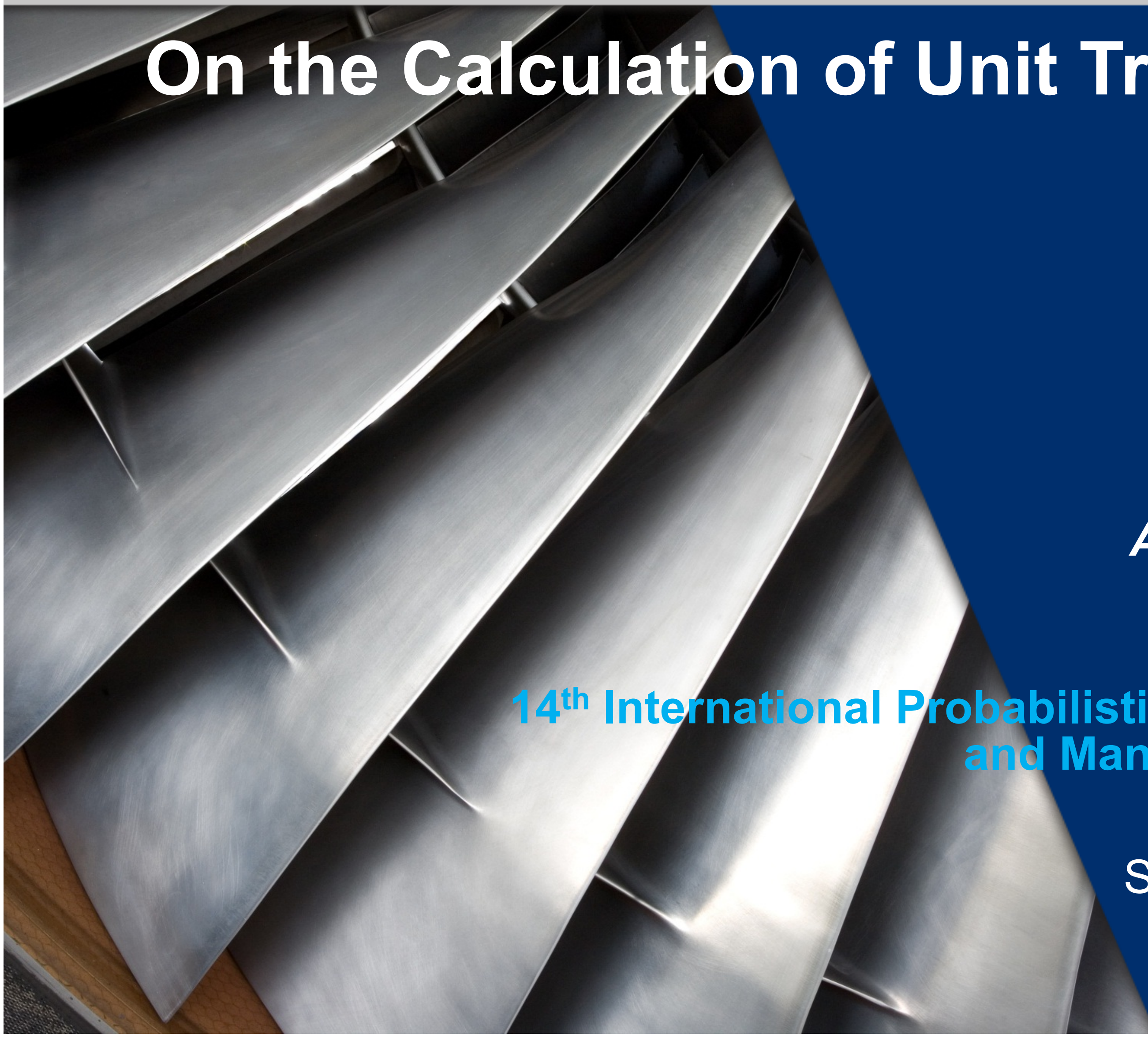
ABS Consulting
AN ABS GROUP COMPANY

On the Calculation of Unit Trip Frequency



Presented by

James C. Lin
ABSG Consulting Inc.

Presented at

14th International Probabilistic Safety Assessment and Management Conference

Los Angeles, CA
September 16-21, 2018

Introduction

- **Computerized, online trip monitor**
  - Calculate the unit trip frequency based on the actual plant configuration.
  - Include in fault trees combinations of equipment failures and unavailability which can lead to a nuclear unit trip.
  - Similar to risk monitor, the risk metric is the frequency of unit trips.
  - Includes user-friendly interfaces to facilitate the specification/input of the actual plant configuration.
  - 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.**
  - Due to insufficient drivers, the development and implementation of the trip monitor in the U.S. did not progress very far at that time.

Calculation of Trip Frequency

- **The methodology used to calculate the trip frequency is the same as the calculation of the loss of support system initiating event frequencies**
  - Typically are evaluated using fault tree models.
  - To model the frequency of failures of systems/functions, the fault tree model developed to model the failure probability of mitigation functions/systems must be expanded to account for the order in which 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 "Support System Initiating Events Identification and Quantification Guide" discusses the major concepts and issues associated with the use of fault tree modeling techniques for the development of initiating event frequencies for loss of a support system.**
  - 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.
  - The frequency of support system failure initiating events modelled using the fault tree approach has been largely developed manually by explicitly enumerating all the combinations of failure sequences.

Evaluating System Failure Frequency – Conceptual Approach

- **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.**
  - 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 2-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.**
  - 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 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.
  - The restoration time for the initially failed component should not exceed the LCO AOT.

Evaluating System Failure Frequency – Conceptual Approach

- **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 24 hours.**
- **The 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.

Evaluating System Failure Frequency – Conceptual Approach

- **For a redundant system with 2 normally running trains, there are 2 different failure sequences because either train can be the initially failed train.**
  - The fault tree model developed for the system failure probability involves only 1 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 with 2 failure-during-operation events.
  - Since either one of these 2 failure-during-operation events can be the initial failure, the 2 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.
    - (2) failure of running Train B followed by failure of running Train A during the period of restoration for Train B.

Evaluating System Failure Frequency – Conceptual Approach

- **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.
- **This 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.
  - 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 an approximation.

Computer Implementation

- **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**
  - 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.
  - 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.
- **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.**

Computer Implementation

- **During the quantification, the software should**
  - Generate the cutset, one at a time,
  - Determine the failure sequences/subscenarios associated with each cutset,
  - 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,
  - Sum up the frequencies for all of the failure sequences/subscenario for that cutset, and
  - 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 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.

System Failures with More Than 2 Normally Running Components

- **When a system failure involves the joint loss of more than 2 normally running components, the failure exposure time for the subsequent failures in each cutset is not always identical to the restoration time for the initially failed component ($?_1$).**
  - In a system with 3 redundant, normally running components, the failure exposure time for the 2nd failure is the restoration time for the first/initial failure; i.e., $?_1$.
  - The failure exposure time for the 3rd failure should be determined by the earlier timing of restoration of either the 1st failure or the 2nd failure; i.e., the shorter of the restoration time for the 1st failure ($?_1$) and the sum of the time between the 1st failure and the 2nd failure (t) and the restoration time for the second failure ($?_2$).
  - The failure exposure time for the 3rd failure should be Minimum($?_1$, t+$?_2$).
- **The mathematic expression used to rigorously evaluate the system failure frequency of 3 redundant, normally running components using the accurate failure exposure time is quite complex.**
  - Although conservative, using the same failure exposure time (i.e., the restoration time for the 1st failure) for the 2nd failure and the 3rd failure is considered a reasonable approximation

Failure of Normally Operating Support Components

- **To calculate the unit trip frequency more accurately, 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.**
  - 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.
  - For 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.

Failure of Normally Operating Support Components

- For a normally operating support component (e.g., an electrical bus) providing support to a normally standby component (e.g., a normally standby pump), the failure of this normally operating support component can also be considered as the initial failure in the calculation of the system failure frequency (failure of this normally operating support component only impacts the standby pump which does not immediately affect the status of the normally running system).
  - 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.

- **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.

Common Cause Failures

- **The treatment of the CCFs is similar to that for the independent failures.**
  – For demand failure modes, the CCF terms are only included in the subsequent failure events.
  – For running failure modes, the CCF 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 ?, ?, and ?) 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.

Existing PRA Software

- **As of the writing of this paper, 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.**
  - 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.
    - 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 RiskSpectrum, 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.
    - 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.
    - 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.

Existing PRA Software

- **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 modeling of the system failure frequency does not account for the effect of the support equipment failures.
  - Can only evaluate the combinations of failures within the system for which the failure frequency is being addressed.

Conclusions

- **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.

Thanks for your attention &
Time for Questions