorous method and the approximation options for evaluating the unit trip frequency are described. In addition, the techniques used to address the effects of support equipment failures will also be explained.

2. EVALUATION OF SYSTEM FAILURE FREQUENCY BASED ON FAULT TREE MODEL FOR SYSTEM FAILURE PROBABILITY

2.1. Conceptual Approach

First, we will use the simplest case to explain how the frequency of failure of a normally running system, which may include one or more normally running trains is addressed for both the unit trip frequency and support system failure frequency. As described previously, fault tree logic can be manually developed to correctly model and quantify the frequencies of all of the failure sequences leading to the system failure. However, this fault tree development process is time-consuming and error prone. The ideal approach is to automate the process for calculating the system failure frequency using the fault tree developed for evaluating the system failure probability, which is concise and easy to develop.

For a two-train, redundant system with a normally running train and a normally standby train, the system fails if the normally running train fails first/initially and the normally standby train also fails subsequently before the initially failed train is restored and returned to service. As such, the system failure sequence is simply the failure of the normally running train followed by the failure of the standby train during the time when the initially failed trained is being restored. The system failure frequency is thus the product of the frequency of failure of the normally running train and the probability of failure of the standby train during the restoration time for the initially failed train. The frequency of failure of the normally running train is in terms of the number of failure per unit time; e.g., per year. The probability of failure of the standby train may involve the sum of the probability of failure of the standby train to start on demand and the probability of failure of the standby train during the time of restoration of the initially failed train. Note that the restoration time for the initially failed component should not exceed the limiting condition for operation allowed outage time (AOT). This failure sequence can be expressed mathematically as follows:

$$\text{f(system failure)} = \lambda_R * [P_{SS} + (1 - e^{-\lambda_S \tau_R})] \qquad (1)$$

where λ_R = failure rate of the normally running train (failures/year)
P_{SS} = start failure probability of the standby train
λ_S = failure rate of the normally standby train (failures/hour)
τ_R = restoration time for the initially failed (< AOT), normally running train

In contrast, for a mission time failure probability model used in a typical PRA, the main difference is that failures of both the normally running train and the normally standby train are evaluated for their probabilities of failure during the mission time of, for example, 24 hours. For the system failure frequency calculation, the failure probability during the 24-hour mission time for the normally running train needs to be changed to a yearly failure rate. In addition, the failure exposure time for the normally standby train needs to be revised from a 24-hour mission time to the restoration time for the initially failed train, which in most cases is different from 24 hours.

Therefore, based on the preceding, the simple algorithms that can be used in evaluating the system failure frequency using the fault tree model developed for the system failure probability for a failure combination involving a failure of a normally running component and a failure of a normally standby component include:

- For the initial failure in the failure combination, change the calculation of the basic event for a failure mode associated with a failure during operation from probability of failure during the mission time (or failure exposure time) to a yearly failure rate using a unit conversion factor.

- For the subsequent failure in the failure combination, change the failure exposure time from 24-hour mission time to the restoration time for the initial failure.

For a redundant system with two normally running trains (e.g., A and B), there are two different failure sequences because either train can be the initially failed train. In comparison, the fault tree model developed for the system failure probability involves only one failure combination in the lumped parameter PRA model, which is failure of Train A during the mission time in conjunction with failure of Train B during the same mission time; i.e., a failure combination (or cutset) with two failure-during-operation events. Since either one of these two failure-during-operation events can be the initial failure, the two failure sequences are (1) failure of running Train A followed by failure of running Train B during the period of restoration for the failed Train A, and (2) failure of running Train B followed by failure of running Train A during the period of restoration for Train B. The system failure frequency for this redundant system with two normally running trains can be expressed mathematically as:

$$\text{f(system failure)} = \lambda_A * (1 - e^{-\lambda_B \tau_A}) + \lambda_B * (1 - e^{-\lambda_A \tau_B}) \qquad (2)$$

where λ_A and λ_B are the failure rates for the normally running Train A and Train B, respectively
τ_A and τ_B are the restoration time for the initially failed Train A and Train B, respectively

Thus, the general algorithm that should be used in evaluating the failure frequency using the failure probability model for this failure combination is:

- Select one of the running failure events as the initial failure event and change its basic event value from a probability based on a failure exposure time to a yearly failure rate. Change the failure exposure time for the remaining (i.e., the subsequent) running failure event to the restoration time for the component involved in the initially failed event.

- Select the other running failure event as the initially failed event and make similar calculation changes.

The above approach can be implemented using the minimum cutsets generated from the fault tree model developed for the system failure probability. In each cutset, the events involving failure during operation for normally running components can be identified and selected as the initial failure event, one at a time. The remaining events in the same cutsets will assume the restoration time of the initially failed component as their failure exposure time. In this manner, each cutset with "n" failure-during-operation events for normally running components will be split into "n" failure sequences, each with an initial failure event and the subsequent failure events. Assigning the restoration time associated with the initially failed component as the failure exposure time for all of the subsequent failure events is in some cases an approximation which will be discussed in more detailed later.

2.2. Computer Implementation

Now, we will discuss the approach that can be used to calculate the system failure frequency from the minimum cutsets derived from the fault tree model developed for the system failure probability. In principle, each basic event (corresponding to a failure mode for a piece of equipment) has a failure rate and a repair/restoration time. The repair/restoration time is typically not included in the fault tree model for a PRA and it needs to be entered into the software database for the calculation of the system failure frequency. In addition, it should be specified whether the basic event can be the first/initial failure or not; i.e., whether it is a normally running component. The specific failure exposure time used for the quantification of the value for each basic event in the subsequent failures will be dependent on the initial failure in that failure sequence/subscenario (note that each cutset may have a number of failure sequences/subscenarios depending on which basic event occurs first); i.e., the restoration time for the component involved in the initial failure.

For example, Cutset ABCD involves failures of Components A and B which both are normally running (and as such both can be the first/initial failure, but one at a time). C is a standby failure mode for a support component and D is a normally running support component. This cutset involves the following failure sequences/subscenarios:

1. A(first/initial failure) * B(failure during restoration time for A) * C(standby demand failure) * D(failure during restoration time for A)

2. B(first/initial failure) * A(failure during restoration time for B) * C(standby demand failure) * D(failure during restoration time for B)

3. D(first/initial failure) * A(failure during restoration time for D) * B(failure during restoration time for D) * C(standby demand failure)

So, each basic event only needs to have the following information in the database for quantification (a) whether it can be the first/initial failure because it is a normally running component, (b) its failure rate, and (c) its failure restoration time. Therefore, the quantification software database needs to store the above information for each basic event.

The basic event for the first/initial failure is calculated as (failure rate per hour; i.e., λ)*8766. The basic event involving failure during the restoration time of the initially failed component is calculated as (failure rate per hour; i.e., λ)*(restoration time for the initially failed component), or it can be calculated more accurately using the formula 1-EXP(-λt). Standby demand failure is simply evaluated by the demand failure probability. The frequency of the above failure sequences is expressed as:

$$\text{f(system)} = \begin{array}{l} \lambda_A * (1 - e^{-\lambda_B \tau_A}) * P_{d,C} * (1 - e^{-\lambda_D \tau_A}) + \\ \lambda_B * (1 - e^{-\lambda_A \tau_B}) * P_{d,C} * (1 - e^{-\lambda_D \tau_B}) + \\ \lambda_D * (1 - e^{-\lambda_A \tau_D}) * P_{d,C} * (1 - e^{-\lambda_B \tau_D}) \end{array} \tag{3}$$

where λ_A, λ_B, and λ_D are the failure rates for A, B, and D, respectively
τ_A, τ_B, and τ_D are the restoration times for A, B, and D, respectively
$P_{d,C}$ is the demand failure probability of C

The specific failure exposure time used in the calculation of the value for each basic event associated with the subsequent failures in each cutset is determined by the first/initial failure in the cutset failure sequence/subscenario. During the quantification, the software should (1) generate the cutset, one at a time, (2) determine the failure sequences/subscenarios associated with each cutset, (3) calculate the frequency for each failure sequence/subscenario based on the product of the initial failure frequency and the basic event values associated with the subsequent failures determined from the failure exposure time equal to the restoration time for the initial failure in that failure sequence/subscenario, (4) sum up the frequencies for all of the failure sequences/subscenario for that cutset, and (5) based on the sum of the failure sequences/subscenarios for that cutset, determine if that cutset should be screened out.

After all the cutsets have been generated, evaluated, and calculated for the total frequencies of their failure sequences/subscenarios, the frequencies for the cutsets that are not screened out are summed up to obtain the final frequency value for the group of cutsets generated from the top event of interest.

The frequency of system failure can thus be expressed as:

$$\text{f(system failure)} = \sum_{i=1}^{I} f(MCS_i) =$$

$$\sum_{i=1}^{I} \sum_{j=1,i}^{J,i} \lambda_{i,j} \Big(\prod_{k=1,k\neq j,i}^{J,i} (1-e^{-\lambda_{i,k}\tau_{i,j}}) \prod_{l=1,i}^{L,i} (1-e^{-\lambda_{i,l}\tau_{i,j}}) \prod_{m=1,i}^{M,i} P_{i,m} \Big) \qquad (4)$$

Where MCS_i = the ith minimum cutset
I = total number of minimum cutsets not screened out
j = the jth normally operating component that fails initially in the ith cutset
J = the total number of normally operating components in the ith cutset
k = the kth normally operating component that fails subsequently in the ith cutset
l = the lth standby component that fails during operation in the ith cutset
L = the total number of standby component that fail during operation in the ith cutset
m = the mth demand failure probability in the ith cutset
M = the total num be of demand failure probabilities in the ith cutset
λ = component failure rate
τ = restoration time for failed component
P = demand failure probability

As such, the process is very simple. The key is that the software must be able to implement this calculation process using the cutsets generated from the fault tree models developed for the system failure probability.

3. GENERALIZATION FOR SYSTEM FAILURE WITH MORE THAN TWO NORMALLY RUNNING COMPONENTS

When a system failure involves the joint loss of more than two normally running components (A, B, and C), the failure exposure time for the subsequent failures in each cutset is not always identical to the restoration time for the initially failed component (τ_1). For example, in a system with three redundant, normally running components, the failure exposure time for the second failure is the restoration time for the first/initial failure; i.e., τ_1. However, the failure exposure time for the third failure should be determined by the earlier timing of restoration of either the first failure or the second failure; i.e., the shorter of the restoration time for the first failure (τ_1) and the sum of the time between the first failure and the second failure (t) and the restoration time for the second failure (τ_2). In other words, the failure exposure time for the third failure should be Minimum(τ_1, t+τ_2).

Assuming that the three normally running, redundant components are A, B, and C, the failure frequency of this failure combination with three running failures can be mathematically expressed as follows based on the possible failure sequences:

$$\begin{aligned}\text{f(system failure)} = {} & \lambda_A * \{\int_0^{\tau_A} \lambda_B [\int_t^{Min(\tau_A, t+\tau_B)} e^{-\lambda_C t} \lambda_C dt']dt + \int_0^{\tau_A} \lambda_C [\int_t^{Min(\tau_A, t+\tau_C)} e^{-\lambda_B t} \lambda_B dt']dt\} + \\ & \lambda_B * \{\int_0^{\tau_B} \lambda_A [\int_t^{Min(\tau_B, t+\tau_A)} e^{-\lambda_C t} \lambda_C dt']dt + \int_0^{\tau_B} \lambda_C [\int_t^{Min(\tau_B, t+\tau_C)} e^{-\lambda_A t} \lambda_A dt']dt\} + \\ & \lambda_C * \{\int_0^{\tau_C} \lambda_B [\int_t^{Min(\tau_C, t+\tau_B)} e^{-\lambda_A t} \lambda_A dt']dt + \int_0^{\tau_C} \lambda_A [\int_t^{Min(\tau_C, t+\tau_A)} e^{-\lambda_B t} \lambda_B dt']dt\} \quad (5)\end{aligned}$$

Where λ_A, λ_B, and λ_C are the failure rates for A, B, and C, respectively
τ_A, τ_B, and τ_C are the restoration times for A, B, and C, respectively

In the first line of the equation, there are two failure sequences. The first failure sequence involves A as the first failure, B as the second failure, and C as the third failure. The second failure sequence involves A, C, and B as the first, second, and third failures, respectively. The second line of Equation (5) includes Failure Sequence B, A and C as well as Failure Sequence B, C, and A. Similarly, the third line of Equation (5) involves Failure Sequence C, B, and A as well as Failure Sequence C, A, and B.

It should be noted that, in the Equation (5) calculation of the probability of failure during the time the preceding failure is being restored, only the failure rate λ is used as the integrand to simplify the mathematics, as opposed to be using the rigorous expression of failure density $\lambda e^{-\lambda t}$ for the exponential failure model.

As can be seen from Equation (5) above, the mathematic expression used to rigorously evaluate the system failure frequency of three redundant, normally running components using the accurate failure exposure time is quite complex. Therefore, although conservative, using the same failure exposure time (i.e., the restoration time for the first failure) for the second failure and the third failure is considered a reasonable approximation of Equation (5), as shown in the following:

$$\text{f(system)} = \begin{aligned} & \lambda_A * (1 - e^{-\lambda_B \tau_A}) * (1 - e^{-\lambda_C \tau_A}) + \lambda_B * (1 - e^{-\lambda_A \tau_B}) * (1 - e^{-\lambda_C \tau_B}) + \\ & \lambda_C * (1 - e^{-\lambda_A \tau_C}) * (1 - e^{-\lambda_B \tau_C}) \end{aligned} \quad (6)$$

In fact, it is extremely rare that a system is configured with three redundant trains running during normal operation when only one is required for success. In great majority of the designs, the number of normally running trains is at most one more than the required number of trains for success. As such, a system failure in these designs could only involve failures of two normally running trains, not three. Furthermore, the results of a unit trip frequency model is typically dominated by single failures and at most some additional, double failures. Therefore, the failure combinations involving three normally running trains or components should only have insignificant contribution, even if they exist.

4. FAILURE OF NORMALLY OPERATING SUPPORT COMPONENTS

In most of the past fault tree models developed manually in PRAs to calculate the support system failure initiating event frequencies, the systems/components providing the support functions (e.g., electrical bus) to the systems being evaluated (e.g., component cooling water system) are not explicitly modelled in detail. This is mainly because, if support components for the support systems are also modelled rigorously, the fault tree models for these support system failure initiating event frequencies will become much more complicated due to the large number of additional failure combinations (involving failures of support components in conjunction with failures of the components in the support systems being evaluated), to the extent it may not be easily managed with the manual fault tree development process.

If we want to calculate the unit trip frequency more accurately, however, the failure combinations involving failures of the support components in conjunction with failures of the components in the systems being evaluated may also need to be accounted for. Fortunately, using an automated process of evaluating the minimum cutsets generated from the fault tree models developed for the system failure probability, the impacts of the support component failures are already included in the fault tree models and can be evaluated in the same manner as any other minimum cutsets derived from the fault tree model developed for the system being studied.

It must be noted that the normally operating support components may provide support to a normally running component and to a normally standby component. For the case of a normally operating support component (e.g., an electrical bus) providing support to a normally running component (e.g., a normally running pump), failure of this normally operating support component can certainly be considered as the initial failure in a minimum cutset generated from the fault tree model developed for the system failure probability. For the case of a normally operating support component (e.g., an electrical bus) providing support to a normally standby component (e.g., a normally standby pump), can the failure of this normally operating support component also be considered as the initial failure in the calculation of the system failure frequency (especially because failure of this normally operating support component only impacts the standby pump which does not immediately affect the status of the normally running system)? The answer is yes. In this case, even though failure of the normally operating support component for a normally standby pump will not manifest its impact immediately while the normally running pump is still working, its failure impact can still contribute to the failure combination leading to the loss of the system as soon as the normally running pump fails.

As such, the normally operating support components for the system being analyzed can be treated just like any other normally running equipment. In the process of automated evaluation of the cutsets generated from the fault tree models for the system failure probability, failure of the normally operating support component should be considered as one of the initial failures in identifying the failure sequences regardless whether they provide support to a normally running component in the system being evaluated or they support a normally standby component.

5. COMMON CAUSE FAILURES

The treatment of the common cause failures (CCF) is similar to that for the independent failures. For demand failure modes, the common cause failure terms are only included in the subsequent failure events. For running failure modes, the common cause failure terms can also serve as the initial failure event, the frequency of which is determined by converting the hourly common cause failure rate (which may include the product of the independent failure rate and such CCF parameters as β, γ, and δ) to an annual rate. When the CCF terms are modelled as subsequent failure events, the failure exposure time for these CCF events can also be approximated by the restoration time for the component involved in the initial failure.

6. EXISTING PRA SOFTWARE

Currently, neither CAFTA nor RiskSpectrum includes any software features that can quantify the system failure frequency directly using the fault tree model developed for the system failure probability, which is much more compact and easier to develop than the fault tree model for the frequency of system failure.

However, the CAFTA software does have a CSRAM Rate/Lamba option which can be used to post-process the fault tree cutsets offline for the calculation of system failure frequency. However, it cannot be used in the quantification of the integrated model to provide the system failure frequency values since it is not in a format that can be directly linked in the integrated model.

In the RiskSpectrum software, the calculation of the frequency for non-repairable components (Type 6 Basic Events) can be used to calculate the failure frequency of normally running equipment. However, the frequency of the initial failure is calculated using the hazard intensity value; i.e., not the straight hazard frequency which should be used for the evaluation of the initiating event frequency. Also, the probability of the subsequent failures is not evaluated using the equipment restoration time, as it should be. Instead, the same mission time is used for all subsequent equipment failures.

The only PRA software that has the capability to calculate, in an integrated manner, the system failure frequency directly from the fault tree developed for the system failure probability is RISKMAN. Nevertheless, the RISKMAN software modeling of the system failure frequency does not account for the effect of the support equipment failures. It can only evaluate the combinations of failures within the system for which the failure frequency is being addressed.

7. CONCLUSION

A calculation approach has been developed that can be used to automate the evaluation of the system failure frequency from the concise fault tree model developed for the system failure probability. This same approach can be applied for the calculation of the support system failure initiating event frequency and the calculation of the unit trip frequency for the trip monitor.

This calculation process can be implemented in the fault-tree linking PRA software to permit the direct calculation of the support system failure frequencies as part of the integrated fault tree model since all of the support components are already linked directly to the equipment supported. The direct linking of the fault tree models for the support system failure initiating events with the plant response/mitigation portion of the model makes the PRA model more integrated and can be used more readily for such applications as risk monitor. This is especially true for the fault tree linking software since the event tree linking software (e.g., RISKMAN) has already incorporated this approach in its software platform.

References

[1] Electric Power Research Institute, "*Introduction to Simplified Generation Risk Assessment Modeling*," EPRI 1007386, January 2004.

[2] Electric Power Research Institute, "*Generation Risk Assessment (GRA) Plant Implementation Guide*," EPRI 1008121, December 2004.

[3] Electric Power Research Institute, "*Trip Monitor Customization and Implementation Guideline*," EPRI 1009112, January 2004.

[4] Electric Power Research Institute, "*Generation Risk Assessment (GRA) at Cooper Nuclear Station*," EPRI 1011924, December 2005.

[5] Electric Power Research Institute, "*Support System Failure Initiating Events Identification and Quantification Guide*," EPRI 1016741, December 2008.