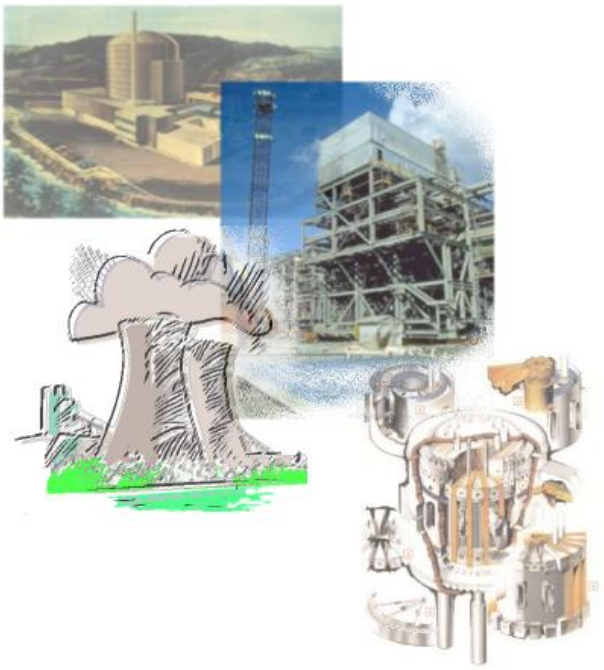
Risk Assessment in Event Evaluation

The Use of Probabilistic Risk Assessment
for the Evaluation of Incidents



Produced for the U.S. Nuclear Regulatory Commission

by

Curtis Smith
Dana Kelly
Mike Calley

Idaho National Laboratory

Spring 2011

FOREWORD

Incidents at locations such as nuclear power plants, waste repositories, and medical treatment facilities occur at many different times and under a variety of situations. Even the most modern, well run organizations may experience events that are precursors to more serious situations. Currently, the U.S. Nuclear Regulatory Commission evaluates a variety of such events at commercial nuclear plants via the Significance Determination Process (SDP), Management Directive 8.3, and the Accident Sequence Precursor (ASP) program. In these programs, the analyst calculates a conditional risk measure (e.g., conditional core damage probability) for an initiating event situation or an unplanned equipment outage. This calculation is called an "event evaluation."

An "event evaluation" uses a probabilistic risk assessment model to obtain a risk measure that is conditional on the situation which existed during an incident. The *Risk Assessment in Event Evaluation* material is intended to address how this evaluation is performed using modern risk analysis tools. Specifically, we will discuss four areas of interest:

1. Background material related to event evaluations.
2. A theoretical framework behind event evaluation calculations.
3. Pragmatic considerations when performing event evaluations using risk analysis tools.
4. Guidance for performing event evaluations when using the SAPHIRE and GEM software.

Upon completion of this course material, the reader should be familiar with the concept of performing an event evaluation. The reader should also be able to identify the key issues relevant to performing an event evaluation as well as the mechanics of performing an evaluation using the supplied software and risk models. Lastly, the reader should be aware of uncertainties and limitations inherent in the results of typical event evaluations.

RELATED READING

Coe, D. H., "Improving Risk Insight Utilization and Communication in the Inspection, Assessment, and Enforcement Programs of the Nuclear Regulatory Commission," *Proceedings of PSA'99, International Meeting on Probabilistic Safety Assessment, August 1999,* pp. 765-771.

Eide, S. A. et al., *Reevaluation of Station Blackout Risk at Nuclear Power Plants. Analysis of Loss of Offsite Power Events: 1986-2004*, NUREG/CR-6890, December 2005.

Fleming, K. N., *Risk-Informed Decision Making*, "Validation of PSAs for Use in Risk Monitoring Applications," *American Society of Mechanical Engineers*, PVP-Vol. 35B, July 1997.

Hoertner, H. and S. Babst, "Results of the Precursor Analysis for German Nuclear Power Plants," *Proceedings of PSA'99, International Topical Meeting on Probabilistic Safety Assessment, August 1999,* pp. 731-737.

Mosleh, A., *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, U.S. NRC, NUREG/CR-5801, 1993.

Mosleh, A, D. Rasmuson, and F. Marshall, *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, 1998.

Poloski, J., D. Marksberry, C. Atwood, and W. Galyean, *Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995*, NUREG/CR-5750, 1999.

Smith, C. L., "Calculating Conditional Core Damage Probabilities for Nuclear Power Plant Operations," *Reliability Engineering and System Safety,* **59** (1998), pp. 299-307.

U. S. NRC, *Risk Assessment of Operational Events Handbook*, Vol. 1, Rev. 1.01, January 2008.

CONTENTS

CONTENTS (cont.)

1. INTRODUCTION

Section 1 contains an introduction to the topic of *Risk Assessment in Event Evaluation*. A brief overview of the course material, example problems, and history of event evaluations are provided.

Learning Objectives

- Explain the intent of the *Risk Assessment in Event Evaluation* material.
- Describe the history and evolution of event evaluation.
- Describe the two types of PRA models available for commercial nuclear power plant risk analysis

Section 1 Topics

Notes for this Section

ASP	Accident Sequence Precursor
BWR	boiling water reactor
CCDP	conditional core damage probability
ISLOCA	interfacing-systems loss-of-coolant accident
LDCA	loss of DC bus
LLOCA	large-break loss-of-coolant accident
LOCCW	loss of component cooling water
LOOP	loss of offsite power
LOSWS	loss of service water system
MLOCA	medium-break loss-of-coolant accident
PRA	probabilistic risk assessment
PWR	pressurized water reactor
SGTR	steam generator tube rupture
SLOCA	small-break loss-of-coolant accident
SPAR	standardized plant analysis risk
TRANS	reactor trip/transient

1.1 Overview

- What is an "event evaluation?"

  > "Event evaluation is a technique where a probabilistic risk assessment (PRA) model is used to obtain a risk measure conditional on the situation existing during an actual or hypothetical event."

- The *Risk Assessment in Event Evaluation* material is intended to

  ◊ Discuss background material related to event evaluations.

  ◊ Present the theoretical framework behind event evaluations.

  ◊ Illustrate practical considerations when performing event evaluations.

  ◊ Illustrate steps and provide guidance for performing event evaluations using the SAPHIRE 8 code (Workspace).

- Major topics and areas of discussion that are covered in the *Risk Assessment in Event Evaluation* material include

  ◊ PRA models that are available for use in event evaluation.

  ◊ The risk measures that may result from an event evaluation.

  ◊ Details on the two types of event assessments.

  ◊ How to treat and model common-cause failure events.

  ◊ Issues related to initiating events and system recovery actions.

  ◊ Processing event evaluations with the GEM software.

  ◊ Evaluating uncertainty in the event evaluation.

  ◊ The display and interpretation of event evaluation results.

1.2 Example Problems

- Several of the sections presented include example problems and workshops.

  ◊ For the sections prior to the SAPHIRE 8 Workspace overview (i.e., Sections 1-7), the workshops will consist of questions that can be answered without the help of a computer.

  - These questions are intended to help reinforce the concepts that are presented in the respective section.

  ◊ For the sections after the SAPHIRE 8 Workspace overview (i.e., Section 9-13), the workshops will consist of problems that require exercising the SAPHIRE software.

  - These questions are intended to provide "hands-on" experience in performing an event evaluation using current tools.

1.3 History of Event Evaluation

- Around 1977, the U.S. NRC Risk Assessment Review Group acknowledged the potential for accident precursor events to contribute to the overall plant operational risk.

  ◊ The Review Group recommended that "potentially significant sequences, and precursors, as they occur, be subjected to the kind of analysis contained in WASH-1400." WASH-1400 is also known as the "Reactor Safety Study."

- In 1982, the first of a series of NUREG/CR reports was published that addressed the Review Group's recommendation.

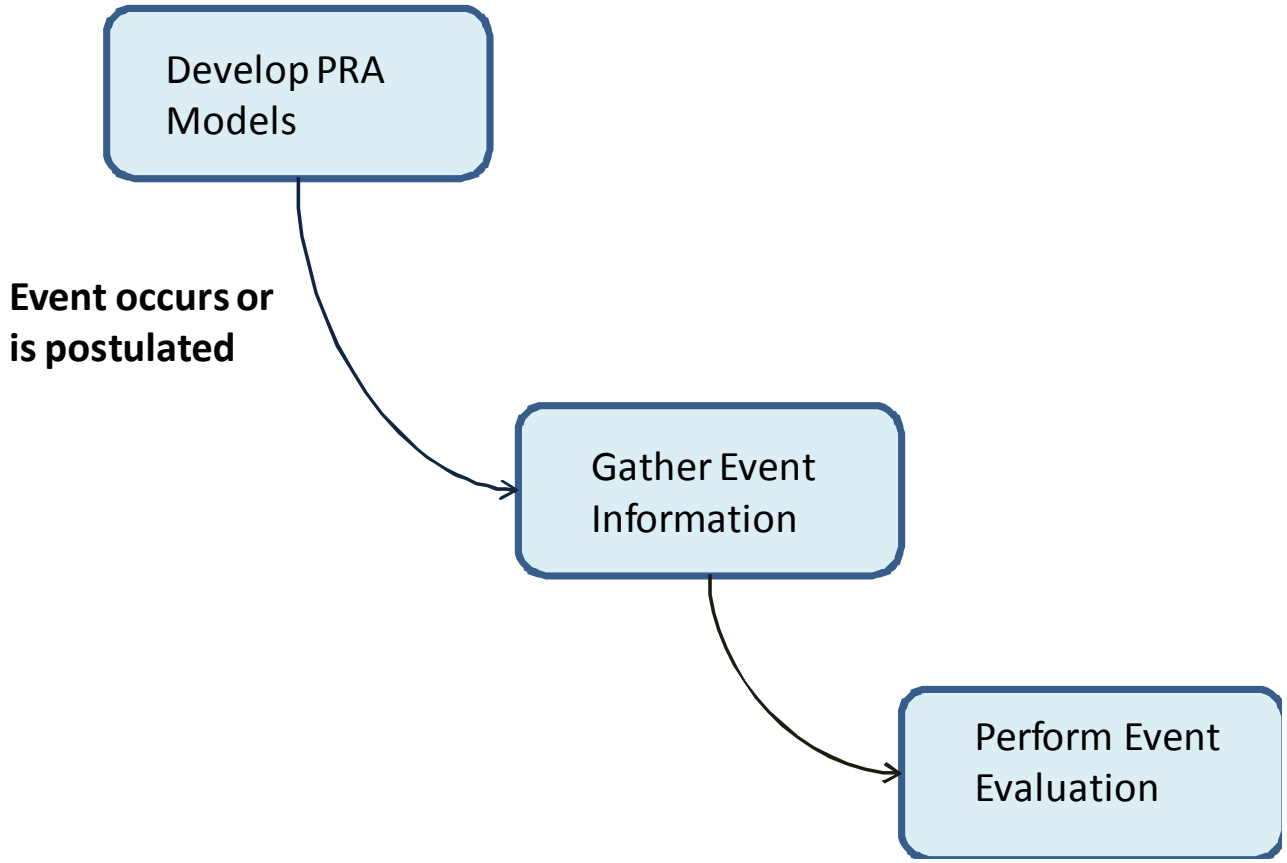
  ◊ NUREG/CR-2497, *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report*, addressed precursor events from the 1969 to 1979 time period.

  ◊ Other NUREG/CR (NUREG/CR-4674) reports in the series addressed precursor events for subsequent years. These reports are the Accident Sequence Precursor (ASP) analyses documents.

  ◊ These older analyses utilized simplistic models and evaluation techniques. In this course, we will present and provide detailed models and techniques.

- To perform an event evaluation, several processes must be completed prior to the actual analysis of an incident.

An overview of a typical event evaluation process



In this course, we will focus primarily on the last step in the process. We will, though, discuss some of the PRA models available for event evaluations.

1.4 Summary of Nuclear Power Plant PRA Models

- In general, two types of nuclear power plant models are in use by the industry and NRC.
  - ◊ Detailed models developed by individual plants. This model type is referred to as a "detailed PRA model."
  - ◊ Standardized models used by the NRC. This model type is referred to as a "standardized plant analysis risk", or SPAR model.
- The SPAR PRA models are available in the SAPHIRE 8 computer code.

- The main difference between the two types of PRA models is the level of detail built into the models, although this difference is lessening with time.

  ◊ The SPAR models all contain a consistent number of event trees for categories of PWR and BWR plants.

  ◊ For the SPAR models, the number of fault trees for each PWR or BWR class varies, depending on the plant-specific front-line systems needed to prevent core damage.

    - These fault trees have detail down to the component level.
    - Revision 3 (Rev. 3) and above also contain support systems.

  ◊ For the detailed utility PRA models, the number of event and fault trees contained in the PRA can vary significantly from plant to plant, and they generally contain somewhat more detail than the SPAR models.

    - The utility PRA may contain more event trees (and analyzed initiating events) than the SPAR model (SPAR models evaluate all utility PRA initiating events that contribute greater than 1 percent overall CDF).
    - The utility PRA may contain more fault trees than the SPAR model.

- The SPAR plant categorization scheme groups plants based upon similar responses to transients and accidents. Differences are based upon:

  ◊ Front-line systems included in the plant design.

  ◊ Availability of unique mitigative features that provide core protection.

- The SPAR plant categorization scheme was developed by examining how the systems for each reactor plant are used to perform protective functions required to prevent core damage following certain initiating events. A list of analyzed initiating events include (from ”Generic PWR” SPAR model):

  - ◊ HPI Cold Leg Interfacing System Loss-of-coolant Accident
  - ◊ LPI Cold Leg Interfacing System Loss-of-coolant Accident
  - ◊ RHR Suction Interfacing System Loss-of-coolant Accident
  - ◊ Large Loss-of-coolant Accident
  - ◊ Loss of Vital Voltage Bus A
  - ◊ Loss of Condenser Heat Sink
  - ◊ Loss of Vital DC Bus A
  - ◊ Loss of Vital DC Bus B
  - ◊ Loss of Feedwater
  - ◊ Loss of Offsite Power (Grid Related, Plant Centered, Switchyard Related, and Extreme Weather Related)
  - ◊ Loss of Service Water
  - ◊ Medium Loss-of-coolant Accident
  - ◊ Small Loss-of-coolant Accident
  - ◊ General Plant Transient
  - ◊ Loss of Component Cooling Water
  - ◊ Steam Generator Tube Rupture
  - ◊ Reactor Vessel Rupture (Excessive Loss-of-coolant Accident)

- Project statistics for the ”Generic PWR” SPAR model include:

Item	**Number**
Fault Trees	250
Event Trees	29
Basic Events	3689
Accident Sequences	2144
Event Failure Modes	19

Summary - The SPAR models are categorized (i.e., grouped) by plant design corresponding to similar responses to transients and accidents. The SPAR models also are quite uniform across the model population since similar modeling assumptions, techniques, data, and size are used during the model construction.

- For this course, the computer exercises (e.g., in the SAPHIRE software) will utilize the ”Generic PWR” SPAR model.

- The SPAR models utilize several SAPHIRE features to assist in the construction of the PRA model

  ◊ Template events, where the event data is shared as part of an overall generic database tied to EPIX/RADS data reported by the industry.

  ◊ Analysis module to numerically evaluate common-cause failure probabilities.

  ◊ Analysis module to determine the frequency and recovery probability for losses of offsite power.

- Documentation for the SPAR models are provided in a subdirectory in the electronic database.

NOTES

.

2. RISK MEASURES FOR EVENT EVALUATION

Section 2 introduces the various risk measures calculated in an event evaluation. Examples of how to calculate these risk measures are provided.

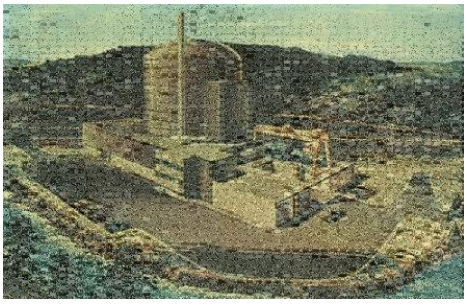
Learning Objectives

- Describe two types of event evaluations used for the analysis of events and provide an example of each.
- Define core damage probability (CDP) and conditional core damage probability (CCDP).
- Define the event importance measure.
- Discuss alternative risk measures.

Section 2 Topics

Notes for this Section

ASP	Accident Sequence Precursor
CCDP	conditional core damage probability
CD	core damage
CDP	core damage probability
DG	diesel generator
SPAR	standardized plant analysis risk (the PRA models used by the SAPHIRE software)



2.1 Introduction

- Event evaluation is a technique by which a PRA model is used to calculate a risk measure conditional on the situation existing during an event.

  ◊ A PRA model is modified to account for specific initiators, failures, or conditions that occurred during the event in question.

- Two types of event analysis are used:

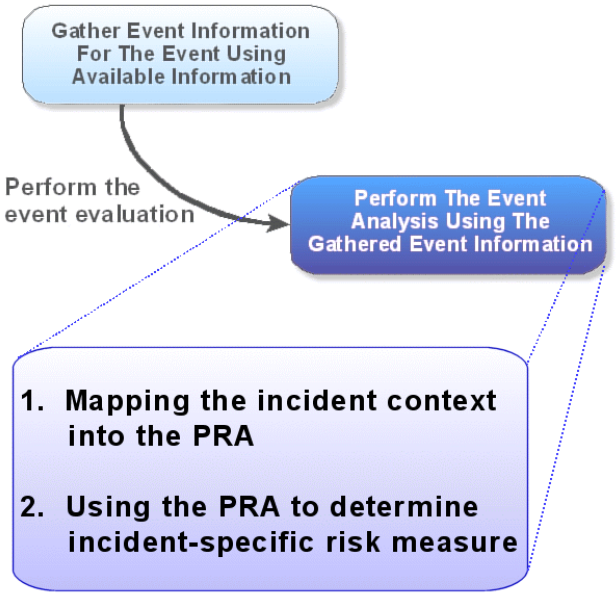
  ◊ Events involving an *initiator*. These are called **initiating event assessments**.

  Examples:
  1) Offsite power was lost during a storm while at full power.
  2) A shipping cask was dropped during transportation.
  3) An electric generator stopped supplying power to a critical bus.

  ◊ Events involving a *reduction* in safety system reliability or function for a specific *duration*. These are called **condition assessments**.

  Examples:
  1) A manual valve was improperly installed and was inoperable for several months.
  2) A generator fuel supply was found to be empty due to a leak.

- Two general steps take place during the actual event evaluation:



- **Gathering detailed information about the event is crucial**.

  ◊ Knowledge of the system design and operation, along with details found in the PRA model, are required to map the incident into the PRA model accurately, and will help to avoid unnecessarily conservative results.

    – Lack of detailed information may require the analyst to make conservative assumptions.

  ◊ Questions about equipment recoverability and potential for common cause failure complicate the modeling of typical events.

  ◊ Types of information that are needed for an event evaluation include

    – Chronology of actions during event.
    – Operator actions including recovery of systems.
    – Equipment failures and failure causes.
    – Equipment unavailability (e.g., equipment out for testing)
    – Conditions that may have hindered operation.
    – Cause of initiating event (if applicable).
    – Location of equipment.

- Mapping the event into the PRA model is a prerequisite to obtaining event evaluation measures.

  MAPPING the event into the PRA model is the process of modifying the PRA so that it represents the conditions of the event (either actual or hypothetical) being modeled. In other words, the context surrounding the event is imposed on the PRA model and boundary conditions.

- Once the PRA model is selected, then modify the model.

    – Adjust the initiating events depending on the type of event being evaluated.
    – Determine impacts on system reliability, which potentially include.

      1. Modeling failed, unavailable, or degraded components.
      2. Modifying common cause failure probabilities.
      3. Modifying nonrecovery probabilities.
      4. Changing the structure/assumptions of the PRA model.

- After mapping the event into the PRA, risk measures for the event can be calculated.
- Several different types of risk measures could be used to evaluate the risk significance of an event.
  - ◊ For example, we could find a conditional probability of core damage given a specified condition.

    P(core damage|offsite power was lost **and** DG A *did not start*)=...

  - ◊ An increase in core damage probability, referred to as "event importance," can be found by subtracting the nominal core damage probability from the conditional probability.

    $\text{Importance}_{\text{event}} = P(CD|\textit{event conditions}) - P(CD|\text{nominal conditions})$

  - ◊ Alternatively, we could use a ratio measure instead where we would divide the conditional probability by the nominal probability.
  - ◊ A conditional frequency of core damage could be found given a specified condition and duration.
  - ◊ Similarly, a conditional frequency of large early release of fission products from containment could be calculated.
  - ◊ Traditional PRA importance measures can be obtained for the basic events in the cut sets. Examples of these importance measures include
    - Fussell-Vesely, Birnbaum, and Risk Increase Ratio (a.k.a., RAW).
  - ◊ Uncertainty analysis of the results via Monte Carlo sampling is also possible.
  - ◊ Lastly, quality checks should be made of the resulting analysis.

Summary: The good and the bad →

***Good**: An abundance of risk metrics are available for modern event assessments.*

***Bad**: An abundance of risk metrics are available for modern event assessments.*

2.2 Conditional Probability Calculations

- Conditional probability calculations attempt to estimate the probability of a bad outcome (e.g., core damage) given that an event or condition occurred.

  ◊ For nuclear power plants, the conditional core damage probability (CCDP) given condition Z is

$$P(CD \mid Z) = \frac{P(CD \cap Z)}{P(Z)} = CCDP$$

  where P(Z) > 0.

Boolean algebra review #1 ⇨	∪ represents a logical OR operation (or union) ∩ represents a logical AND operation (or intersection)

Example #1: Assume that the (nominal) minimal cut sets are

CD = IE·A·B + IE·A·C + IE·B·C + IE·D

where, for conciseness, "·" indicates the logical AND operation and "+" indicates the logical OR operation. What this means is that to get core damage (CD), we first have to have an initiating event (IE) and then either (1) A and B fail, (2) A and C fail, (3) B and C fail, or (4) D fails.

◊ The condition to model is that initiator IE occurred while component C was inoperable (and was not recoverable).

◊ Thus, we want to calculate

P(CD| IE =True, C=True)

(i.e., the CCDP if this is a nuclear power plant PRA).

Boolean algebra review #2 ⇨	(Event A) "AND" (TRUE house event) = Event A (Event A) "OR" (TRUE house event) = TRUE

◊ In terms of event probabilities, we can rewrite the Example #1 equation as

P(CD) = P(IE·A·B + IE·A·C + IE·B·C + IE·D)

This is the expression for the probability of the union of the minimal cut sets that one would obtain using a fault tree/event tree tool like SAPHIRE. When we have a set of minimal cut sets, we need to quantify the union of those cut sets to obtain our results.

◊ In PRA, this problem is typically approached with one of three methods[1]

1. Rare event approximation: This calculation approximates the probability of the union of minimal cut sets by assuming cut sets are mutually exclusive (i.e., no overlap of cut sets). The equation for the rare event approximation is

$$P = \sum_{i=1}^{m} Ci$$

where P is the probability of interest, C_i is the probability of the i'th cut set, and m is the total number of cut sets.

2. Minimal cut set upper bound: This calculation approximates the probability of the union of minimal cut sets by assuming each cut set is independent of all other cut sets (i.e., no shared basic events in multiple cuts sets which means each basic event appears in only one cut set). The equation for the minimal cut set upper bound is

$$P = 1 - \prod_{i=1}^{m} (1 - Ci)$$

where P is the probability of interest, C_i is the probability of the i'th cut set, and m is the total number of cut sets. Note (1) that the capital pi symbol implies multiplication and (2) most PRA tools, including SAPHIRE, utilize this equation as the default method of quantification.

3. Exact: This calculation calculates the probability of the union of minimal cut sets by accounting for the overlap of cut sets and properly accounts for whether or not each cut set is independent of all other cut sets. This calculation can be very time consuming. There are various methods for determining the exact probability given a set of cut sets. The most common approach is referred to by SAPHIRE as “min-max.” The min-max approach works by obtaining various combinations of the minimal cut sets to form higher-order sets. Then, finds the probability from the "first order" set (which are just the cut sets you started with). From this value, you subtract the

[1]A newer approach to quantification is the binary decision diagram (BDD), which can produce an exact result very quickly. This option is not yet widely available in U. S. PRA software.

probability from the "second order" set. From this value you add the probability from the "third order" set. From this value you subtract the probability from the "fourth order" set, etc., with as many passes as you have cut sets.

Note, when you begin with a typical number of PRA cut sets, the exact probability calculation performed in this fashion may be very time consuming or even impossible to compute. Thus, the true exact solution is rarely employed in practice. Often, an approximation is performed by specifying the number of passes to perform. SAPHIRE will perform up to 50 passes.

As an example, when there are two cut sets, or CD = A + B, looks like

$P(CD)_{exact} = P(A) + P(B) - P(A \cap B)$

Note the "AND" sign (∩) in the equation. This implies that Boolean algebra must be performed for each higher-order set, which greatly complicates the quantification.

◊ Now, back to our example. We must quantify the equation for Example #1. Let us evaluate this equation using both the rare event approximation and the exact equation.

P(CD) = P(IE·A·B + IE·A·C + IE·B·C + IE·D)

Rare event approximation:

$$P = \sum_{i=1}^{4} C_4$$

= P(IE·A·B) + P(IE·A·C) + P(IE·B·C) + P(IE·D)

Probabilities to quantify this equation to be presented next.

Exact (inclusion-exclusion)

= P(IE) ·[P(A·B) + P(A·C) + P(B·C) + P(D) - P(A·B·A·C) - P(A·B·B·C) - P(A·B·D) - P(A·C·B·C) - P(A·C·D) - P(B·C·D) + P(A·B·A·C·B·C) + P(A·B·A·C·D) + P(A·B·B·C·D) + P(A·C·B·C·D) - P(A·B·A·C·B·C·D)]

Now, we still need to evaluate the Boolean algebra in the exact probability expression. So, let us do that and also rewrite the equation by denoting that P(IE) = ie, P(A) = a, etc. Assuming independence, we have

P(CD) = ie (ab + ac + bc + d - abc - abc - abd - abc - acd - bcd + abc + abcd + abcd + abcd - abcd)
= ie (ab + ac + bc + d - 2abc - abd - acd - bcd + 2abcd)

◊ This equation would then be used to calculate the *exact* probability of having core damage. Again, we still need the event probabilities.

◊ The condition for Example #1 was that we want to evaluate initiator IE occurring while component C is inoperable (and was not recoverable). Thus, our CCDP is

$P(CD| IE=True, C=True) = P(A + B + D)$

Rare event approximation:

$= P(A) + P(B) + P(D) = a + b + d$

Exact (inclusion-exclusion)

$= P(A) + P(B) + P(D) - P(A\cdot B) - P(A\cdot D) - P(B\cdot D) + P(A\cdot B\cdot D)$
$= a + b + d - ab - ad - bd + abd$

◊ To calculate the CCDP, we need values for the event probabilities. Assume

- $P(IE| IE\ occurred) = 1$
- $P(A) = 1 \times 10^{-1}$
- $P(B) = 2 \times 10^{-1}$
- $P(C) = 5 \times 10^{-2}$
- $P(D) = 5 \times 10^{-3}$.

◊ Finally then, the CCDP using the assumed probability values is

Rare event approximation:

$P(CD| IE=True, C=True) = a + b + d = (0.1) + (0.2) + (0.005)$
$= 0.305 \approx 0.3$

Exact (inclusion-exclusion)

$P(CD \mid IE=True, C=True) = a + b + d - ab - ad - bd + abd$

$= (0.1) + (0.2) + (0.005) - (0.02) - (0.0005) - (0.001) + (0.0001)$

$= 0.2836 \approx 0.3$.

◊ We can now state that "the conditional core damage probability, or CCDP, given that initiator IE occurs while component C is inoperable (and is not recoverable) is about 0.3."

◊ Other examples of how the CD equation changes when different components fail are shown below.

$P(CD \mid nominal) = P(IE \cdot A \cdot B + IE \cdot A \cdot C + IE \cdot B \cdot C + IE \cdot D)$

$P(CD \mid IE=True, A=True) = P(B + C + D)$

$P(CD \mid IE=True, D=True) = 1.0$ (the system has failed)

$P(CD \mid D=True) = P(IE \cdot A \cdot B + IE \cdot A \cdot C + IE \cdot B \cdot C + IE)$

$= P(IE)$

2.3 Event Importance Calculations

- Event Importance calculations attempt to estimate the change in core damage probability given that an event or condition occurred.

  ◊ The event importance for core damage given an incident where Z fails is

  $$\text{Importance}_{\text{event}} = \text{CCDP} - \text{CDP}$$

  where CCDP is the conditional core damage probability given Z fails
  CDP is the nominal core damage probability.

  ◊ The $\text{Importance}_{\text{event}}$ calculation is a difference of two probabilities, and, as such, is not a probability (hence the name "Importance").

  Note that the CCDP could be *lower* than the CDP (for example, if you are proposing a hypothetical design improvement), thereby resulting in a negative $\text{Importance}_{\text{event}}$ value.

  ◊ The $\text{Importance}_{\text{event}}$ gives us a sense of the relative differences between the two probabilities.

  ◊ We will see later that the SAPHIRE software calculates an $\text{Importance}_{\text{event}}$ for condition assessments.

  – Event cases that have a nominal case (i.e., CDP) subtracted from a CCDP are just a type of importance measure. This numerical result has been mislabeled in the past as a CCDP.

- Example #2 for an $\text{Importance}_{\text{event}}$ calculation: Assume that our nominal minimal cut sets for core damage are

  $$CD = IE \cdot A \cdot B + IE \cdot A \cdot C + IE \cdot B \cdot C + IE \cdot D$$

  ◊ The condition to model is that component C was inoperable (and was not recoverable) for a duration of 30 days.
  ◊ We want to calculate

  $$P(CD|C=True) - P(CD) = CCDP - CDP$$

  (i.e., $\text{Importance}_{\text{event}}$) where the duration is 30 days.

◊ Assuming that the events IE, A, B, C, and D are independent and their probabilities can be written as P(IE) = ie, P(A) = a, P(B) = b, P(C) = c, and P(D) = d, we can write the CDP as

$P(CD) = P(IE \cdot A \cdot B + IE \cdot A \cdot C + IE \cdot B \cdot C + IE \cdot D)$

Rare event approximation:

$= ie\ (ab + ac + bc + d) = CDP$

Exact (inclusion-exclusion)

$= ie\ (ab + ac + bc + d - 2abc - abd - acd - bcd + 2abcd)$
$= CDP$

◊ The condition to model for Example #2 is that component C was inoperable (and was not recoverable). Thus, our CCDP is

$P(CD|\ C=True) = P(IE \cdot A + IE \cdot B + IE \cdot D)$

Rare event approximation:

$= ie\ (a + b + d) = CCDP$

Exact (inclusion-exclusion)

$= ie\ (a + b + d - ab - ad - bd + abd) = CCDP$

◊ Again, to calculate the CDP and CCDP, we need values for the event probabilities. Assume

- P(IE|duration of 30 days) = 1×10^{-2}
- P(A) = 1×10^{-1}
- P(B) = 2×10^{-1}
- P(C) = 5×10^{-2}
- P(D) = 5×10^{-3}

◊ The exact CDP and CCDP using the probability values above are

CDP = P(CD) = 0.000378 = 3.8E-4

CCDP = P(CD | C=True) = 0.00284 = 2.8E-3

◊ Therefore, our $\text{Importance}_{\text{event}}$ is

$$\text{Importance}_{\text{event}} = 0.00284 - 0.000378 = 0.00246 \approx 2.5\text{E-}3$$

Note that for initiating event analysis, the $\text{Importance}_{\text{event}}$ is not calculated.

Summary:

We tend to use only two risk metrics for event evaluations:

P(Core Damage | event) = CCDP

$\text{Importance}_{\text{event}}$ = CCDP - CDP

Fortunately, we have software to perform the Boolean algebra!

2.4 Risk Measures Used for Other Types of Analyses

- The NRC regulates nuclear power plant operation through a combination of several regulatory processes. One of these processes, safety oversight, includes activities such as inspection, assessment of performance, evaluation of experience, and other general support activities.

  As part of these regulatory activities, a variety of risk metrics are utilized. At this point, we have provided details on three metrics, a CCDP, CDP, and $\text{Importance}_{\text{event}}$.

- To help contrast the process for event evaluations with other NRC activities, we will briefly look at two risk-related activities.

  ◊ Significance Determination Process (SDP)
  ◊ Generic Issue Resolution

- The Significance Determination Process (SDP) is one of the methods that the NRC uses to assist in risk-worth determination of inspection incidents. In general, it is less formal (quantitatively) than the process described in the Event Evaluation course.

  ◊ The Phase 2 SDP uses simplified checklists to estimate a change in "annualized core damage frequency (CDF)." The checklist is basically a look-up version of the PRA. (This method has been built into the latest versions of the SPAR models and SAPHIRE 8. These models and SAPHIRE are ready for use.)

  ◊ The three steps to determining the CDF are: (1) estimate the initiator frequency, (2) estimate the incident duration, and (3) estimate remaining mitigating system capability.

  ◊ Then, estimate (via the checklists) P(CD | initiator), or a CCDP, where the probability is forced to be over a year.

  Note that if one knows the rate (λ) of an event like core damage, the probability of one of more events can be found by:

  $P(\text{event}) = 1 - \exp(-\lambda T)$ If $(\lambda T) < 0.1$, then $P(\text{event}) \approx \lambda T$

◊ Decision criteria are provided via regions (and associated colors) of interest:

Red	Increase is ≥ 10^{-4}/yr
Yellow	Increase is between 10^{-5}/yr but less than 10^{-4}/yr
White	Increase is between 10^{-6}/yr but less than 10^{-5}/yr
Green	Increase is < 10^{-6}/yr

◊ What should an analyst do if incident not in checklist?

First, check PRA (on your own or via risk specialist)
If not in PRA, check Maintenance Rule
If not in Maintenance Rule, assume unimportant

- Generic Issue Resolution

To assess the cost effectiveness of a particular plant alternative, a dollar-to-person-rem averted ratio (DPR) is generated.

A value of $2,000 per person-rem averted has been used by the NRC as an upper bound in deciding whether corrective measures may be appropriate.

When onsite averted costs (i.e., a potential reduction of onsite accident costs) are included as a cost offset, the DPR ratio becomes;

$$DPR = \frac{Cost\ of\ \ Alternative - Onsite\ Averted\ Cost}{Offsite\ Person - rem\ Averted}$$

As part of the calculation for onsite averted cost and the person-rem averted, the change in core damage frequency (due to the proposed modification) is estimated.

2.5 Workshop

3. INITIATING EVENT ASSESSMENT

Section 3 discusses the theory behind performing initiating event assessments, which are performed when the event being evaluated involves the occurrence of a PRA initiating event.

Learning Objectives

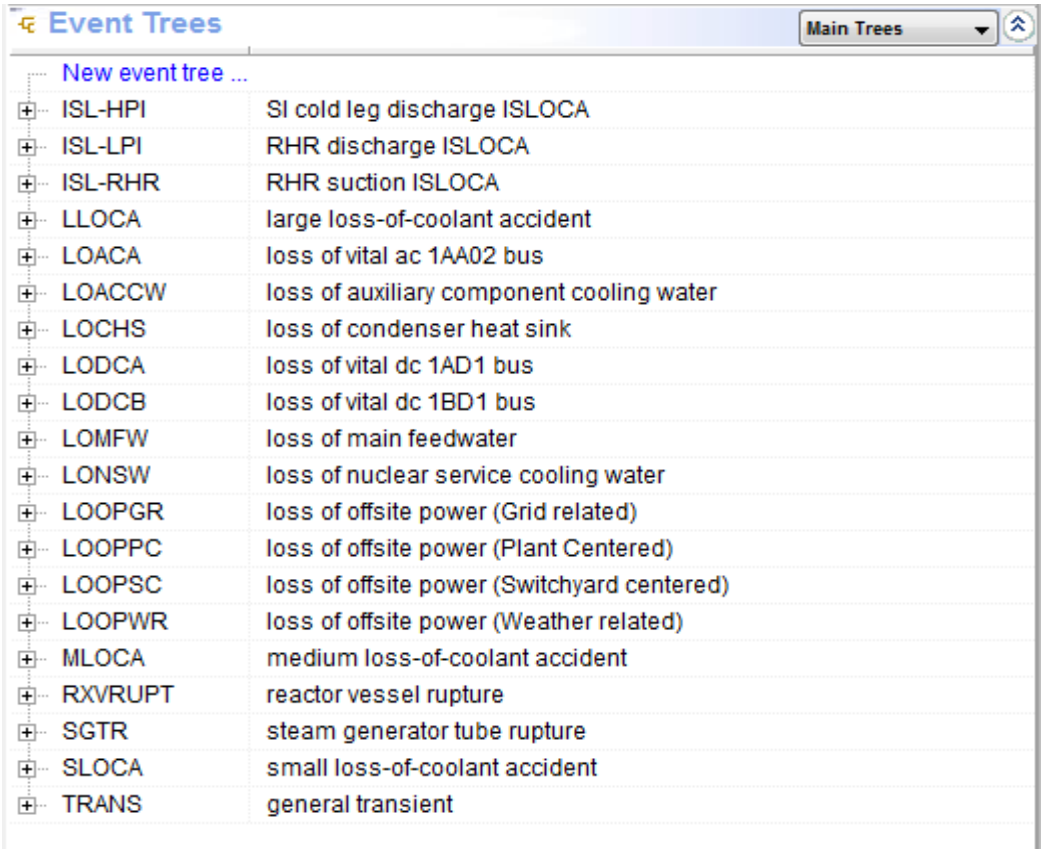
- ◊ Explain the initiating event assessment and the steps involved.
- ◊ State the appropriate risk measure for an initiating event assessment.

Section 3 Topics

Notes for this Section

3.1 Introduction

- Event evaluations are performed in order to quantify the risk potential from a particular incident, either actual or hypothetical.
    - ◊ For initiating event assessments, the risk arises due to an initiator occurring.
        - – Following the upset condition caused by the initiator, the facility or system in question is immediately forced into a "risky" situation. Recall that the initiating event is the first event in an accident sequence, leading to core damage; without the initiating event, we cannot have core damage.
        - – Components or systems that are degraded or inoperable at the time the initiator occurs increase the overall risk of the event if they impact systems intended to respond to the upset caused by the initiating event.
        - – A core damage probability can be calculated that is conditional upon the initiator occurring and the initial conditions of the event.
    - ◊ For the SPAR models, a set of initiators is modeled (for example, from the “Generic PWR” Model).



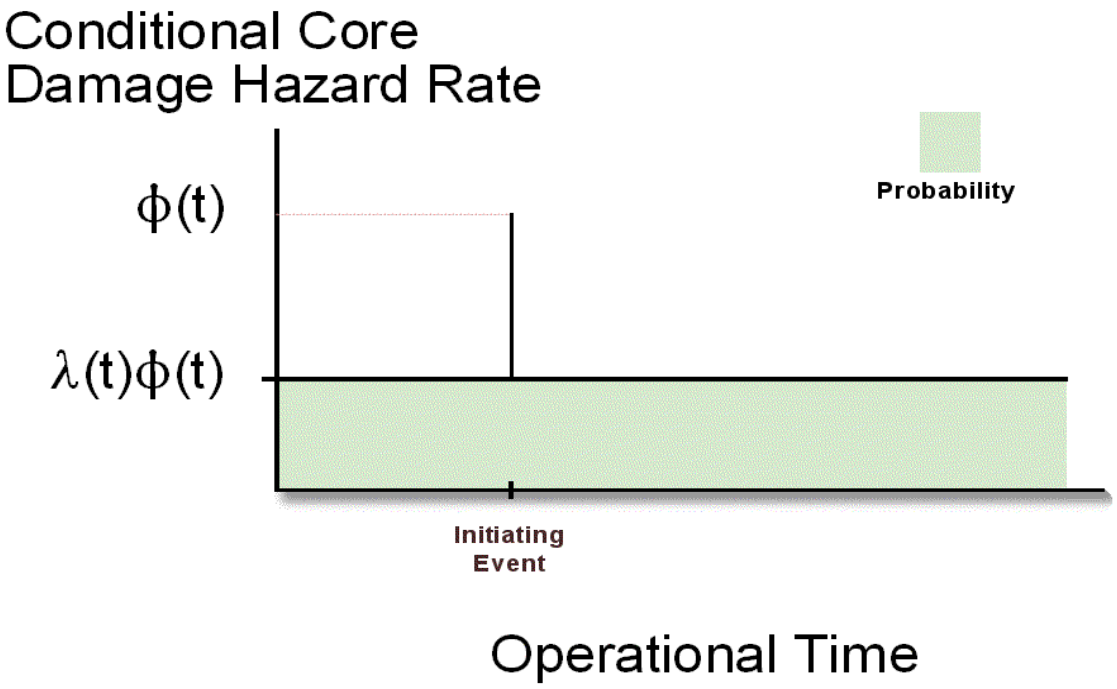
- The risk that is calculated is like a "risk spike" for the event.

  where:

  $\lambda(t)$ is the initiating event rate

  $\Phi(t)$ is the conditional probability of core damage given the initiating event.

  Note that the product $\lambda(t)\cdot\Phi(t)$ is the core damage frequency (or hazard rate). Further, since a PRA models many initiators, the overall core damage frequency is the summation of the product of each initiating event (λ_i) and its associated plant response (Φ_i).



  ◊ The "risk spike" is the risk result given by the PRA model.

- The "risk spike" is not really a spike. The risk is more like a step function that returns to nominal conditions after the initiator scenario is completed (and the plant is returned to power operations).

  – Following an initiator, plant and operator responses will determine the likelihood of core damage.

  – Response time to deal with an initiating event varies from minutes to days.

- ◊ Looking more closely at the terms shown above:

  $\lambda(t)$ represents the frequency of initiating events at the plant.

  $\Phi(t)$ represents the systems that respond to an initiating event. That is, what is the probability that the plant's structures, systems, and components fail to prevent core damage.

- ◊ Multiple, simultaneous component or system outages at the time of the initiator should be modeled by mapping the outage into the model.

- For actual event evaluations, the analyst will normally use the available PRA models in conjunction with additional resources.

  - ◊ Plant or system drawings, descriptions, and modeling notebooks.

  - ◊ Final Safety Analysis Reports, individual plant examinations, and plant source books.

  - ◊ Event reports.

  - ◊ Discussion with cognizant personnel.

3.2 Treatment of Initiating Events

- For initiating event assessments, the initiating events in a model must be modified to reflect the event in question.

  - ◊ First, those initiators that did not occur are set to a FALSE (zero probability) house event.

    - – Since initiating events are ANDed with other basic events in the sequence cut sets, sequences with a FALSE house event in every cut set will not show up in the results.
    - – Alternatively, one could set the probability of the initiators that do not occur to a value of zero (this will also remove sequences).

◊ Second, for the initiator that did occur, its value should be modified depending on the type of initiator, either (a) non-recoverable or (b) recoverable.

(a) NON-RECOVERABLE INITIATORS:

Set the initiating event to a TRUE house event (1.0).

For example, in the case where a loss of a vital DC bus occurs, *and if* there is no chance of recovering the bus, the initiating event should be set to a TRUE house event.

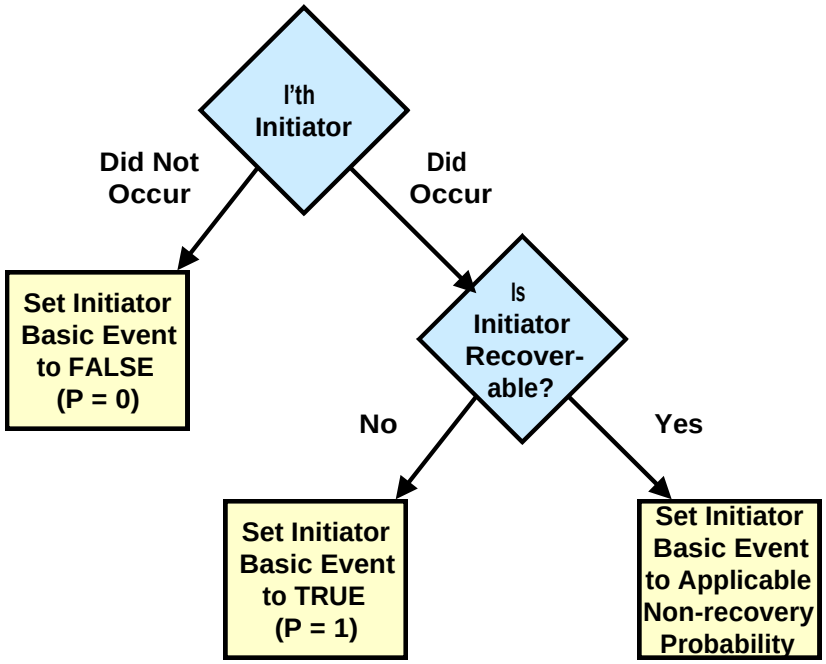
(b) RECOVERABLE INITIATORS

Set the initiating event to a representative "nonrecovery" probability.

For example, in the case where offsite power is lost and it is recovered (i.e., is recoverable), then the initiator should be set to its short-term nonrecovery probability.
The section on recovery actions discusses this case in detail.

◊ Based upon the information provided in the event documentation (e.g., LER), the analyst must determine whether or not the initiator is considered to be recoverable.

◊ In summary, for initiating event assessment, the initiating events should be modified according to the flow diagram below.



3.3 Treatment of Component Recovery

- The components or systems that are inoperable at the time the initiator occurs need to be evaluated in order to determine whether they are recoverable.

    ◊ If a component or system is not recoverable, it (and its nonrecovery event, if present) should be set to TRUE.[2]

        – Remember that setting a component or system to a TRUE house event indicates that the component or system is failed (i.e., not able to perform its intended function).

        – Failed components or systems will not show up in the resulting sequence cut sets. Rather, the TRUE house event will alter the logic that is used in the PRA model.

        – Reasons why a component or system may not be recoverable include:

            ▪ Nonrepairable component failure
            ▪ Harsh environment (e.g., high radiation, high temperature)
            ▪ Location (e.g., inside containment versus outside)
            ▪ Timing/staffing limitations

    ◊ If a component or system **is** recoverable, its associated nonrecovery basic event should be set to an appropriate nonrecovery probability. If a nonrecovery event is not present, then the analyst may have to add a nonrecovery event to the model. Note that merely setting the component event to the estimated nonrecovery probability will cause an undesired effect on common-cause failure probability if the component is a member of a component group whose common-cause failure probability is calculated automatically by the SAPHIRE plug-in.

        – The component or system nonrecovery probability is generally estimated using a human reliability method (e.g., SPAR-H).

        – Section 7 provides additional discussion on aspects related to nonrecovery modeling and probability determination.

        – Recoverable components or systems are generally those that were actually recovered during the course of the event.

[2]This may affect a common-cause failure probability calculated by SAPHIRE. This potential is being ignored for now. Adjustments to common-cause are considered in a Section 6.

– But, if a component or system is not recovered for a particular event, it is not automatically categorized as nonrecoverable.

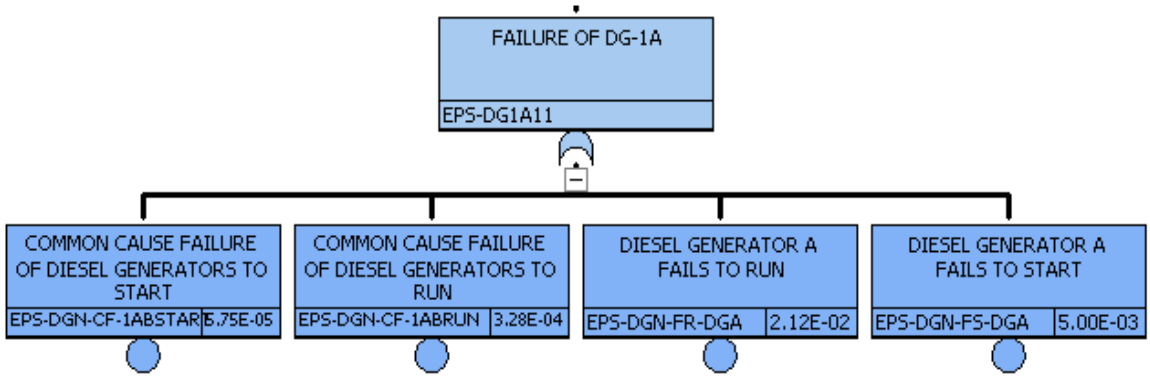
– If a failed component is not needed in order to prevent core damage (possibly because some other component or system did not fail), plant operators may not immediately attempt to recover the failed component or system.

3.4 Treatment of Component Common Cause Failures

- Many PRA models have common cause failures included in the fault tree logic.

◊ These common cause failure events are generally either train-level or component-level events.

An example of component-level common cause failure events (from a SPAR model) are shown below.



In the figure, the diesel generators have both a common cause "fails to start" and a "fails to run" basic event.

◊ For those components or systems which are operable (or in standby and are potentially operable) at the time of the initiating event, no modifications are needed for their common cause failure parameters.

◊ Recall that we are not attempting to quantify "what WAS the probability" of an event.

◊ Instead, we are attempting to estimate "what is the probability" conditional upon the incident, or in other words, how close was the incident to proceeding to a PRA-type consequence.

- If a component or train is inoperable at the time of the initiating event, three steps must be performed.

    1. Identify the failure attributes (i.e., cause factors) for inoperable equipment to determine how to treat the failed component.

    2. Calculate new common cause failure probability based upon failure criteria (if the common-cause module in SAPHIRE is *not* used).

    3. Modify the common cause failure probability in the PRA model (if the common-cause module in SAPHIRE is *not* used).

- We will discuss specifics of the common cause probability modifications in Section 6, "Treatment of Common Cause Events."

Summary:

The adjustment of the PRA model to account for event specifics is important.

Items such as non-recovery probabilities and the probability of common-cause failure have a direct impact on the bottom-line results.

3.5 Appropriate Risk Measure for Initiating Event Assessment

- The risk measure for ***initiating event*** assessments is the CCDP.
    - ◊ This measure is conditional upon both
        - – A particular initiating event occurring (and the others not occurring)
        - – Components, trains, or systems that are degraded or inoperable at the time the initiator occurs.

- An event importance (i.e., $\text{Importance}_{\text{event}}$) is not calculated for initiating event assessments.
    - ◊ The determination of the CDP may not be obvious (e.g., is instantaneous probability or the probability over a short duration needed?).
    - ◊ The CDP for an initiating event assessment would be like an instantaneous risk measure.

Summary:

When presented with an initiating event assessment, the overall results will be in the form of a CCDP.

3.6 Workshop

4. CONDITION ASSESSMENTS

Section 4 discusses the theory behind performing condition assessments. Condition assessments are analyses for events where a system or component was known to be degraded or inoperable for a certain length of time, during which no initiating event occurred.

Learning Objectives

- Explain a condition assessment and the steps taken for the treatment of initiating events in a condition assessment.

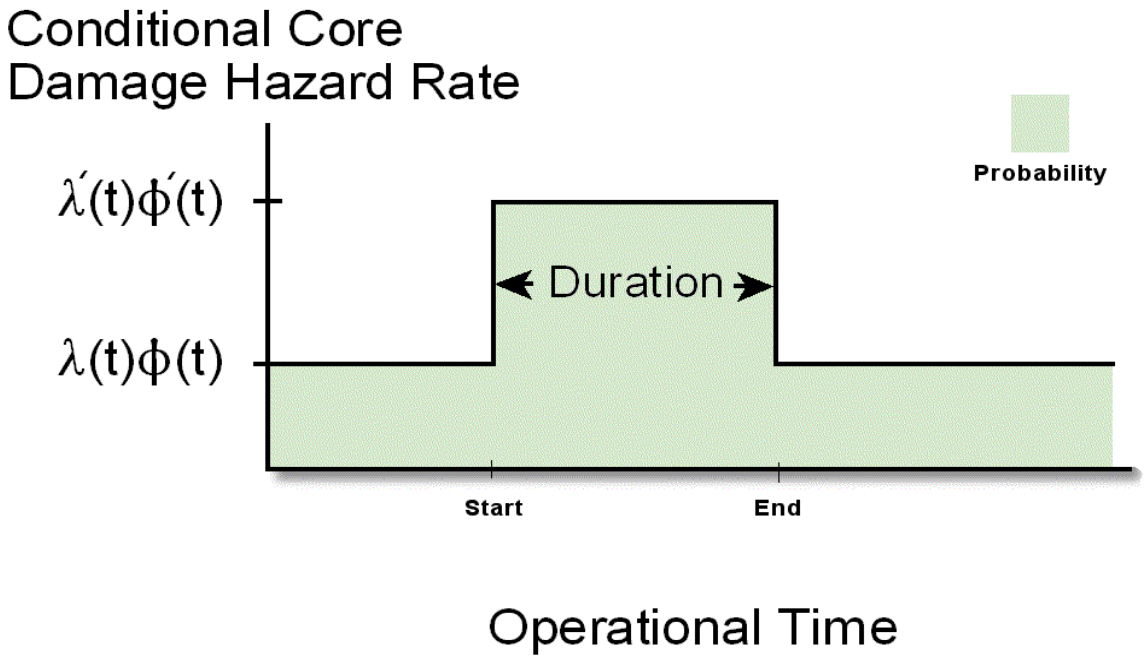
- State the appropriate risk measure for a condition assessment.

Section 4 Topics

Notes for this Section

4.1 Introduction

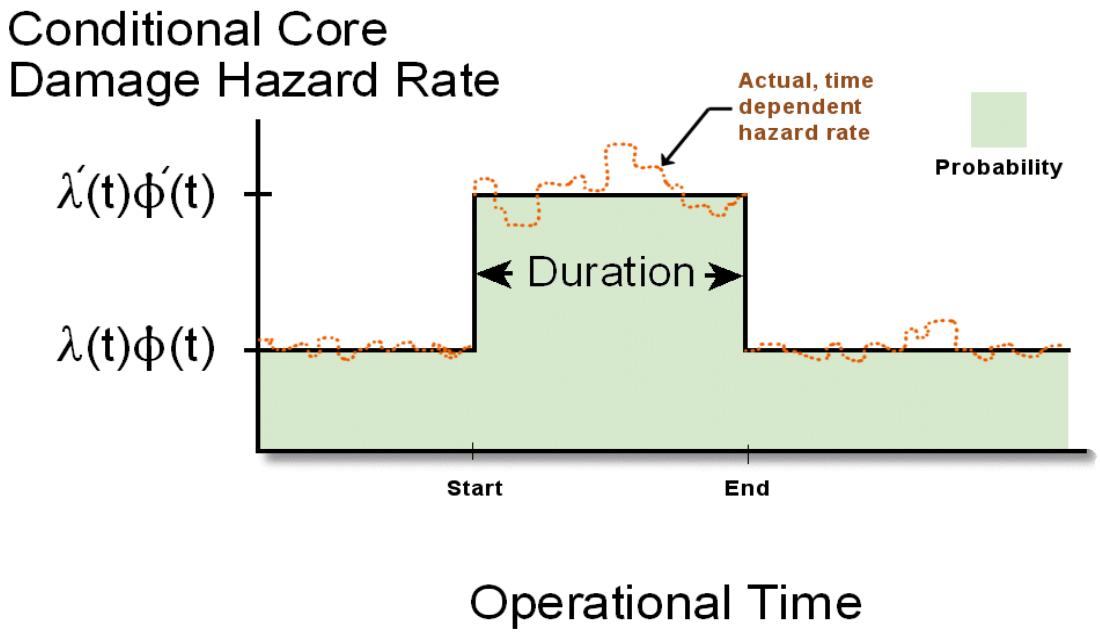
- Event evaluations are performed in order to quantify the risk due to a particular event.
    - ◊ For condition assessments, the risk arises due to
        - – A component or system (or more than one) being degraded or inoperable for a certain length of time, during which no initiating event occurred.
        - – The "length of time" is the duration over which the risk is calculated.



- Again, λ(t) is the initiating event rate and Φ(t) is the conditional probability of core damage given an initiating event.
    - ◊ The product of these two terms is the core damage frequency.

- The core damage frequency is assumed to be constant over the duration of the event.
  - ◊ This constant (λ' Φ') is the *conditional* risk result given by the PRA model.
  - ◊ If the configuration changes (say due to maintenance, testing, or other failures), then we have a new risk level.
    - – "Risk monitors" map individual plant configurations into the PRA over the course of days or weeks for use in outage planning.

      Note that risk monitors typically ***exclude*** basic events that represent test/maintenance outages as probabilities (i.e., the average unavailability over the year due to test/maintenance).
    - – Important component or system outages that occur over the entire duration of the event **will be** modeled. Incidental component outages (either risk-insignificant components or very short duration events) may not be modeled.
  - ◊ The time-varying core damage hazard rate is, for condition assessments, assumed to be constant over the duration of interest.

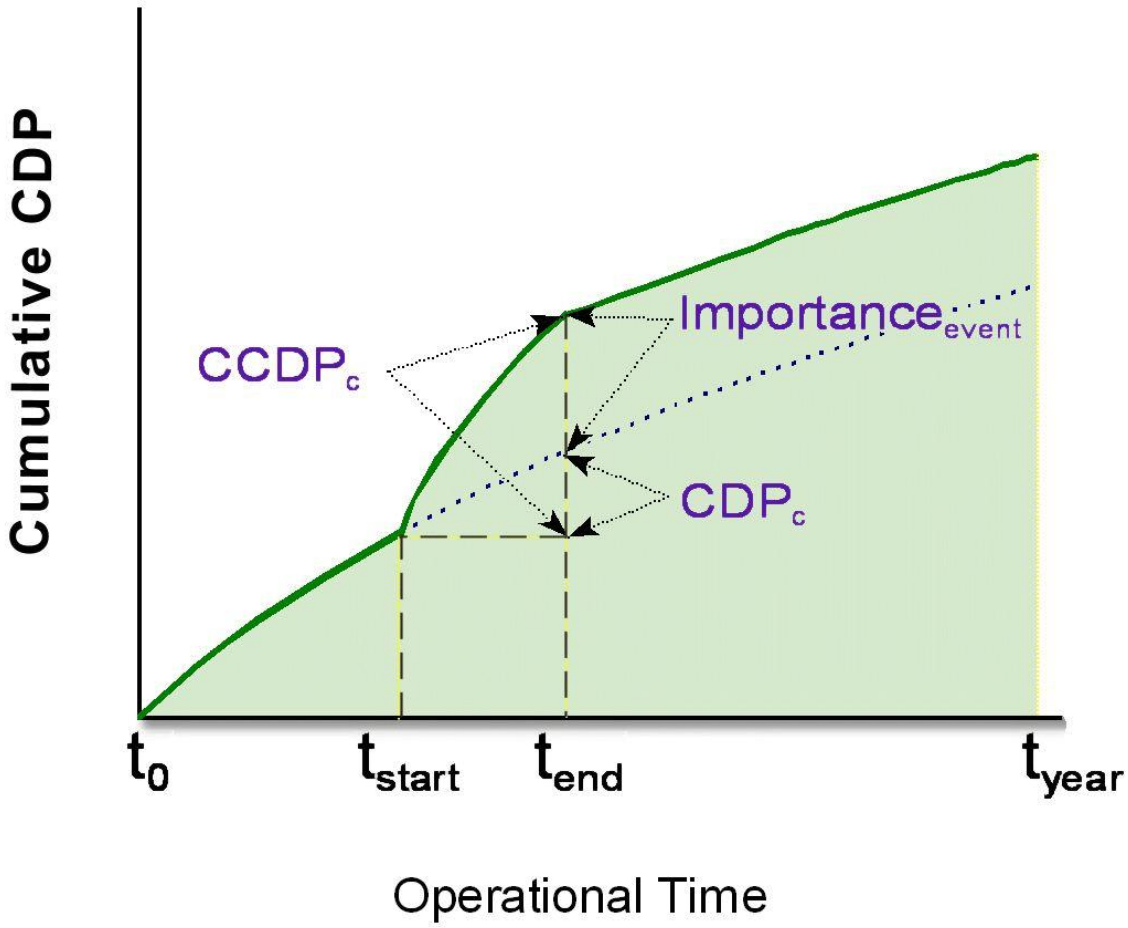


- For a condition assessment, a cumulative "risk profile" *could* be constructed based upon the results of the event evaluations that are performed.

◊ The cumulative, time-dependent CDP curve shown in the following figure is constructed by knowing that the cumulative failure probability is:

$$F(t) = 1 - e^{-\int_0^t \lambda(t)\phi(t)dt}$$

where we estimated the core damage frequency [λ'(t)Φ'(t)] from 0 to time *t*.



4.2 Treatment of Initiating Events for Condition Assessments

- For a condition assessment, it is assumed that none of the initiating events (as modeled in the PRA) actually occurred.

    ◊ Although no initiator occurred, there is still a probability that any of the initiating events could have occurred during the duration of the event.

        – Consequently, we need to account for this probability that an initiating event could have occurred.

    ◊ The initiator probabilities are necessary even if the event duration is very short compared to the expected arrival rates of the initiating events.

        – The probability of more than one initiator is usually negligible, but the calculation for the initiator probability accounts for such situations.

        – An initiator does not lead to core damage without subsequent failure of plant safety systems (hence the formulation of λΦ).

        – This calculation assumes that the initiator, if it occurred, would reveal the condition.

- Assuming that the arrival of an initiating event can be modeled as a standard Poisson (think random) process, we can estimate the probability of core damage as

$$P(\text{core damage}) = 1 - e^{-\int_0^T \lambda(t)\phi(t)\,dt}$$

$$P(\text{core damage}) = 1 - e^{-\lambda\phi T}$$

where:

λ(t) is the arrival rate of the initiating event (with units of inverse time)
Φ(t) is the probability of the accident sequence cut sets
T is the duration (with units of time).

This calculation assumes that λ(t) and Φ(t) are constant over time T.

◊ The approximation $(1 - e^{-\lambda\Phi T}) \approx \lambda\Phi T$ is valid for the equation above as long as the product λΦT has a value less than 0.1.

4.3 Treatment of Components for Condition Assessments

- The components or systems that are inoperable during the *entire* duration need to be evaluated in order to determine whether they are potentially recoverable.

    ◊ The treatment of components for condition assessments is identical to that presented for initiating event assessment (Section 3.3). Section 7 provides additional detail specific to non-recovery probability determination.

4.4 Treatment of Component Common Cause Failures

- The treatment of common cause failures is the same as that in the initiating event assessment section (Section 3.4). Section 6 provides additional detail specific to conditional common cause probability determination.

4.5 Appropriate Risk Measure for Condition Assessments

- The risk measure for **condition assessments** is the increase in core damage probability, or "event importance" (i.e., $\text{Importance}_{\text{event}}$).

$$\text{Importance}_{\text{cond}} = \text{CCDP} - \text{CDP}$$

where;
CCDP is the **conditional** core damage probability
CDP is the **nominal** core damage probability.

    ◊ This measure is conditional upon both

        – The probability of any initiating event occurring during the event duration.
        – Components, trains, or systems that are degraded or inoperable for the duration of the event.

- Both the CCDP and CDP are available from the evaluation.

    ◊ The CDP is the nominal core damage probability over the event duration.

        – No specific component outages are modeled in the CDP evaluation.
        – A risk monitor will typically have all test and maintenance unavailabilities set to zero for the CDP calculation.

- Component outages (specific to the incident) are modeled in the CCDP evaluation.

Summary:

When presented with a condition assessment, the results will generally be in the form of an "event (condition) importance."

At this point, let us review the two types of event evaluations

Item	Assessment Type	
	Initiating Event Assessment	**Condition Assessment**
Unique Attributes	Initiating Event HAPPENS (at a point in time)	One or more component/system are degraded or inoperable for some duration of time (t_2 - t_1) Initiating event did not occur
Treatment of Initiating Events	Set initiator to TRUE (or non-recovery probability) for the initiating event that occurred. Others initiators are set to FALSE.	CCDP = $1-e^{(-\Sigma\lambda_i \Phi_i T)}$ *where,* λ_i *= i'th initiator frequency* Φ_i *= P(CD | i'th initiator)* *T = duration of condition* Note that λ_i may increase from the nominal value if conditions impact likelihood of seeing an initiating event. For example, outage of one service water pump may increase the likelihood of losing the service water system.
Treatment of Components	Failed components –> TRUE and adjust CCF. Degraded components -> increased failure probability Non-failed components –> leave at their nominal failure probabilities	Failed components –> TRUE and adjust CCF. Degraded components -> increased failure probability Non-failed components –> leave at their nominal failure probabilities
Risk Metric	CCDP	CCDP - CDP

4.6 Workshop

5. EVENT EVALUATION AND SAPHIRE

Section 5 describes how SAPHIRE can be used to perform both initiating event and condition assessments.

Learning Objectives

– Demonstrate proficiency with SAPHIRE by performing workshop exercises related to an initiating event and condition assessment.

Section 5 Topics

5.1 Overview of Steps Involved in the Analysis
5.2 Steps for Event Evaluation in SAPHIRE
5.3 Modifying the Nominal PRA Model
5.4 Workshop

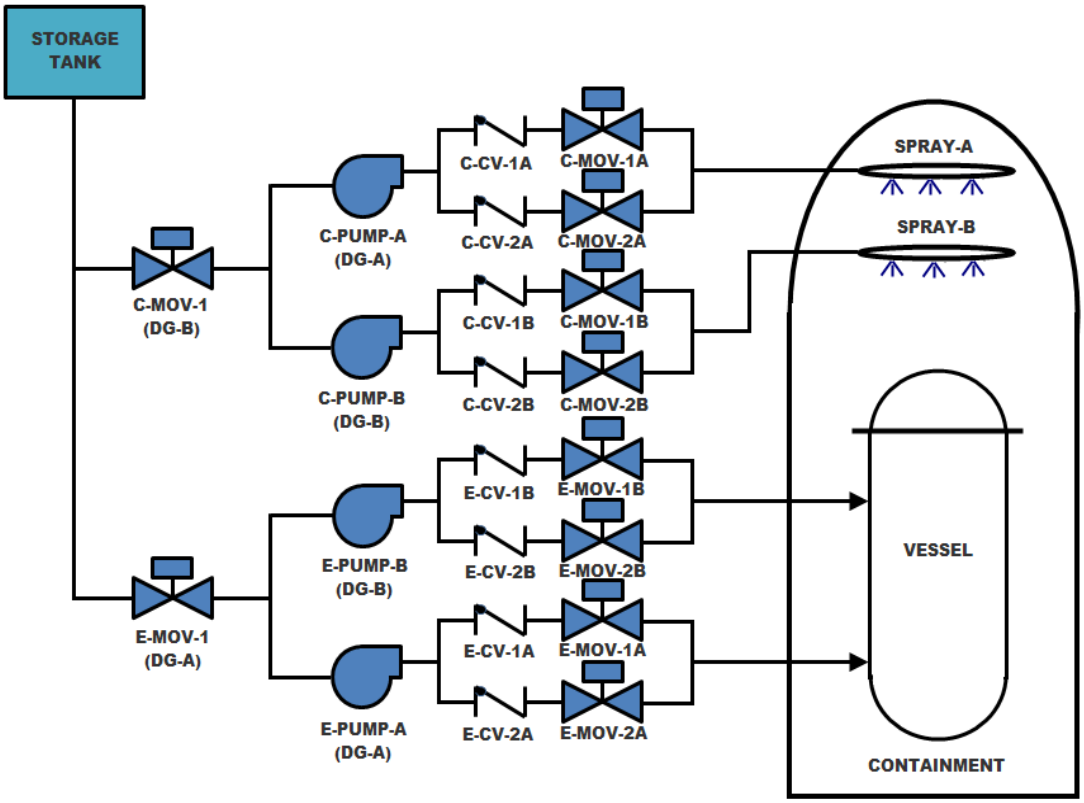
5.1 Overview of Steps Involved in the Analysis

- In this section, we will discuss how to use SAPHIRE to perform limited event assessments. We will demonstrate the steps involved, namely:

    1. Define the event assessment by constructing a "change set."
    2. Apply the change set to the data.
    3. Solve the applicable accident sequences.
    4. Report the results.

- Note that SAPHIRE reports accident sequence **frequency** (for the sequence analysis) – it is up to the analyst to calculate applicable probabilities (e.g., CCDP) using these frequencies. Later, we will see how the SAPHIRE Workspace automates this probability calculation.

- We will use the DEMO project. A simplified diagram of the plant modeled by the DEMO project is shown below. We will perform a condition assessment where DG-A is out of service for 876 hours (1/10th of a year).



5.2 Steps for Event Evaluation in SAPHIRE

- First, we need to make a change set in SAPHIRE. Change sets are "data filters" that allow us to adjust the nominal (or base) probabilities to new, case-specific values.

- We will use the DEMO project for this example, so make sure it is selected.

- In this example, we need to fail the DG-A basic event (EPS-DGN-FS-A). Note that DEMO has no recovery events, so we will ignore this adjustment in this example.

- To make the change set, select View and then check **Change Sets** so this list panel will show on the left side of SAPHIRE.

    ◊ To create a Change Set, double click the **New Change Set** and enter the Change Set name and description.

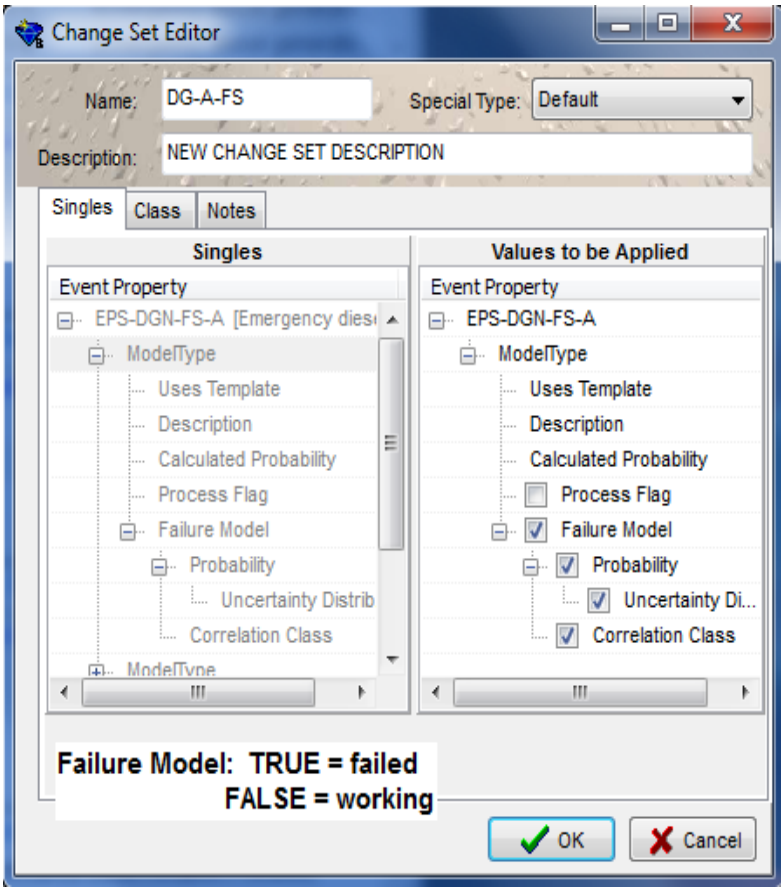
    ◊ To make a data change in the Change Set, drag the diesel generator basic event (EPS-DGN-FS-A) and drop it into the Single tab field.

    ◊ Now, click the basic event in the **Singles** field to expand out the options in the **Values to be Applied** field.

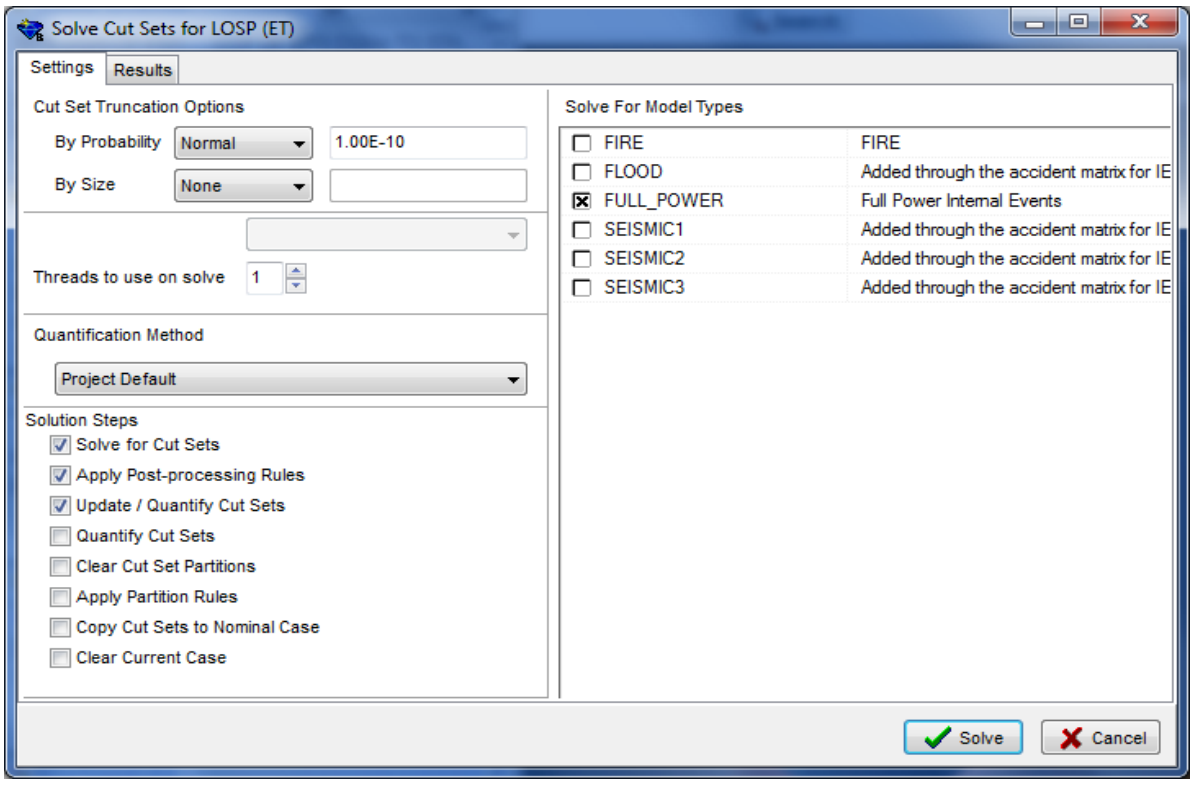
    ◊ In the **Values to be Applied** field check the Failure Model box and click the text field next to this option to get a drop down box.

    ◊ To fail the diesel generator, change the "Failure Model" to **TRUE (house event true)**. Click **OK** to exit and return to the list of change sets.

    ◊ At this point, we have made the change set and set the diesel generator fails to start to failed. We still need to "mark" the change set so we can use it.



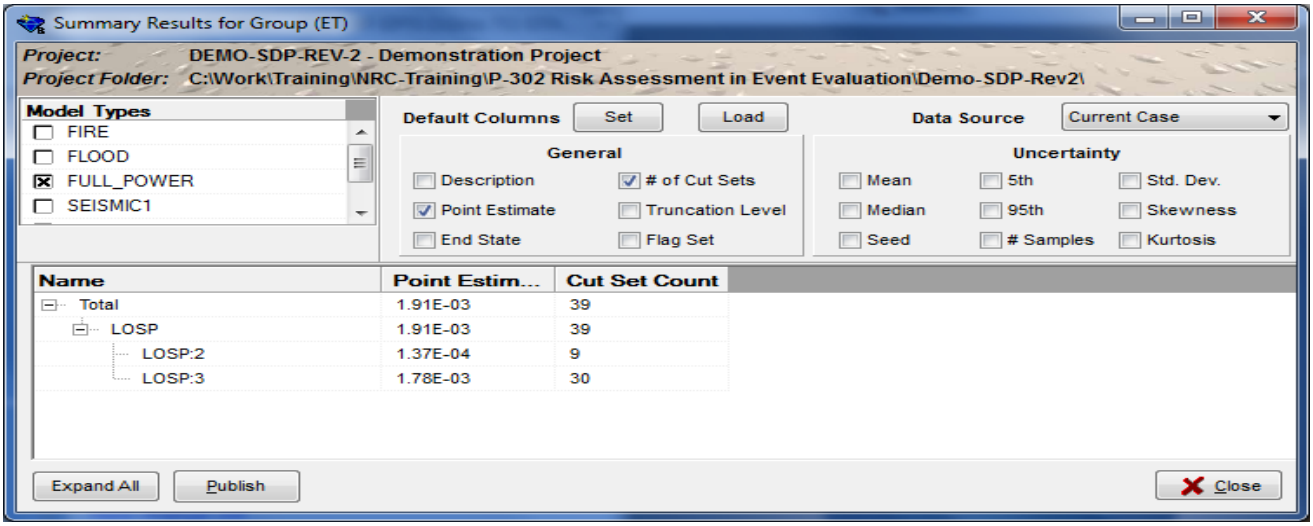
- To use a change set, the box in front of the change set needs to be selected.
    - ◊ Once the box is checked a number will appear.
    - ◊ Since we only have one change set, we sho**uld see the** number 1 next to the change set, indicating that it will be applied first. Once a number shows up the change set is invoked and the data change will be used in the cut set generation.
- Now we need to solve our accident sequences.
    - ◊ Highlight the LOSP event tree.
    - ◊ Click the right mouse button and then select the **Solve** option.
        - – Solve uses the event tree and fault tree logic associated with the sequences. The sequence frequency is quantified using the minimal cut set upper bound approximation.
        - – Accept the default solve options.



- ◊ Click the **Solve** button to solve the sequence minimal cut sets.

- We now need to view our results.

  ◊ With the event tree still highlighted, click the right mouse button and then select the **View Summary Results** option. A screen similar to that below should appear.



  ◊ The results of the analysis are shown above (Current Case).

    – This result is a *frequency*, a frequency of core damage, in units of per year.

  ◊ The nominal results of our PRA are shown when the Data Source drop down option is selected and "Nominal Case" is selected (Sequence 2 = 1.31E-05, Sequence 3 = 3.91E-05, and Total = 5.22E-05).

- The traditional risk measure for **condition assessments** is the “event importance” (i.e., $Importance_{event}$).

  ◊ Recall that the event importance for core damage is

$$Importance_{event} = CCDP - CDP$$

  Where : CCDP is the conditional core damage probability
  CDP is the nominal core damage probability.

    – So, how do we get the CCDP and CDP from the related frequencies?

- Recall that if we know the frequency of a Poisson process, we can calculate the probability of the associated event (say core damage) by

$$P(\text{core damage}) = 1 - \exp\left[-\int_0^T \lambda(t)\Phi(t)dt \right]$$
$$= 1 - \exp\left(-\lambda\Phi T\right)$$

Where: $\lambda\Phi$ is the core damage frequency.

◊ Consequently, one can find CCDP and CDP by:

$$CCDP = 1 - e^{-(1.91E-03/yr)(0.1yr)} = 1.91E-03$$

$$CDP = 1 - e^{-(5.22E-05/yr)(0.1yr)} = 5.22E-04$$

◊ And then...

$$\text{Importance}_{\text{event}} = 1.91\text{E-}03 - 5.22\text{E-}04 = 1.39\text{E-}03$$

5.3 Modifying the Nominal PRA Model

- In some situations, you may wish to modify the underlying or "nominal" PRA model.
    - ◊ For example, perhaps the frequency of transients is updated for the model...this frequency would replace the existing transient value.
    - ◊ For details of how to make this modification, refer to the SAPHIRE Basics course manual.
- In SAPHIRE, to change the nominal data, double click the basic event in the Basic Events list panel and then make the appropriate changes.

5.4 Workshop

6. TREATMENT OF COMMON-CAUSE EVENTS

Section 6 reviews common cause failure modeling in PRA, discusses the calculations performed by the CCF module in SAPHIRE, and describes adjustments to CCF probabilities used in event evaluation.

Learning Objectives

- Understand the Basic Parameter Model for common cause failure and the alpha-factor method used to quantify it in the SPAR models.
- Explain the guidelines for common cause failure probability adjustments for a two- or three-train system for the following cases:
  - ◊ Failure with common-cause potential,
  - ◊ Failure without common-cause potential (independent failure),
  - ◊ Component outage for preventive maintenance or testing.

Section 6 Topics

6.1 Introduction
6.2 Review of Basic Parameter Model and Alpha-Factor Method
6.3 Common Cause Issues for Event Evaluations
6.4 Adjusting CCF Probabilities
6.5 Workshop

Notes for this Section

Additional information on common-cause modeling can be found in the P-200 course material and in the RASP Handbook, Vol. 1.

6.1 Introduction

- Common cause failure modeling, a subset of dependent failure analysis, is covered in detail in the course *System Modeling Techniques for PRA (P-200)*.
    - ◊ Common cause failure analysis attempts to model failures of multiple components due to causes that are not captured explicitly in the PRA.
        - – Recall, for example, a power supply common to multiple components would be included in the PRA fault trees; this type of dependency is not a common cause failure.
    - ◊ Common cause failures frequently appear as one of the dominant failure events for redundant trains.
        - – Since nuclear power plants have high levels of redundancy, minimal cut sets containing common cause failures tend to be among the most dominant contributors to risk.
- Since the time of WASH-1400, several methods of common cause failure modeling have been proposed. These methods all rely on the Basic Parameter Model and include
    - ◊ Beta Factor method
    - ◊ Multiple Greek Letter method
    - ◊ Alpha Factor method
- Common cause modeling is an important issue for event assessment.
    - ◊ A component failure may impact the probability that other like components could fail due a common cause mechanism. Thus, we need to estimate the "conditional" common cause failure probability for the impacted group of redundant components.
    - ◊ Testing and maintenance outages will affect the common cause failure probabilities.
    - ◊ The nominal PRA value of a common cause basic event is valid only for the nominal configuration.
        - – Changes to component configuration (e.g., failure, test, maintenance) impacts the common-cause potential.

- When a component is disabled (either failed or purposely removed from service), the context of the PRA changes.

    ◊ In general, the disabled component will fall into one of three categories.

    1. Actual or potential ***common cause*** failure, or information is insufficient to judge (default category)

    2. A ***testing or preventive maintenance*** outage (not due to a failure)

    3. ***Independent failure***. (requires conclusive evidence to justify).

6.2 Review of Basic Parameter Model and Alpha-Factor Method

A common cause component group (CCCG) is a group of redundant components (redundant in design, function, environment, etc.) judged to be vulnerable to common cause failure. The Basic Parameter Model partitions the total failure probability of each component in the CCCG into independent and common cause contributors. We illustrate this partitioning for a CCCG with three components:

$$A_T = A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC}$$
$$B_T = B_I \cup C_{AB} \cup C_{BC} \cup C_{ABC}$$
$$C_T = C_I \cup C_{AC} \cup C_{BC} \cup C_{ABC}$$

If the success criterion for the CCCG is that one of the three components must operate, then the minimal cut sets for the CCCG are

$\{A_I, B_I, C_I\}$, $\{A_I, C_{BC}\}$, $\{B_I, C_{AC}\}$, $\{C_I, C_{AB}\}$, and $\{C_{ABC}\}$.

The Basic Parameter Model assumes that the probabilities of similar events involving similar components are the same. This approach takes advantage of the physical symmetries associated with identical redundant components in reducing the number of parameters that need to be quantified. Thus, we set $A_I = B_I = C_I = Q_1$. Similarly, we have $C_{AB} = C_{AC} = C_{BC} = Q_2$ and $C_{ABC} = Q_3$. The failure probability for the CCCG can then be written as

$$Q_1^3 + 3Q_1Q_2 + Q_3$$

Had the success criterion been two-out-of-three, the failure probability for the CCCG would become

$$3Q_1^2 + 3Q_2 + Q_3$$

The CCF plug-in module in SAPHIRE uses the second two terms in these equations as the probability of the CCF event for that CCCG.

The Q_ks are not estimated directly. Rather, more easily estimated parameters are introduced. This leads to the various approaches listed in the Introduction (e.g., beta factor). The SPAR models use the most recent of these, the ***alpha-factor method***.

The parameters in the alpha-factor method are Q_t, the total failure probability for a component, defined as in the Basic Parameter Model, and α_k, which is the fraction of failures in the CCCG that involve failure of k components. Thus, α_1 is the fraction of failures that are independent (no common-cause), α_2 is the fraction of failures in which two components fail due to common cause, etc.

For a staggered-testing scheme, that is, one in which the components in the CCCG are not all tested at the same time, one can write the Q_ks as follows, where m is the number of components in the CCCG:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t$$

For a non-staggered testing scheme, that is, one in which the components in the CCCG are tested at the same (or close) time, one can write the Q_ks as follows, where m is the number of components in the CCCG:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \qquad \text{where: } \binom{m-1}{k-1} = \frac{(m-1)!}{(k-1)!\,(m-1)!},\ \alpha_t = \sum_{i=1}^{m} k\alpha_k$$

The inputs to the CCF plug-in in the current version of SAPHIRE are the testing scheme (default is staggered for SPAR models), the size of the CCCG (m), the failure criterion, Q_t, and the α_ks. SAPHIRE then automatically calculates the probability of the CCF event, which represents failure of all components in the CCCG, using the above equations.

6.3 Common Cause Issues for Event Evaluations

- Frequently, in the application of many common cause models, all the combinations of common cause and independent failures may not be included.

    ◊ Including all combinations increases the complexity of the models while only increasing the common cause probability by a few percent.

    ◊ Also, most PRAs do not include common cause events for all components. For example, in the SPAR models, the components that do have common cause events include:

    - Air operated valves
    - Diesel generators
    - Heat exchangers
    - Motor driven pumps
    - Motor operated valves
    - Turbine driven pumps

    ◊ While components that may not have common cause events include:

    - Power operated valves
    - Relief valves
    - Safety valves

- When performing an event evaluation, we need to worry about three different cases.

    I. ***Common cause*** failure or insufficient information

    - These affect the inoperable component but the failure mechanism may have the potential to impact the other redundant components.

    II. ***Independent*** failure

    - These effectively reduce the redundancy of the system. In other words, we have one less redundant component, but the remaining components may still fail due to either independent failures or a common cause failure.

    III. ***Testing/Maintenance*** outage(s)

    - Scheduled preventive maintenance and testing outages fall into this category.

- Like the "independent failure" case above, these outages reduce the redundancy of the system due to the component(s) being made unavailable.

- Testing or maintenance caused failures ***do not*** belong in this category and would generally be put into another category.

- In practice, it is difficult to distinguish between a component that has suffered a potential common cause failure and one that has failed independently.

  ◊ Assuming a common-cause type of failure (**Case I**) leads to the highest (most conservative) CCDP or event importance.

  ◊ Assuming independent failure (**Case II**) or test/maintenance outages (**Case III**) leads to the lowest (least conservative) CCDP or event importance.

- One must make a judgment call as to the potential failure scenario on each event evaluation.

  ◊ As a default, one should assume **Case I** is applicable.

  ◊ If the failure definitely could not have been shared by the other redundant components (if the situation happened again and again), then **Case II** is applicable.

  ◊ The NRC is working on guidance to help distinguish independent failures. A NUREG/CR should be published later this year and guidance will be incorporated into the RASP Handbook.

  ◊ Further, one should consider running a sensitivity calculation where the common cause assumption is varied in order to determine the potential impact on the overall results.

6.4 Adjusting CCF Probabilities

In the SPAR models, some components have more than one failure mode in addition to test and maintenance unavailability. For example, a component that must change state and perform a function for a specified period of time will have two additional failure modes: failure to start and failure to run. There will be a CCF event for both of these failure modes and this complicates the algebra in what follows.

6.4.1 Two Trains - Failure with Common Cause Potential

For a two-train CCCG, letting R denote failure to run, and S failure to start, we have the following nominal minimal cut sets:

$$S = \left\{ A_I^R B_I^R, A_I^S B_I^S, A_I^R B_I^S, A_I^S B_I^R, C_{AB}^R, C_{AB}^S \right\}$$

The nominal CCF probability is thus

$$P(CCF) = Q_2^S + Q_2^R$$

Assume that component A fails to start, and we cannot conclude that the failure was independent of component B. Applying the definition of conditional probability, we have

$$P(S \mid A_t^s) = \frac{P(S \cap A_t^s)}{P(A_t^s)}$$
$$= \frac{P(A_I^S B_I^S \cup A_I^S B_I^R \cup A_I^S C_{AB}^R \cup C_{AB}^S)}{P(A_t^s)}$$
$$= \frac{(Q_1^S)^2}{Q_t^S} + \frac{Q_1^S Q_1^R}{Q_t^S} + \frac{Q_1^S Q_2^R}{Q_T^S} + \frac{Q_2^S}{Q_t^S}$$
$$= \alpha_1^S \left(Q_1^S + Q_1^R \right) + \alpha_1^S Q_2^R + \alpha_2^S$$

So the conditional CCF probability becomes approximately α_2^S.

Intuitively, what has happened is that the observed failure of A to start, with CCF potential, has not affected the total failure probability of component B, which includes C^R_{AB}. Even though we saw a failure to start of component A, there may be causes that would result in a failure to run, which are shared with component B, and contribute to the total failure probability of B. SAPHIRE 8 will eventually automate this adjustment. For now, the analyst must modify basic events as follows:

- ◊ Set the independent basic event representing the observed failure to TRUE
- ◊ Set the CCF basic event for the unobserved failure mode (failure to run in our example) to FALSE. Without this second adjustment, SAPHIRE will keep the fails-to-run CCF event at its nominal value, which is incorrect, as there cannot be both common-cause failure to start and failure to run.

Example Calculation

- In the RHR fault tree in the Generic PWR SPAR model, there are CCF basic events called RHR-MDP-CF-START and RHR-MDP-CF-RUN.
  - ◊ The event RHR-MDP-CF-START would have a nominal failure probability of P(ZA-MDP-FS-02A02)*P(RHR-MDP-FS-1A) = 6.27E-5.
  - ◊ What would P(RHR-MDP-CF-START) be if we observed a failure of the B RHR pump to start during a test, and we could not rule out the potential for CCF of the A pump?

P(RHR-MDP-CF-START) should become P(ZA-MDP-FS-02A02) = 4.18E-2.

We would obtain this by setting RHR-MDP-FS-1B to TRUE and RHR-MDP-CF-RUN to FALSE.

6.4.2 Two Train – Independent Failure of One Component

Next assume that we observe a failure to start of component A, but where there is no potential for CCF. Now we must condition on an observed ***independent*** failure of A to start. Again applying the definition of conditional probability, we have

$$P(S \mid A_I^S) = \frac{P(A_I^S B_I^S \cup A_I^S B_I^R + A_I^s C_{AB}^R)}{P(A_I^S)}$$
$$= P(A_I^S) + P(B_I^S) + P(C_{AB}^R) = Q_1^S + Q_1^R + Q_2^R$$
$$= Q_1^S + Q_t^R$$

Because the failure was independent, any cut sets involving CCF for failure to start are removed. Thus, we are left with an independent failure of B to start and a total failure of B to run.

In the current version of SAPHIRE (without using the RASP CCF module), the analyst must set the independent event representing the observed failure to TRUE and **both** CCF events to FALSE. Both CCF events are set to FALSE because the SPAR models use Q_t rather than Q_1 for failure of B, so we have to avoid double-counting the CCF for failure to run. In our earlier RHR example, if the failure of the B pump to start was judged to be independent, we again set RHR-MDP-FS-1B to TRUE.

6.4.3 Two Trains - Test or Maintenance Outage

Finally, if one of the components is out of service for preventive test and maintenance, then we cannot observe a failure of that component to start or run. Assuming this is the A component, this reduces the level of redundancy by one, so the probability that the CCCG fails becomes just $B_t^R + B_t^S$. Removing component A from service has not affected the total failure probability of component B: $B_t = B_I + C_{AB}$. Note that C_{AB} still contributes to B_t. Even though we cannot observe CCF of both components with one out of service for test or maintenance, the causes that could lead to CCF are still present and contribute to the total failure probability of the remaining component.

To model this in SAPHIRE, the analyst would, continuing the RHR example from earlier, would set the test-and-maintenance event for pump A (RHR-MDP-TM-1A) to 1.0 (not TRUE), and set both CCF events to FALSE. Next, generate cut sets. Setting the test-and-maintenance event to 1.0 allows recovery rules to be applied to properly remove combinations that would be disallowed by

Technical Specifications. However, the resulting cut sets are not minimal. To get minimal cut sets, go back and set RHR-MDP-TM-1A to TRUE and perform a cut set update; do not regenerate cut sets.

6.4.4 Three Trains - Potential CCF

For a three-train CCCG with two failure modes, the algebra is more complicated, but the basic principles still apply. For a one-of-three success criterion, the minimal cut sets for the CCCG are

$$S = \left\{ \begin{array}{l} A_I^R B_I^R C_I^R, A_I^S B_I^R C_I^R, A_I^R B_I^S C_I^R, A_I^R B_I^R C_I^S, A_I^R B_I^S C_I^S, A_I^S B_I^R C_I^S, A_I^S B_I^S C_I^R, A_I^S B_I^S C_I^S, \\ A_I^R C_{BC}^R, B_I^R C_{AC}^R, C_I^R C_{AB}^R, A_I^S C_{BC}^S, B_I^S C_{AC}^S, C_I^S C_{AB}^S, A_I^R C_{BC}^S, A_I^S C_{BC}^R, B_I^R C_{AC}^S, B_I^S C_{AC}^R, \\ C_I^R C_{AB}^S, C_I^S C_{AB}^R, C_{ABC}^S, C_{ABC}^R \end{array} \right\}$$

Thus, the nominal CCF probability is given by

$$P(CCF) = 3Q_1^R Q_2^R + 3Q_1^S Q_2^S + 3Q_1^R Q_2^S + 3Q_1^S Q_2^R + Q_3^S + Q_3^R$$

One thing to notice about these cut sets is the presence of "failure mode cross-products," such as $A_I^R C_{BC}^S$. Such terms are not included in the calculation of CCF probability by the current SAPHIRE plug-in. If we observe a failure to start of component A, with CCF potential, we apply the definition of conditional probability, as before. After considerable Boolean algebra, the cut sets above reduce to those shown in the following table.

Table 1 Results for CCCG of size 3 conditioned on failure to start of component A with CCF potential

Number	Cut Set	Cut Set Probability	Conditional Probability
1	S-ABC	2.325E−05	4.65E-03
2	A-S, B-R, C-R	6.607E−07	1.32E-04
3	A-S, R-BC	6.530E−07	1.31E-04
4	A-S, R-ABC	4.340E−07	8.68E-05
5	B-R, S-AC	3.886E−07	7.77E-05
6	C-R, S-AB	3.886E−07	7.77E-05
7	A-S, B-S, C-R	2.790E−07	5.58E-05
8	A-S, B-R, C-S	2.790E−07	5.58E-05
9	A-S, S-BC	1.645E−07	3.29E-05
10	B-S, S-AC	1.645E−07	3.29E-05
11	C-S, S-AB	1.645E−07	3.29E-05
12	A-S, B-S, C-S	1.184E−07	2.37E-05
13	A-S, C-R, R-AB	7.575E−09	1.52E-06
14	A-S, B-R, R-AC	7.575E−09	1.52E-06
15	R-AB, S-AC	4.455E−09	8.91E-07
16	R-BC, S-AC	4.455E−09	8.91E-07
17	R-AC, S-AB	4.455E−09	8.91E-07
18	R-BC, S-AB	4.455E−09	8.91E-07
19	A-S, C-S, R-AB	3.206E−09	6.41E-07
20	A-S, B-S, R-AC	3.206E−09	6.41E-07
21	R-ABC, S-AC	2.961E−09	5.92E-07
22	R-ABC, S-AB	2.961E−09	5.92E-07
Total		**2.699E−05**	**5.400E−03**

Dividing through by A_t^S gives the conditional probability of failure for the CCCG.

The CCF probability calculated by the SAPHIRE 8 (compound event) plug-in does not include all of the terms in this equation; the cross-products are dropped. The new CCF module (RASP failure model) in Ver. 8 is being designed to perform all the necessary calculations automatically.

To approximate the correct answer using the current SAPHIRE plug-in, the analyst must set the observed independent failure event to TRUE and the independent failure event for the unobserved failure mode to 1.0.

Example Calculation

- In the DEMO model, there are CCF basic events called CCS-MDP-CF-FS1 and CCS-MDP-CF-FR1 (created just for this example).

  ◊ The event CCS-MDP-CF-FS would have a nominal failure probability of

  $$\frac{3}{2}\alpha_1^S\alpha_2^S\left(Q_t^S\right)^2+\alpha_3^S Q_t^S$$

  Using the values in the DEMO model, this equation gives a nominal probability of 4.74E-05. The analogous expression for failure to run gives a nominal probability for event CCS-MDP-CF-FR1 of 1.52E-06.

  ◊ What would P(CCS-MDP-CF-FS1) become if we observed a failure of the B HPI pump to start during a test, and we could not rule out the potential for CCF of the A or C pumps?

  Set CCS-MDP-FS-A to TRUE and CCS-MDP-FR-B to 1.0. The adjusted value of CCS-MDP-CF-FS1 is 1.58E-02. Note also that the value of CCS-MDP-CF-FR1 has increased slightly, to 3.09E-06. Setting CCS-MDP-FR-B to 1.0 has caused the CCF probability for failure to run to be adjusted to $2Q_1Q_2 + Q_2 + Q_3$.

6.4.5 Three Trains - Test or Maintenance Outage

If we have one train in test and maintenance, say the A train, the cut sets for the CCCG reduce to the following:

$$S=\left\{\begin{array}{l} B_I^R C_I^R, B_I^S C_I^R, B_I^R C_I^S, B_I^S C_I^S, \\ C_{BC}^R, B_I^R C_{AC}^R, C_I^R C_{AB}^R, C_{BC}^S, B_I^S C_{AC}^S, \\ C_I^S C_{AB}^S, B_I^R C_{AC}^S, B_I^S C_{AC}^R, C_I^R C_{AB}^S, C_I^S C_{AB}^R, \\ C_{ABC}^S, C_{ABC}^R \end{array}\right\}$$

Because the test-and-maintenance basic events are not inputs to the current SAPHIRE CCF plug-in, SAPHIRE will not automatically adjust the CCF probability. In most cases, the increase over the nominal value will be small. If the analyst wishes to reflect the change in CCF probability, they will have to input the adjusted value manually. As above, first set the test-and-maintenance event to 1.0, so that recovery rules will be applied correctly, then set it to TRUE and perform a cut set update to produce minimal cut sets. In the current Ver. 8 of SAPHIRE, these adjustments are performed via the multipass evaluation, which does this automatically.

6.4.6 Three Trains - Independent Failure

If the observed failure of a component is judged to be independent, so there is no potential for CCF of other components in the CCCG, the cut sets reduce considerably from the nominal situation. Assume we have observed an independent failure to start of component A. The cut sets for failure of the CCCG become

$$S \cap A_I^S = A_I^S B_I^R C_I^R \cup A_I^S B_I^R C_I^S \cup A_I^S B_I^S C_I^R \cup A_I^S B_I^S C_I^S \cup A_I^S B_I^R C_{AC}^R \cup A_I^S C_I^R C_{AB}^R \cup A_I^S C_{BC}^S \cup A_I^S C_{BC}^R \cup A_I^S B_I^S C_{AC}^R \cup A_I^S C_I^S C_{AB}^R \cup A_I^S C_{ABC}^R$$

In deriving this result we have applied the assumption that the Basic Parameter Model constitutes a partition of each failure mode. This leads to the elimination of cut sets such as $A_I^S C_I^R C_{AB}^S$.

The results of applying this calculation to our size-three example above are shown in the table below.

Table 2 Results for CCCG of size 3 conditioned on independent failure to start of component A

Number	Cut Sets	Cut Set Probability	Conditional Probability
1	A-S, B-R, C-R	6.607E−07	1.35E-04
2	A-S, R-BC	6.530E−07	1.33E-04
3	A-S, R-ABC	4.340E−07	8.84E-05
4	A-S, B-S, C-R	2.797E−07	5.70E-05
5	A-S, B-R, C-S	2.797E−07	5.70E-05
6	A-S, S-BC	1.645E−07	3.35E-05
7	A-S, B-S, C-S	1.184E−07	2.41E-05
8	A-S, C-R, R-AB	7.575E−09	1.54E-06
9	A-S, B-R, R-AC	7.575E−09	1.54E-06
10	A-S, C-S, R-AB	3.206E−09	6.53E-07
11	A-S, B-S, R-AC	3.206E−09	6.53E-07
Total		**2.61E−06**	**5.32E−04**

In the current version of SAPHIRE, this can be approximated by setting the independent basic events for both failure modes to 1.0. Note that this will result in non-minimal cut sets. The analyst will have to ensure that the results are reasonable. Note that, as for the test-and-maintenance case above, the increase over the nominal CCF probability will generally be small.

6.5 Workshop

7. TREATMENT OF RECOVERY EVENTS

Section 7 describes the recovery analysis methods used in event evaluation. Recovery analysis estimates the probability that a component that has failed will not be restored. Recovery modeling is applicable to both initiating events and component failures.

Learning Objectives

- Understand the two categories of SPAR recovery modeling.
- Understand recovery for SPAR initiating events.
- Describe the four categories of LOOP events considered by the SPAR models.

Section 7 Topics

7.1 Introduction
7.2 Recovery of Initiating Events
7.3 Recovery of System/Component failures
7.4 Workshop

Notes for this Section

RCP reactor coolant pump

7.1 Introduction

"Recovery analysis" is the process of estimating the probability that a failed component is not restored. As such, it is more appropriately called "nonrecovery analysis" (i.e., the probability that an operator does not restore the system or component).

- Event evaluation recovery modeling is broken down into two general categories:

1. Recovery of initiating events (IEs). In the SPAR models, non-recovery probability is factored into the estimate of IE frequency for all initiators except LOOP.

2. Recovery of system failures. We have different types of recovery analysis, including:

    ◊ Recovery of system failures using the SPAR-H methodology

    ◊ Recovery of AC power system components

    ◊ Modeling of reactor coolant pump (RCP) seal LOCA related events that are LOOP duration-dependent.

- In general, there are two methods of modeling recovery:

    1. One may include nonrecovery evens in the logic models (fault or event trees). Thus, the basic events representing nonrecovery are distributed in the models just like other basic events.

        - Alternatively, the probability of nonrecovery may be included in the basic event's failure probability. The basic event would then represent the component failing AND the component is not recovered.

    2. One may want to append recovery events to the accident sequence cut sets, where recovery rules modify the cut sets after they have been generated from the logic models.

        - Recovery rules are discussed extensively in the Advanced SAPHIRE course. Note that the SPAR Rev. 3 models use both of these approaches, as do many of the plant PRA models.

- Once recovery is applied to the model, the hard work begins, because you must estimate its probability. In the human reliability analysis (HRA) course (P-203), you will discuss methods used to estimate nonrecovery probabilities.

7.2 Recovery of Initiating Events

The General Model

- A general IE model defines the initiator frequency as

$$\lambda_{IE} = \lambda \cdot \mathbf{P(IE\ not\ recovered\ during\ time\ t_{short})}$$

  - ◊ λ is rate at which events of type IE are observed.
  - ◊ t_{short} is the time available before reactor coolant boil-off uncovers the reactor core. The interval t_{short} is plant specific and generally has a value close to 0.5 hours.

- Note that recovering events like IE-LOCA and IE-LOOP leads to a transient. The recovered sequences are not modeled because the resulting sequences would be of low probability compared to the existing TRAN sequences.

- In the SPAR models, the IE nonrecovery probability is embedded in the frequency parameter (λ_{IE}).

LOOP Nonrecovery Probabilities

The SPAR 3+ models use a SAPHIRE "plug-in" for LOOP recovery – this calculation relies on basic events in the database to calculate the LOOP frequencies and offsite power nonrecovery probabilities.

- In the SPAR models the LOOP initiating event frequency (λ_T) is the sum of the frequencies of four individual LOOP categories:

$$\lambda_T = \sum_{i=1}^{4} \lambda_i$$

- The four LOOP categories are:

  1. *Plant-centered* loss of offsite power. Failures include hardware failures, design deficiencies, human errors in maintenance and switching failures. Can be recovered by switching or repairing equipment.

  2. Switchyard-centered loss of offsite power. Failures that are caused by component failures or human actions in the plant switchyard.

3. *Grid-related* loss of offsite power. Failures resulting from grid disturbances. Usually an unanticipated grid weakness, including physical disturbances of transmission lines (e.g., brush fires, earthquakes).

4. *Weather-related* loss of offsite power. Failures resulting from major storms, tornados, hurricanes, high winds, etc.

Table 3-1. Plant-level LOOP frequencies.

		Plant-Level LOOP Frequency				
Mode	LOOP Category	Data Period	Events	Reactor Critical or Shutdown Years	Mean Frequency[a]	Frequency Units[b]
Critical operation	Plant centered[c]	1997–2004	1	724.3	2.07E−03	/rcry
	Switchyard centered[c]	1997–2004	7	724.3	1.04E−02	/rcry
	Grid related	1997–2004	13	724.3	1.86E−02	/rcry
	Weather related	1997–2004	3	724.3	4.83E−03	/rcry
	All	1997–2004	—	—	3.59E−02	/rcry
Shutdown operation	Plant centered[d]	1986–2004	19	383.2	5.09E−02	/rsy
	Switchyard centered[d]	1986–2004	38	383.2	1.00E−01	/rsy
	Grid related	1986–2004	3	383.2	9.13E−03	/rsy
	Weather related	1986–2004	13	383.2	3.52E−02	/rsy
	All	1986–2004	—	—	1.96E−01	/rsy

a. The mean is a Bayesian update using a Jeffreys prior. Mean = (0.5 + events)/(critical or shutdown years).

b. The frequency units are per reactor critical year (/rcry) or per reactor shutdown year (/rsy).

c. For risk studies that combine plant-centered and switchyard-centered LOOPs, the mean frequencies should be added, resulting in 1.25E−2/rcry for the combined category.

d. For risk studies that combine plant-centered and switchyard-centered LOOPs, the mean frequencies should be added, resulting in 1.51E−1/rsy for the combined category.

- The SPAR model event trees include offsite power nonrecovery events. The expression used for calculating the probability of failing to recover offsite power is given by

$$\mathbf{P_{OPRF}}(t_{long} \mid t_{short}) = \mathbf{P}(\mathbf{L} > t_{long} \mid \mathbf{L} > t_{short})$$

where;

L is the duration of a LOOP

t_{long} is a sequence-dependent time requirement that is greater than t_{short}

The most common application is to station blackout sequences (SBO) where

t_{long} = either a battery depletion time or a core uncovery time.

t_{short} = short-term recovery interval based on the time to uncover the reactor core if no safety systems function

In the SPAR models t_{short} is most often zero unless there are multiple failures to recover offsite power events in a given sequence. In these sequences the first event calculation would use a t_{short} of zero and the remaining power recovery failure probabilities would be conditional on the previous failure event.

- We generalized the SPAR recovery so that the probabilities can be calculated when LOOP frequency and LOOP recovery information are divided into plant, switchyard, grid, and weather subclasses by frequency-weighting the class probabilities as follows

$$P_{OPRF}(t_{long} \mid t_{short}) = \frac{1}{\lambda_T} \sum_{i=1}^{n} \lambda_i \frac{(1 - F_{L_i}(t_{long}))}{(1 - F_{L_i}(t_{short}))}$$

where F_L is the distribution of durations (length of time in which offsite power is gone) for the i'th category. Note that F is a cumulative distribution function.

- The model for the LOOP duration for a particular category is a lognormal distribution:

$$f_i(t) = \frac{1}{t\sqrt{2\pi}\sigma_i} \exp\left[-\frac{(\ln t - \mu_i)^2}{2\sigma_i^2} \right]$$

The values of μ and σ for the four LOOP categories can be found from the information shown below, which is taken from NUREG/CR-6890.[4]

Table 4-2. Probability of exceedance curve fit uncertainty parameters for critical and shutdown operation.

LOOP Category	Curve Fit Parameter	Curve Fit Parameter Mean	Underlying Distribution for Curve Fit Parameter	Mean[a]	Error Factor[a]
Plant Centered	Median	0.468	Lognormal	0.468	1.463
	Error Factor	8.306	Lognormal	8.306	1.556
Switchyard Centered	Median	0.677	Lognormal	0.677	1.297
	Error Factor	7.895	Lognormal	7.895	1. 354
Grid Related	Median	1.350	Lognormal	1.350	1.658
	Error Factor	5.759	Lognormal	5.759	1.800
Weather Related	Median	2.211	Lognormal	2.211	2.321
	Error Factor	26.071	Lognormal	26.071	2.662

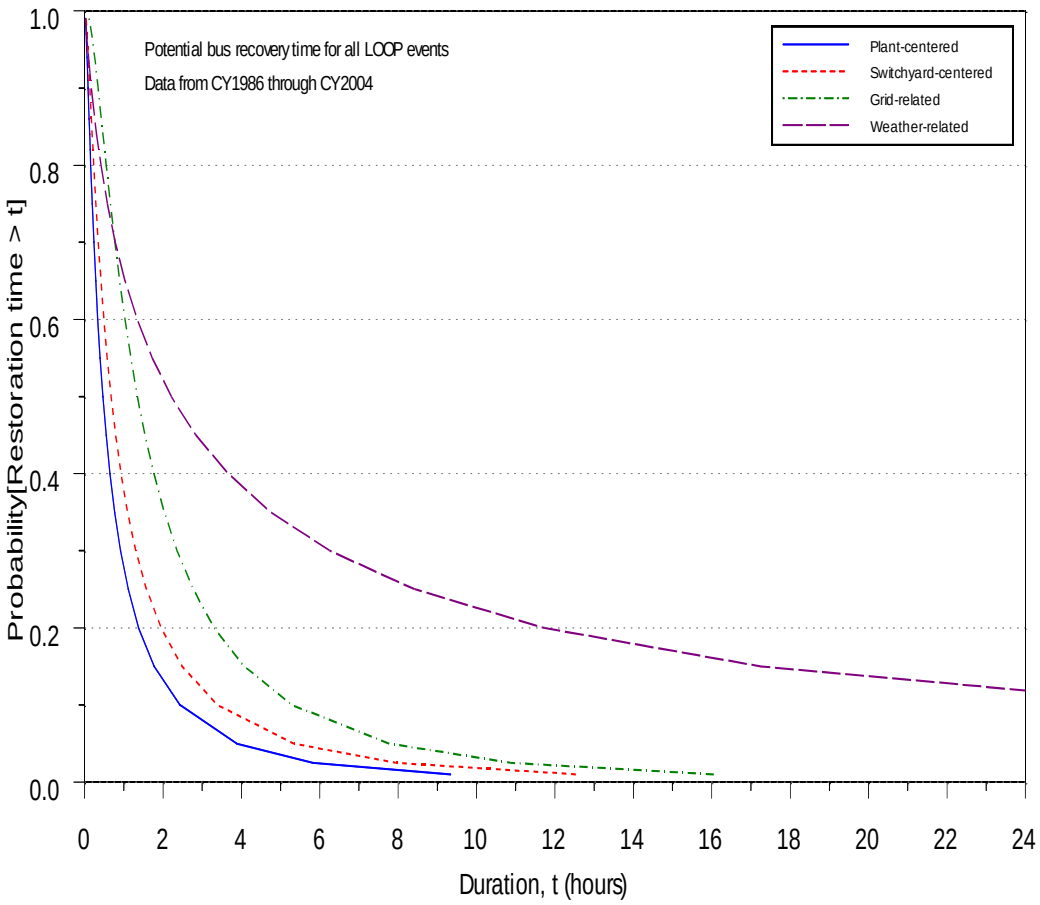
a. To perform an uncertainty analysis, the lognormal distributions are first sampled to obtain values for the curve fit parameters, which are then used to determine a sample estimate for the nonrecovery probability.

For each of the four categories, μ is given by the natural logarithm of the median. For example, for a plant-centered LOOP, we find μ = ln(0.468) = -0.759. The other parameter, σ, is given by ln(Error Factor)/1.645. For a plant-centered LOOP, we would find σ = ln(8.306)/1.645 = 1.287. The table below converts the information above into values for μ and σ.

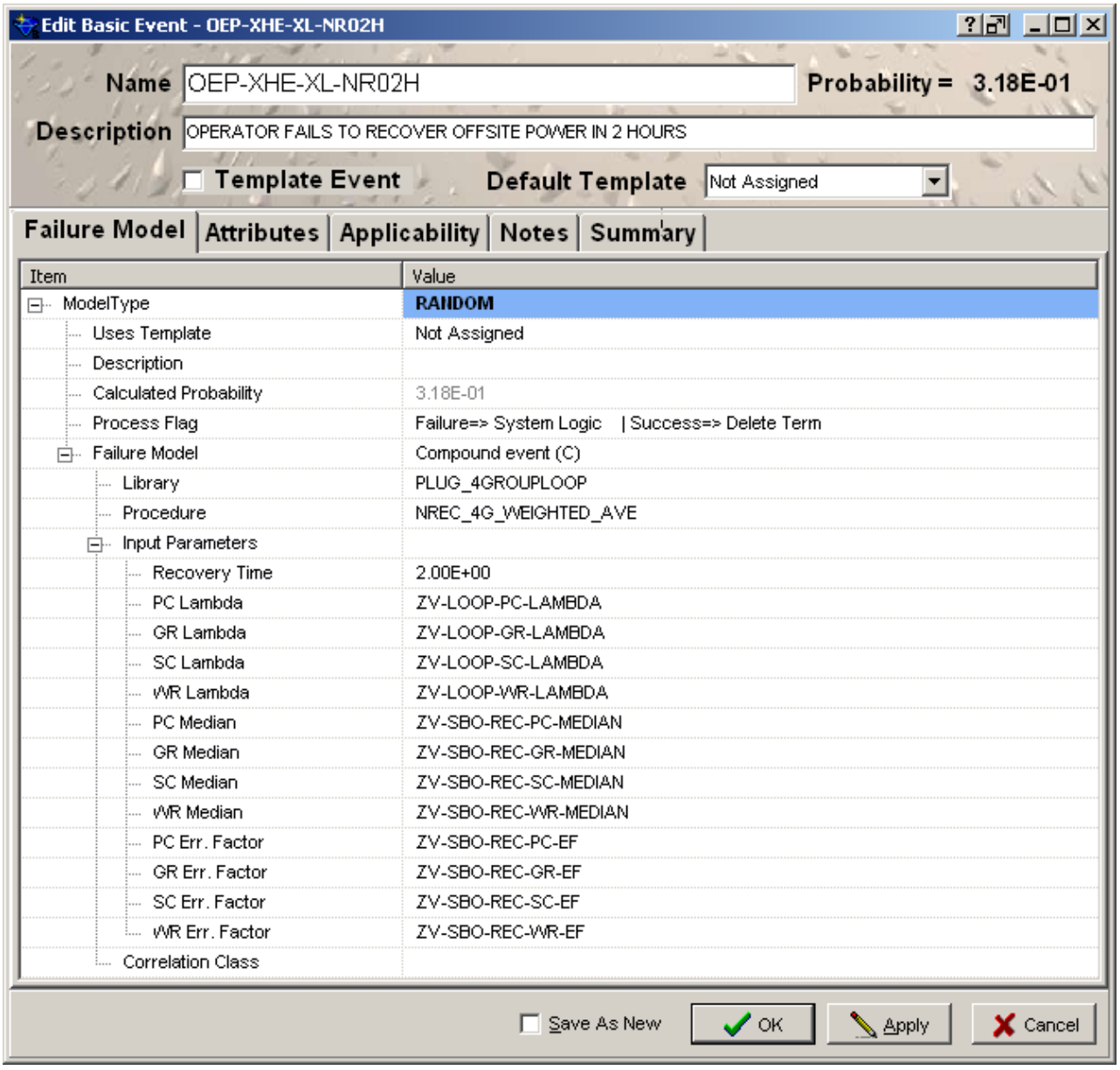
LOOP Category	μ	σ
Plant Centered	-0.759	1.287
Switchyard Centered	-0.390	1.256
Grid Related	0.300	1.064
Weather Related	0.793	1.982

[4]This table includes information about the uncertainty in μ and σ, which we will not use in this course. This issue is addressed in *Advanced Topics in PRA* (P-501).

The figure below shows how the probability of nonrecovery decreases with time for each of the four LOOP categories.



- These parameters and distributions for the LOOP duration events have been incorporated into the latest SPAR models. To use these, however, required development of a LOOP nonrecovery compound event calculation. This calculation is performed by calling the PLUG_4GROUPLOOP.DLL library in SAPHIRE 8.



- Normally, the LOOP nonrecovery compound calculation weights the nonrecovery probability by the LOOP frequency. However, when using the SPAR model for an initiating event assessment, three of the LOOP frequency parameters are set to zero (indicating that type of LOOP did not occur) while one is set to a value of one. In this situation, the LOOP nonrecovery will represent just the LOOP that did occur and is not weighted by the other LOOP types.

7.3 Recovery of System/Component Failures

- Most system failures occur because an operator fails to start the system, or because a system component fails and is not recovered in the time available. This implies a general system fault tree of the form shown in Figure 1.

The methods used to quantify these events are numerous, but we will mention two:

- Use of simplified HRA tools, for example the SPAR HRA worksheets.
    - SPAR-H discussed in Human Reliability Analysis (HRA) P-203 course.
- Use of LOOP and DG-specific recovery curves to quantify station blackout and seal LOCA related probabilities. In the SPAR models, these events have "PRAish" names such as:

OEP-XHE-XL-NR30M	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 30 MINUTES
OEP-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR
EPS-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER EMERGENCY DIESEL IN 1 HOUR

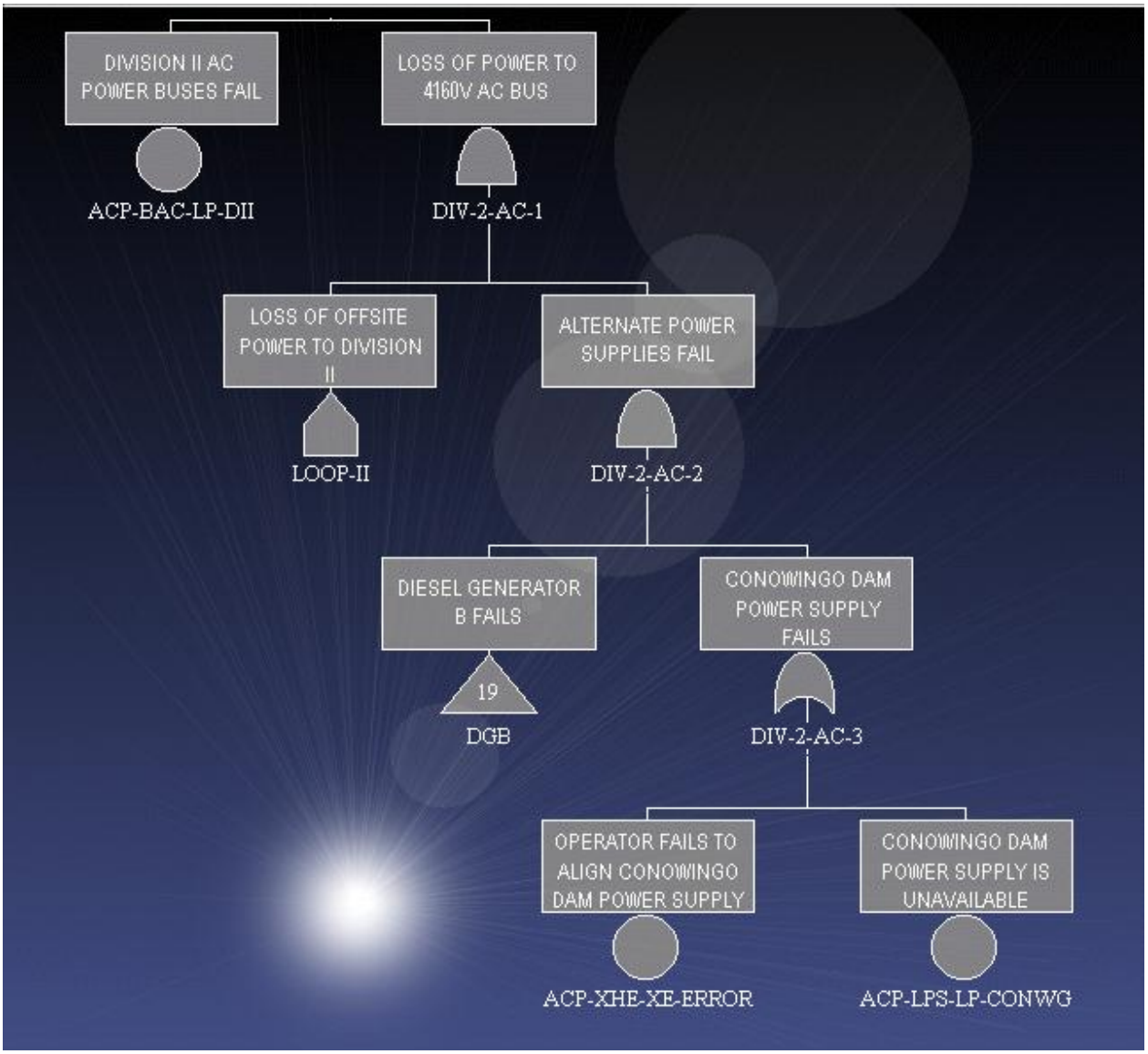


Figure 1. Peach Bottom SPAR division II AC power fault tree

LOOP-Dependent Nonrecovery Probabilities

- This section will address a number of basic events in the SPAR models that are calculated conditional on LOOP category and duration. Such events are those related to long term AC power recovery (i.e., diesel generators) and reactor coolant pump seal LOCA (for PWR models).

- The diesel nonrecovery model is represented by P(G > t_{short}). Previous to the SPAR 3+ models, the aleatory model for EDG recovery was an exponential distribution. The current SPAR models, and corresponding SAPHIRE calculation, model the recovery time as Weibull-distributed. As was the case for the LOOP nonrecovery calculation, the PLUG_4GROUPLOOP.DLL add-in can also estimate emergency diesel generator (EDG) nonrecovery probability. This add-in to SAPHIRE is invoked by selecting the procedure type "DG_RECOVERY" and providing SAPHIRE with the appropriate recovery time and the Weibull α and β parameters.

- The Weibull-based form of f_{DG} (the EDG recovery time density) is:

$$f_{DG}(t) = \frac{\alpha}{\beta}\left(\frac{t}{\beta}\right)^{\alpha-1} \exp\left[-\left(\frac{t}{\beta}\right)^{\alpha}\right]$$

- For recovery of one of two (or more) failed EDGs, NUREG/CR-6890 recommends a value of 0.745 for α and 6.14 hours for β. This implies a mean time to repair an EDG of 7.35 hours. This equation and associated parameter values are built into the DG_RECOVERY plug-in used by SAPHIRE.

7.4 Workshop

8. INITIATOR-TYPE EVENTS using ECA

Section 8 contains a description of how the Events and Conditions Assessment (ECA) in SAPHIRE is used to evaluate events that can be considered as initiating events. Details on how to operate the ECA workspace for a hypothetical event evaluation are provided.

Learning Objectives

- Demonstrate a proficiency with ECA workspace by performing the workshop exercises related to an initiator type of event evaluation.

Section 8 Topics

8.1 Introduction

- This section demonstrates how to use ECA workspace to evaluate events that involve initiators.
  - ◊ As an example of initiating event assessment, we will walk through the evaluation of a loss of offsite power event using the Generic PWR SPAR model.
- Topics to be covered include
  - ◊ A brief overview of the plant,
  - ◊ A discussion of the event to be modeled,
  - ◊ A discussion of the preliminary steps to an analysis of the event,
  - ◊ A walk through of the use of ECA workspace to evaluate the event,
  - ◊ A workshop that models some similar events.
- The basic approach demonstrated in this section will be to estimate the condition probability of core damage (CCDP) as a result of the LOOP event.
- ECA workspace has a built-in procedure that will handle most of the details for the analysis.
  - ◊ The analysts job will be to:
    - Determine what basic events in the SPAR model must be modified to map the event into the model.
    - Enter the appropriate changes through the ECA workspace Initiating Event Analysis interface.

8.2 Plant Overview

- The Generic PWR SPAR model is a four loop plant that does utilize feed-and-bleed capability as an alternative to auxiliary feedwater and main feedwater to remove decay heat from the primary.
  - ◊ For this analysis, we will use this SPAR model.
  - ◊ The model includes the front-line injection and decay heat removal systems.

- A summary of the injection and decay heat removal systems includes:

  ◊ Auxiliary Feedwater System (AFW). AFW has three pump trains. Generally one of three trains is required to feed two of four steam generators.

  ◊ Emergency Power System (EPS). EPS has two dedicated diesel generators and a backup diesel generator that can be connected to either ac electrical bus.

  ◊ High Pressure Injection (HPI)/High Pressure Recirculation (HPR). HPI two different sub-systems, safety injection and charging, that are used to inject water from a large tank into the reactor vessel. The success is one of two SI pumps or one of two charging pumps.

  ◊ Residual Heat Removal System. RHR has two pump trains, one of which is required to provide injection.

8.3 Event Description

A fire near the plant caused the offsite transmission lines to fault. The emergency diesels started and operated as designed. Although offsite power was restored in 5 minutes, emergency electrical buses were supplied by the diesels for 24 hours.

Two days after the LOOP occurred, the RHR A pump recirculation line was found to be obstructed with plastic sheeting material. The material was determined to have been in the recirculation line since the last refueling outage 30 days before the LOOP.

- We will consider this event to be a grid-related loss-of-offsite power initiating event. We will also consider the event to be recoverable.

- We will consider the failure of the RHR pump recirculation line to be a potential common cause failure (the B pump was not affected, although it might have been).

8.4 Preliminary Steps for Initiating Event Assessment

Before starting a new ECA workspace we need to review the model documentation and identify the basic events that must be modified to map the event into the model. We might also need to recalculate some basic event probabilities if we determine that our analysis will require event mappings that are not automatically handled by the ECA workspace.

- The ECA workspace shows the model is preconfigured for grid-related loss-of-offsite power events. We will accept the non-recovery and seal LOCA probabilities provided.

- We will need to account for the failed RHR pump separately. For this example, we will assume that the obstruction would not allow the pump to start. We review the model and find several RHR pump events:

RHR-MDP-CF-RUN	RHR PUMPS FAIL FROM COMMON CAUSE TO RUN
RHR -MDP-CF-START	RHR PUMPS FAIL FROM COMMON CAUSE TO START
RHR -MDP-FR-1A	RHR PUMP 1A FAILS TO RUN
RHR -MDP-FR-1B	RHR PUMP 1B FAILS TO RUN
RHR -MDP-FS-1A	RHR PUMP 1A FAILS TO START
RHR -MDP-FS-1B	RHR PUMP 1B FAILS TO START
RHR -MDP-TM-1A	RHR PUMP TRAIN 1A IS IN TEST OR MAINTENANCE
RHR -MDP-TM-1B	RHR PUMP TRAIN 1B IS IN TEST OR MAINTENANCE

- The failure mode we are looking for is FS

- We can model the recirculation line failure by setting basic event

  RHR-MDP-FS-1A to TRUE

- We will also need to account for the possibility that the remaining RHR pump might have been affected by a common cause failure involving both pumps. Recall (from Section 6.4) that guidance for this potential common cause failure indicates that we need to set to the basic event for the observed failure mode (failure to start, RHR-MDP-FS-1A) to TRUE, and set the basic event representing CCF for the unobserved failure mode (failure to run, RHR-MDP-CF-RUN) to FALSE.

- We can now start the ECA workspace and enter our data. The following checklist will help to assist during the calculation.

Event Analysis Checklist

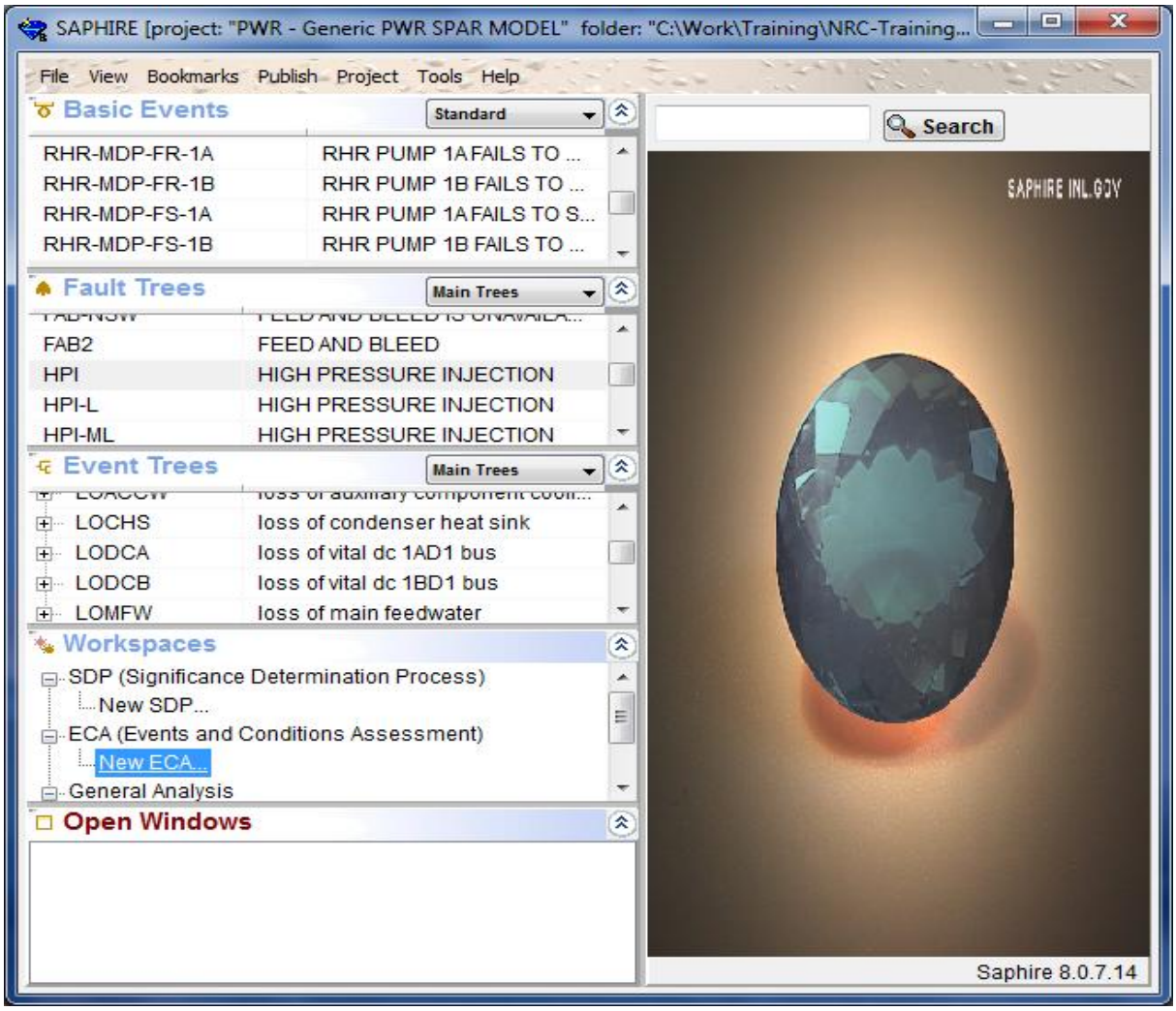
#	Item	Result
1	Is the event an initiating event or condition assessment?	Initiating ☐ Condition ☐ Both ☐
2	If the event is a condition assessment, what is the duration?	hours
3	If the event is an initiating event, is the initiator recoverable? (Note that SAPHIRE (ECA) will adjust the non-recovery probabilities for you automatically)	Yes ☐ No ☐
4	Were any systems, structures, or components (SSCs) inoperable during the event.	Yes ☐ No ☐
5	If the answer to Question 4 was *yes*, identify the SSCs by finding its associated basic event(s) from the PRA model. Only identify "independent failure" related events (e.g., no common-cause yet).	
6	For those basic events identified in Question 5, determine the SSC's non-recovery probability (if it is recoverable from the failure).	
7	Are there any basic events identified in Question 5 that have associated common-cause failure events?	Yes ☐ No ☐
8	For each event that had a yes answer to Question 7, determine the type of SSC failure. Options are: (a) Independent failures (b) Common-cause failures (actual or potential) (c) Testing/Maintenance *Refer to Section 6 for additional information.*	

#	Item	Result
9	List the common-cause basic events that were identified in Question 7. Note that since you are using the Rev. 3+SPAR model, you *will not* (normally) need to adjust these events (they are automatically modified by the software).	
10	You will need to specify in the ECA workspace how to modify each basic event identified in Question 8. From Question 8, if the SSC is an independent failure or testing/maintenance outage, set the event to a probability of 1.0. Otherwise, set it to TRUE.	
11	For those SSCs that were identified in Question 6 and do not have an associated common-cause event, set the SSCs to its non-recovery probability in the ECA workspace.	
12	Process the analysis using the modifications identified in Questions 1 - 11. Record your results of the analysis.	

8.5 ECA Workspace Walk Through

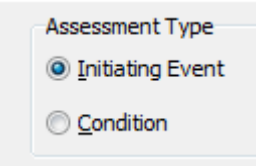
This section will provide a step-by-step guide to performing an event evaluation for the initiating event described in the preceding section.

- Start the ECA workspace by double-clicking the **New ECA**… option in the Workspaces list panel.



This example uses the Generic PWR SPAR model. Make sure this project is opened (i.e., currently working project).

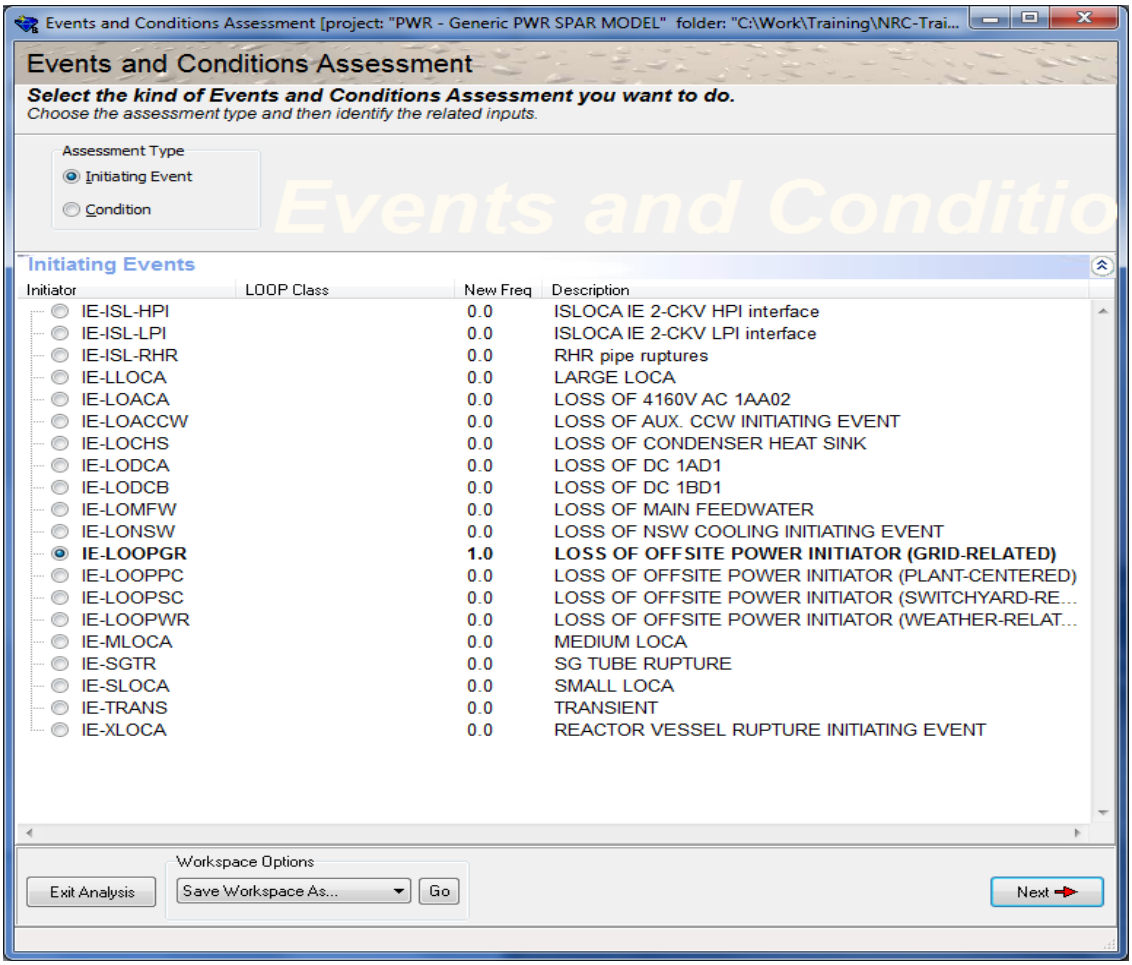
- From the main screen, select the **Initiating Event** radio button.



- The steps we are going to go through are:

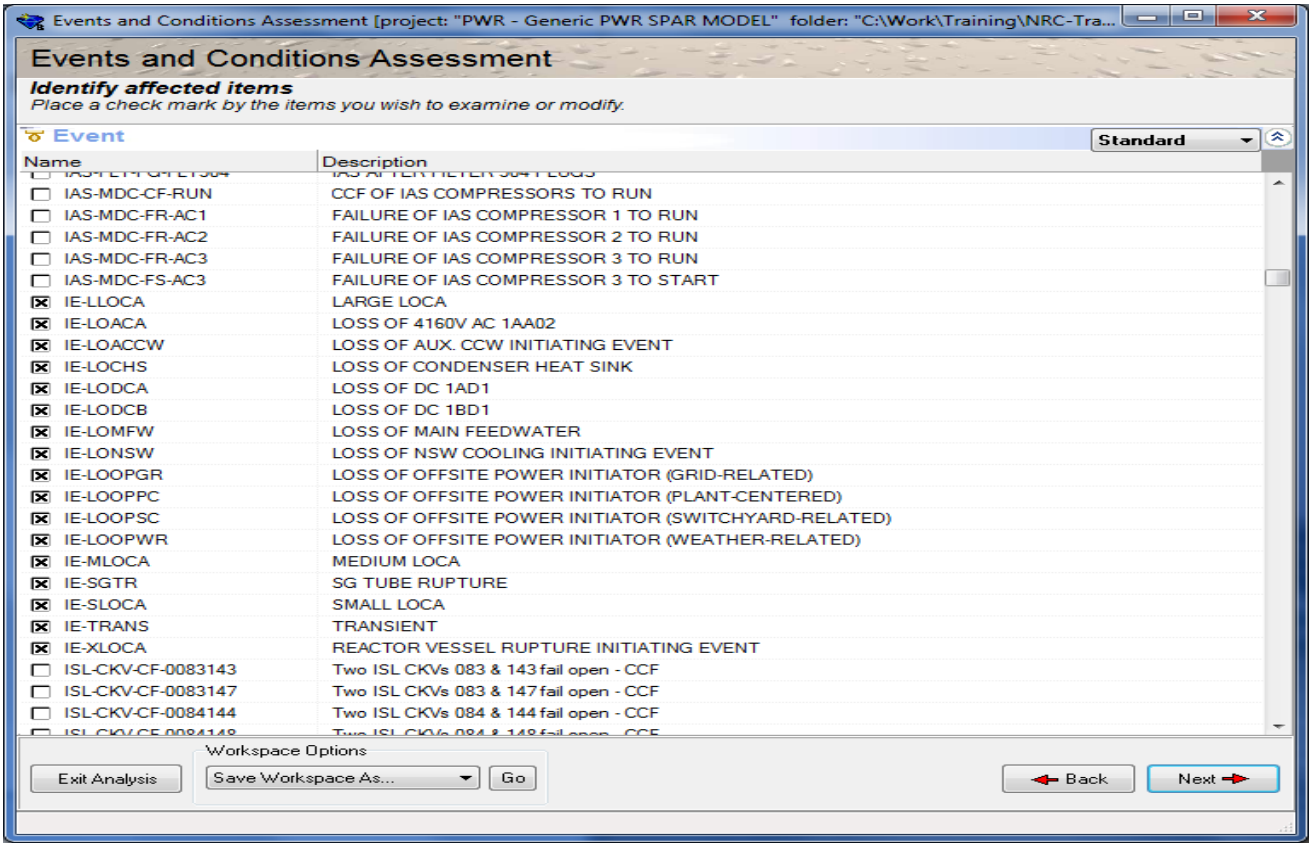
  1. Select the initiating event that did occur
  2. Add any required event modifications
  3. Process the analysis
  4. Review the results

- The ECA workshop will display the Initiating Events screen. From the list of initiating events, select the one that matches the assessment, by **clicking** the radio button next to the initiating event.



- This example is a GRID RELATED LOOP, once the radio button is selected, then click the **Next** button.

- The "Identify affected items" screen allows the analyst to add to or modify the basic event probabilities (if needed) that will be saved with the analysis record.

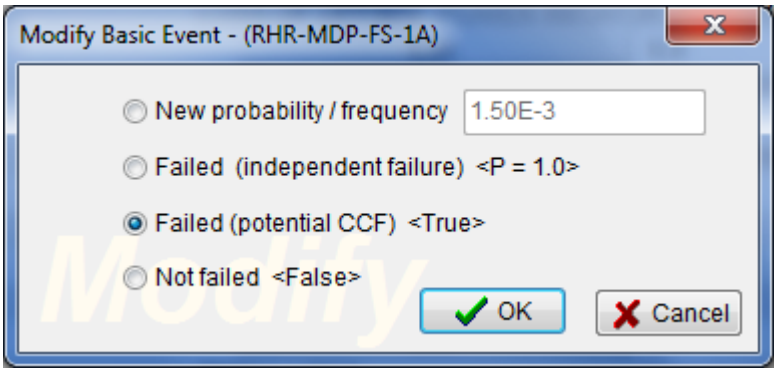


Initially, the initiating events will selected as being modified from their nominal values by being checked. For example, the non-LOOP initiators will be set to zero since these initiators did not occur.

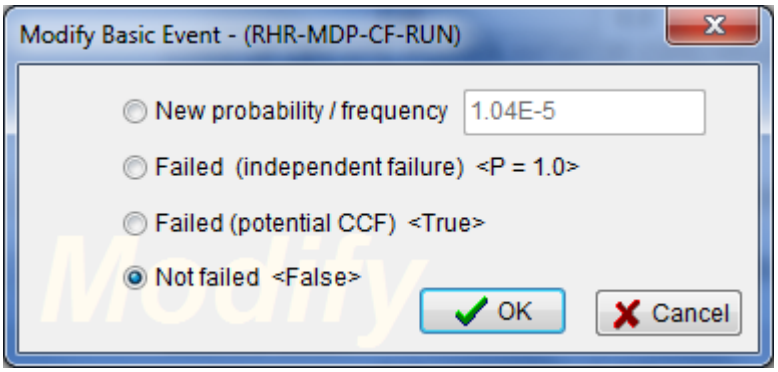
We need to add other events to the list, specifically the events related to the RHR pump.

- Since we need to add additional basic events, scroll down the list and click the check box for the basic event RHR-MDP-FS-1A and RHR-MDP=CF-RUN.

- Set **RHR-MDP-FS-1A** to TRUE.



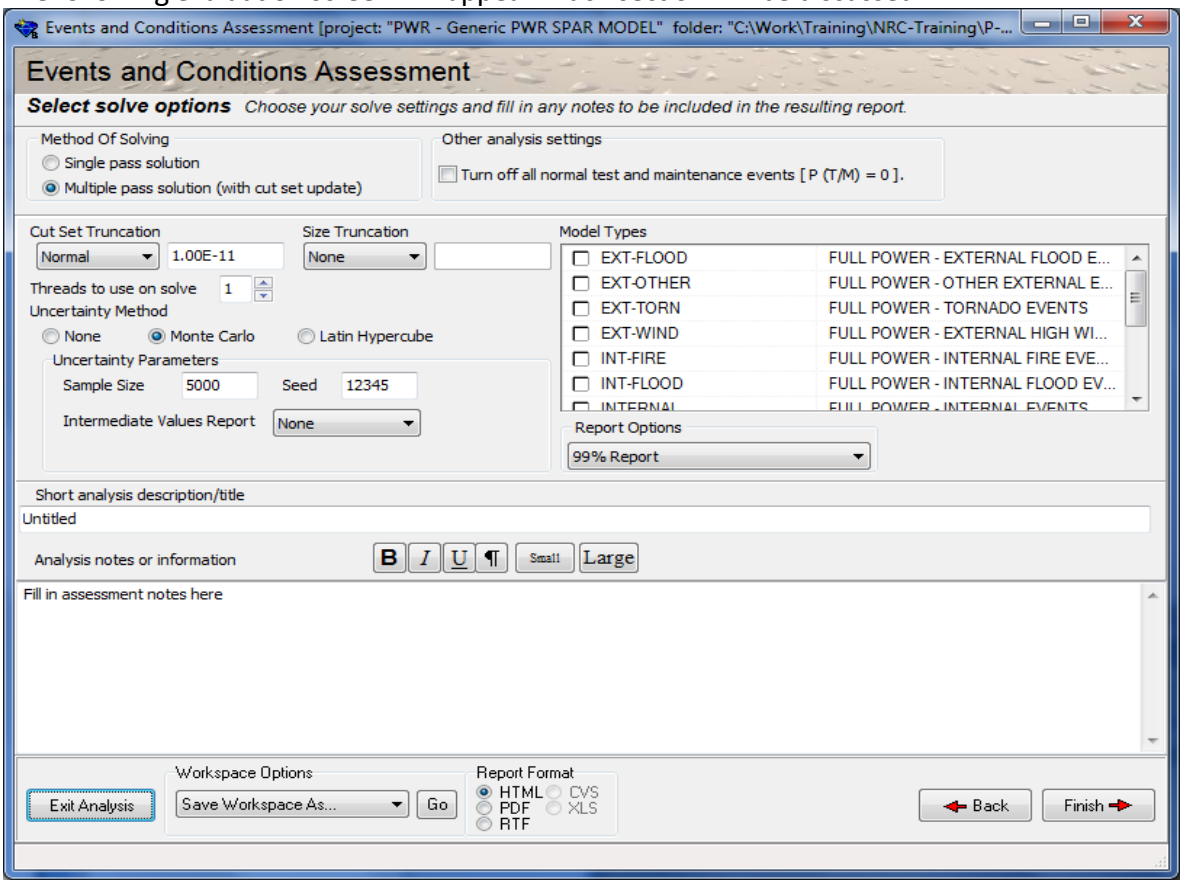
- Find **RHR-MDP-CF-RUN** and set it to FALSE.



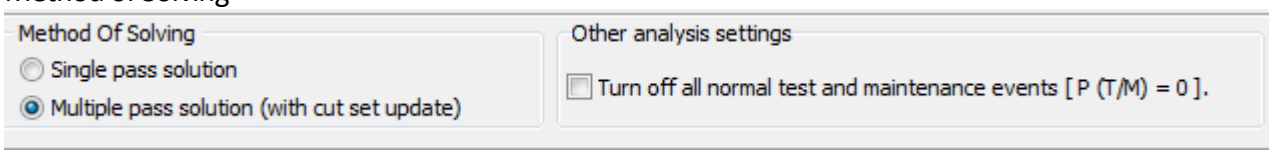
- Select the **Next** button and then set the basic events probabilities.

- Once the two basic events have been adjusted select the **Next** button.

The following evaluation screen will appear. Each section will be discussed.



Method of Solving

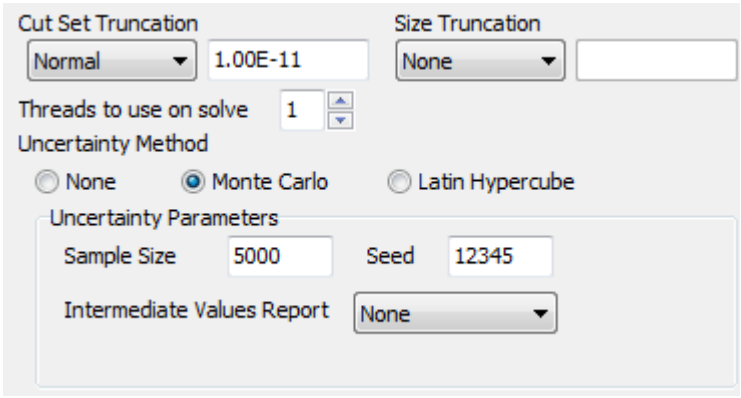


The difference between the single pass with cut set update and the multi-pass routines are:

- The multiple pass solution algorithm will ensure that all sequence post-processing rules are applied even when basic events in the model are specified as a logical "True." The "single pass with cut set update option" does not.
- The multiple pass algorithm will remove non-minimal cut sets (if generated from a post-processing rule) by automatically performing a cut set update.
- SAPHIRE 8 performs the "base case" and the "new case" solving at the same truncation level for both algorithms.

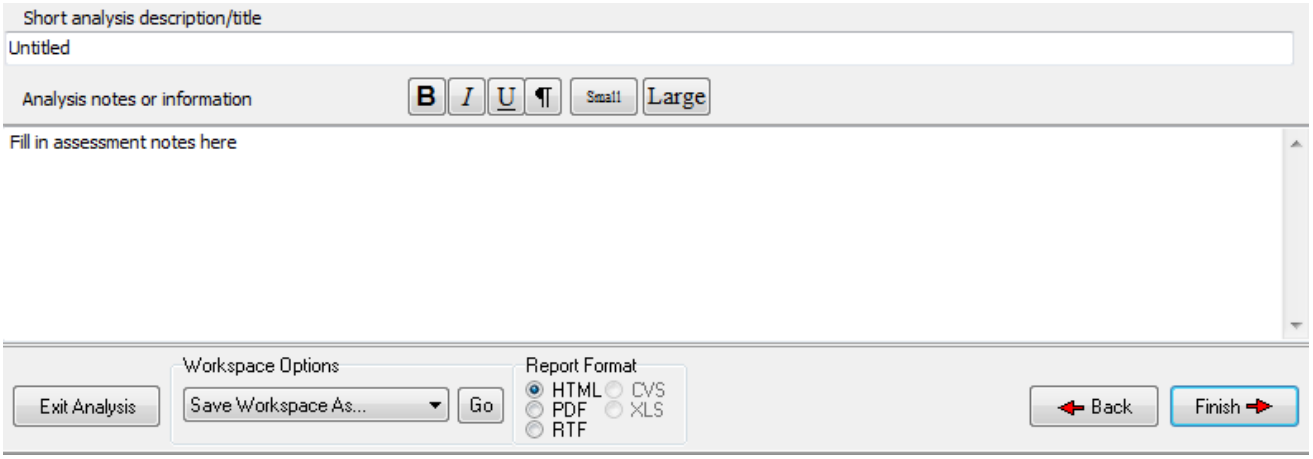
- The "Turn off all T&M events will set all test and maintenance events to 0.0 and then resolve the model, prior to evaluation.

Cut Set Truncation



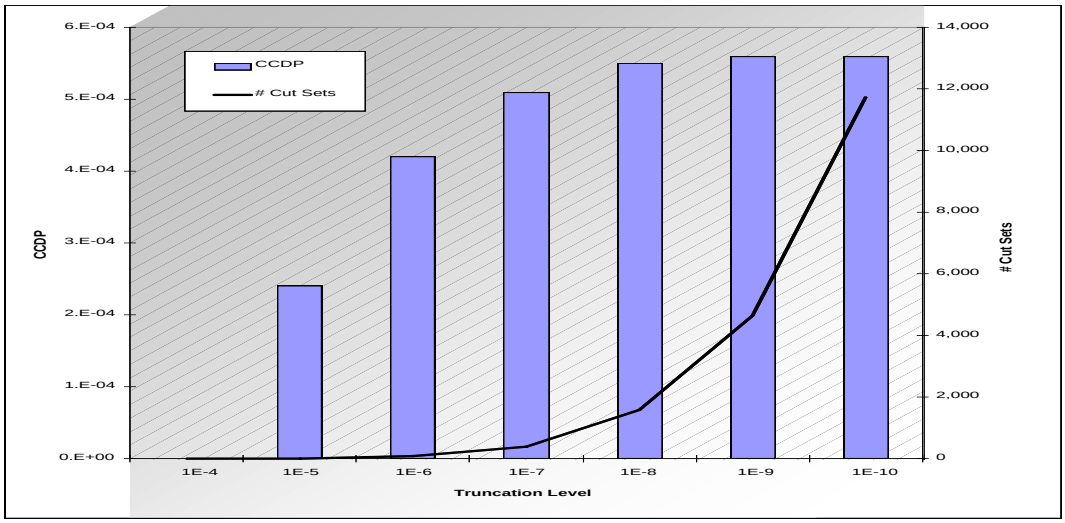
- The nominal truncation will solve all sequences at this truncation (it defaults to the model's default).
- Uncertainty will be evaluated when solving the model (see NUREG/CR-7039, Volume 5, Section2.7).

Description

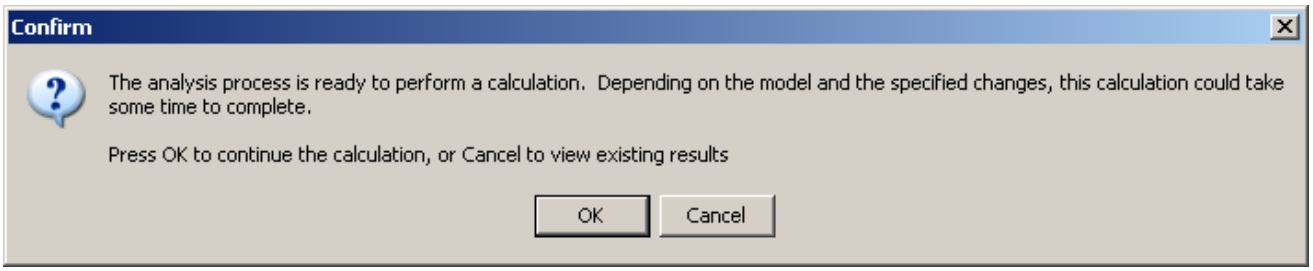


A title can be specified to identify the type of assessment being performed. Also, a description of the event and the components that were affected can be described in the analysis notes block.

- Note that changing the truncation may affect the CCDP similar to that shown below.



- Once all of the information has been selected, click the Finish button and SAPHIRE will process the analysis. The following screen just cautions the analyst that the evaluation may take extra time depending upon the complexity of the model.



- When finished, SAPHIRE will display the Event Assessment screen. The **CCDP** for the event will also be displayed.

- Once the evaluation is complete SAPHIRE will provide a summary report of the evaluation. Each of the pieces of the output will be discussed.

The first part is the overall result.

Initiating Event Assessment Summary

Initiating Event	IE-LOOPGR
CCDP	5.93E-5

Solve Settings

Solve Settings

Cut set Truncation	Normal 1.00E-11
Size Truncation	None
Solve Method	Multiple Pass

Summary of Events Changed

Grid Related LOOP

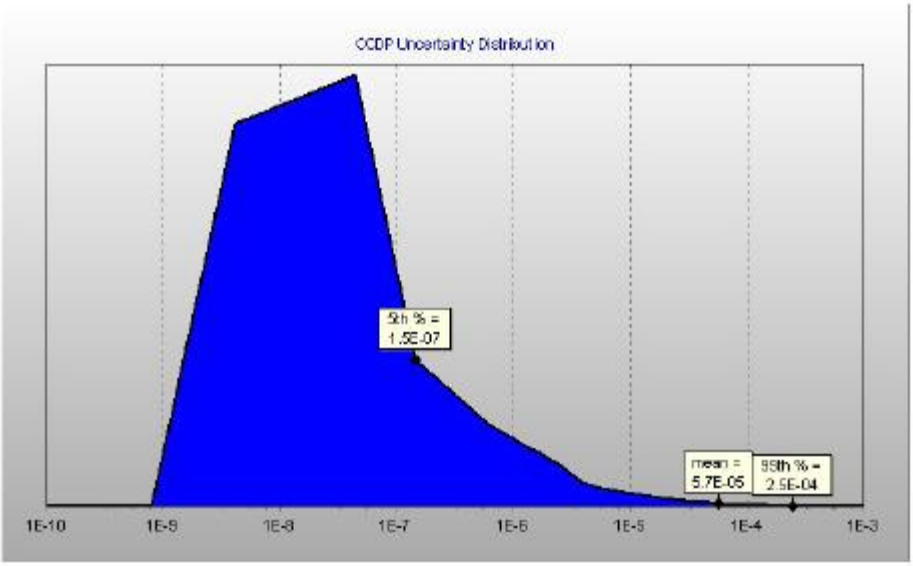
Summary of Conditional Event Changes

Event	Description	Cond Type	Cond Value	Nominal Type	Nominal Value
IE-ISL-HPI	ISLOCA IE 2-CKV HPI interface	N	0.00E+0	S	3.27E-6
IE-ISL-LPI	ISLOCA IE 2-CKV LPI interface	N	0.00E+0	S	3.27E-6
IE-ISL-RHR	RHR pipe ruptures	N	0.00E+0	S	5.62E-6
IE-LLOCA	LARGE LOCA	N	0.00E+0	N	2.50E-6
IE-LOACA	LOSS OF 4160V AC 1AA02	N	0.00E+0	N	9.00E-3
IE-LOACCW	LOSS OF AUX. CCW INITIATING EVENT	N	0.00E+0	N	4.00E-4
IE-LOCHS	LOSS OF CONDENSER HEAT SINK	N	0.00E+0	N	8.00E-2
IE-LODCA	LOSS OF DC 1AD1	N	0.00E+0	N	6.00E-4
IE-LODCB	LOSS OF DC 1BD1	N	0.00E+0	N	6.00E-4
IE-LOMFW	LOSS OF MAIN FEEDWATER	N	0.00E+0	N	1.00E-1
IE-LONSW	LOSS OF NSW COOLING INITIATING EVENT	N	0.00E+0	N	4.00E-4
IE-LOOPGR	LOSS OF OFFSITE POWER INITIATOR (GRID-RELATED)	N	1.00E+0	N	1.86E-2
IE-LOOPPC	LOSS OF OFFSITE POWER INITIATOR (PLANT-CENTERED)	N	0.00E+0	N	2.07E-3
IE-LOOPSC	LOSS OF OFFSITE POWER INITIATOR (SWITCHYARD-RELATED)	N	0.00E+0	N	1.04E-2
IE-LOOPWR	LOSS OF OFFSITE POWER INITIATOR (WEATHER-RELATED)	N	0.00E+0	N	4.83E-3
IE-MLOCA	MEDIUM LOCA	N	0.00E+0	N	2.00E-4
IE-SGTR	SG TUBE RUPTURE	N	0.00E+0	N	4.00E-3
IE-SLOCA	SMALL LOCA	N	0.00E+0	N	6.00E-4
IE-TRANS	TRANSIENT	N	0.00E+0	N	8.00E-1
IE-XLOCA	REACTOR VESSEL RUPTURE INITIATING EVENT	N	0.00E+0	N	1.00E-7
RHR-MDP-CF-RUN	RHR PUMPS FAIL FROM COMMON CAUSE TO RUN	F	False	C	1.04E-5
RHR-MDP-FS-1A	RHR PUMP 1A FAILS TO START	T	True	1	1.50E-3
RHR-MDP-CF-START	RHR PUMPS FAIL FROM COMMON CAUSE TO START	C	4.18E-2	C	6.27E-5

CCDP Uncertainty Analysis (if performed)

CCDP Uncertainty Distribution

5%	Median	Point Estimate	Mean	95%	Seed	Sample Size	Method
1.48E-7	1.80E-5	5.93E-5	5.69E-5	2.48E-4	12345	5000	Monte Carlo



Results from the evaluation listing the dominant event tree and dominant sequences.

Event Tree Dominant Results

Only items contributing at least 1.0% to the total Delta CCDP are displayed.

Event Tree	CCDP	% Contribution	Description
LOOPGR	5.93E-5	100.0%	loss of offsite power (Grid related)
Total	**5.93E-5**	**100%**	

Dominant Sequence Results

Only items contributing at least 1.0% to the total Delta CCDP are displayed.

Event Tree	Sequence	CCDP	% Contribution	Flagset	Description
LOOPGR	15	1.28E-5	21.6%	ETF-LOOP-GR	/RPS-L, /EPS, AFW-L, FAB-L
LOOPGR	16-04-2	1.09E-5	18.3%	ETF-SBO-GR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, BP2, /OPR-04H, /HPI, /SSC, LPR
LOOPGR	16-03-10	7.44E-6	12.5%	ETF-SBO-GR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, /BP2, OPR-04H, DGR-04H, AFW-MAN, SG-DEP-LT1
LOOPGR	16-06	6.20E-6	10.5%	ETF-SBO-GR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, BP2, OPR-04H, DGR-04H
LOOPGR	02-05	5.94E-6	10.0%	ETF-LOOP-GR	/RPS-L, /EPS, /AFW-L, /PORV-L, LOSC-L, /RSD-L, /BP1, BP2, OPR-02H, HPI-L
LOOPGR	02-02-03	4.70E-6	7.9%	ETF-LOOPGR-SLOCA	/RPS-L, /EPS, /AFW-L, /PORV-L, LOSC-L, /RSD-L, /BP1, BP2, /OPR-02H, /RPS, /AFW, /HPI, /SSC, RHR, LPR
LOOPGR	02-02-09	2.85E-6	4.8%	ETF-LOOPGR-SLOCA	/RPS-L, /EPS, /AFW-L, /PORV-L, LOSC-L, /RSD-L, /BP1, BP2, /OPR-02H, /RPS, /AFW, HPI, /SSC1, LPI
LOOPGR	16-45	2.60E-6	4.4%	ETF-SBO-GR	/RPS-L, EPS, AFW-B, OPR-01H, DGR-01H
LOOPGR	16-10-2	1.89E-6	3.2%	ETF-LOOPGR-MLOCA	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, BP1, BP2, /OPR-02H, /HPI, /SSC, LPR
Total		**5.93E-5**	**100%**		

A report of the top 1% dominant cut sets for each sequence is provided.

Cut Set Report - LOOPGR 15

Only items contributing at least 1% to the total are displayed.

#	Prob/Freq	Total%	Cut Set
	1.28E-5	100	Displaying 5873 of 5873 Cut Sets.
1	1.96E-6	15.3	IE-LOOPGR,AFW-MDP-TM-4002,AFW-XHE-XM-TDPBD3,EPS-DGN-FR-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
2	1.20E-6	9.38	IE-LOOPGR,AFW-MDP-TM-4002,AFW-XHE-XM-TDPBD3,EPS-SEQ-FC-DGA
3	7.36E-7	5.75	IE-LOOPGR,AFW-MDP-FS-4002,AFW-XHE-XM-TDPBD3,EPS-DGN-FR-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
4	4.90E-7	3.83	IE-LOOPGR,AFW-MOV-OO-FV5154,AFW-XHE-XM-TDPBD3,EPS-DGN-FR-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
5	4.63E-7	3.62	IE-LOOPGR,AFW-MDP-TM-4002,AFW-XHE-XM-TDPBD3,EPS-DGN-FS-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
6	4.50E-7	3.52	IE-LOOPGR,AFW-MDP-FS-4002,AFW-XHE-XM-TDPBD3,EPS-SEQ-FC-DGA
7	4.17E-7	3.26	IE-LOOPGR,AFW-MDP-FS-4002,AFW-XHE-XM-TDPBD3,EPS-DGN-TM-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
8	3.00E-7	2.34	IE-LOOPGR,AFW-MOV-OO-FV5154,AFW-XHE-XM-TDPBD3,EPS-SEQ-FC-DGA
9	2.78E-7	2.17	IE-LOOPGR,AFW-MOV-OO-FV5154,AFW-XHE-XM-TDPBD3,EPS-DGN-TM-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
10	2.64E-7	2.06	IE-LOOPGR,AFW-MDP-FR-4002,AFW-XHE-XM-TDPBD3,EPS-DGN-FR-DGA,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2
11	2.32E-7	1.81	IE-LOOPGR,ACP-CRB-CC-AA20,AFW-MDP-TM-4002,AFW-XHE-XM-TDPBD3,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XM-DGUN2

The remaining dominant sequence cut sets are also listed.

Referenced Events- lists all of the basic events that part of the cut sets generated from the analysis.

Referenced Events

Event	Description	Probability
ACP-CRB-CC-AA20	FAILURE OF SWITCHYARD AC BREAKER AA20 TO OPEN	2.50E-3
ACP-CRB-CC-BA30	FAILURE OF SWITCHYARD AC BREAKER BA30 TO OPEN	2.50E-3
ACP-CRB-CF-A2030	CCF OF SWITCHYARD AC BREAKERS TO OPEN AA0205/0301	4.25E-5
AFW-MDP-FR-4002	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS TO RUN	5.38E-4
AFW-MDP-FS-4002	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS TO START	1.50E-3
AFW-MDP-TM-4002	AFW MDP P4-4002 UNAVAILABLE DUE TO TEST AND MAINTENANCE	4.00E-3
AFW-MDP-TM-4003	AFW MDPP4-4003 UNAVAILABLE DUE TO TEST AND MAINTENANCE	4.00E-3
AFW-MOV-CC-HV5106	STEAM SUPPLY MOV HV5106 FAILS TO OPEN	1.00E-3
AFW-MOV-OO-FV5154	FAILURE OF AFW MDP B MINFLOW MOV 5154 TO CLOSE	1.00E-3
AFW-TDP-FR-4001	TURBINE DRIVEN FEED PUMP P4-001 FAILS TO RUN	4.10E-3
AFW-TDP-FS-4001	TURBINE DRIVEN FEED PUMP P4-001 FAILS TO START	7.00E-3
AFW-TDP-TM-4001	AFW TDP PUMP P4-001 IS IN TEST OR MAINTENANCE	5.00E-3
AFW-XHE-XM-MANAFW	OPERATOR FAILS TO MANUALLY INITIATE AFW	4.00E-3
AFW-XHE-XM-TDPBD	OPERATOR FAILS TO CONTROL AFW TDP AFTER BATTERY DEPLETION	3.00E-1
AFW-XHE-XM-TDPBD3	OPERATOR FAILS TO CONTROL AFW TDP AFTER BATTERY DEPLETION; NON SBO	1.00E-1
EPS-DGN-CF-1ABRUN	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO RUN	3.28E-4
EPS-DGN-CF-1ABSTART	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO START	5.75E-5
EPS-DGN-CF-DG1ABUN2R	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO RUN	1.21E-4
EPS-DGN-CF-DG1ABUN2S	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO START	1.86E-5

Lastly, the report provides event importance measures from the analysis. The importance measures list only those events that are greater than a predefined truncation.

RIR > 2.00E+00

Event Tree Importance

GROUP

EVENT	OCCUR.	PROB.	FV	RIR	RRR	BB	RII	RRI	UNCERT.
NSW-MDP-CF-START	1367	1.40E-5	1.13E-1	6.47E+3	1.13E+0	3.83E-1	3.83E-1	6.70E-6	7.95E-6
NSW-MDP-CF-RUN	82	2.76E-8	2.14E-4	6.24E+3	1.00E+0	3.70E-1	3.70E-1	1.27E-8	3.55E-8
NSW-CKV-CF-PCKVS	41	2.96E-9	2.16E-5	5.95E+3	1.00E+0	3.52E-1	3.52E-1	1.28E-9	6.24E-9
DCP-BAT-CF-ALL	3	6.43E-8	2.54E-4	3.94E+3	1.00E+0	2.33E-1	2.33E-1	1.51E-8	6.44E-8
RPS-ROD-CF-RCCAS	154	1.21E-6	4.31E-3	3.26E+3	1.00E+0	1.93E-1	1.93E-1	2.55E-7	2.49E-7
AFW-PMP-CF-RUN	50	1.31E-7	3.09E-4	2.23E+3	1.00E+0	1.32E-1	1.32E-1	1.83E-8	3.84E-8
AFW-CKV-CF-125678	44	1.12E-7	2.63E-4	2.22E+3	1.00E+0	1.32E-1	1.32E-1	1.56E-8	3.49E-8
AFW-CKV-CF-113456	44	1.15E-7	2.70E-4	2.22E+3	1.00E+0	1.32E-1	1.32E-1	1.60E-8	3.22E-8
AFW-TNK-FC-CST1	35	4.80E-8	1.12E-4	2.21E+3	1.00E+0	1.31E-1	1.31E-1	6.65E-9	1.15E-8
AFW-CKV-CF-001214	35	5.80E-8	1.35E-4	2.21E+3	1.00E+0	1.31E-1	1.31E-1	8.03E-9	2.47E-8
AFW-CKV-CF-0331358	35	5.80E-8	1.35E-4	2.21E+3	1.00E+0	1.31E-1	1.31E-1	8.03E-9	2.47E-8
NSW-MOV-CF-16689A	388	2.28E-5	3.92E-2	1.67E+3	1.04E+0	9.92E-2	9.92E-2	2.32E-6	2.24E-6
EPS-SEQ-CF-DGAB	489	1.07E-4	1.08E-1	9.95E+2	1.12E+0	5.89E-2	5.89E-2	6.43E-6	9.42E-6
NSW-FAN-CF-FSALL	124	4.00E-6	3.79E-3	9.35E+2	1.00E+0	5.54E-2	5.54E-2	2.25E-7	4.92E-7
NSW-FAN-CF-FRALL	35	2.64E-7	2.45E-4	9.17E+2	1.00E+0	5.43E-2	5.43E-2	1.45E-8	2.07E-8
EPS-DGN-CF-1ABSTART	382	5.75E-5	1.44E-2	2.50E+2	1.01E+0	1.48E-2	1.48E-2	8.56E-7	9.85E-7
EPS-FAN-CF-FSALL	163	1.03E-5	2.56E-3	2.49E+2	1.00E+0	1.47E-2	1.47E-2	1.52E-7	3.17E-7

FV > 5.00E-03

Event Tree Importance

GROUP

EVENT	OCCUR.	PROB.	FV	RIR	RRR	BB	RII	RRI	UNCERT.
IE-LOOPGR	30007	1.00E+0	1.00E+0	1.00E+0	1.90E+38	5.93E-5	0.00E+0	5.93E-5	8.39E-5
EPS-WILSON-SWYD	24169	4.00E-1	6.57E-1	1.99E+0	2.91E+0	9.73E-5	5.84E-5	3.89E-5	1.56E-5
EPS-DUAL-UNITLOOP	23029	5.79E-1	6.53E-1	1.47E+0	2.88E+0	6.69E-5	2.82E-5	3.87E-5	1.65E-5
RCS-MDP-LK-BP2	19691	2.00E-1	5.68E-1	3.12E+0	2.12E+0	1.57E-4	1.26E-4	3.14E-5	1.89E-5
EPS-XHE-XM-DGUN2	13196	1.00E+0	5.21E-1	1.00E+0	2.09E+0	3.09E-5	2.54E-17	3.09E-5	0.00E+0
EPS-XHE-XL-NR04H	2797	5.57E-1	2.34E-1	1.19E+0	1.31E+0	2.49E-5	1.10E-5	1.39E-5	1.69E-6
OEP-XHE-XL-NR04HGR	9764	1.54E-1	2.34E-1	2.08E+0	1.25E+0	7.60E-5	6.43E-5	1.17E-5	6.09E-6
EPS-DGN-FR-DGA	4189	2.12E-2	2.25E-1	1.14E+1	1.29E+0	6.31E-4	6.17E-4	1.34E-5	7.91E-6
AFW-XHE-XM-TDPBD3	1735	1.00E-1	1.56E-1	2.41E+0	1.19E+0	9.27E-5	8.34E-5	9.27E-6	0.00E+0
AFW-XHE-XM-TDPBD	1759	3.00E-1	1.27E-1	1.29E+0	1.14E+0	2.49E-5	1.74E-5	7.47E-6	5.81E-6
OEP-XHE-XL-NR02HGR	4493	3.56E-1	1.14E-1	1.20E+0	1.13E+0	1.85E-5	1.19E-5	6.60E-6	2.12E-6
RHR-MDP-CF-START	3145	4.18E-2	1.13E-1	3.59E+0	1.13E+0	1.60E-4	1.54E-4	6.71E-6	1.63E-6
NSW-MDP-CF-START	1367	1.40E-5	1.13E-1	6.47E+3	1.13E+0	3.83E-1	3.83E-1	6.70E-6	7.95E-6
NSW-MDP-TM-TRNB	3087	1.39E-3	1.11E-1	8.03E+1	1.12E+0	4.71E-3	4.70E-3	6.56E-6	9.26E-6
EPS-SEQ-CF-DGAB	489	1.07E-4	1.08E-1	9.95E+2	1.12E+0	5.89E-2	5.89E-2	6.43E-6	9.42E-6
EPS-SEQ-FC-DGA	2314	3.00E-3	1.08E-1	3.69E+1	1.12E+0	2.13E-3	2.13E-3	6.41E-6	8.99E-6
EPS-DGN-FR-DGB	3429	2.12E-2	1.01E-1	5.68E+0	1.11E+0	2.83E-4	2.77E-4	6.00E-6	3.56E-6
AFW-MDP-TM-4002	738	4.00E-3	8.51E-2	2.22E+1	1.09E+0	1.26E-3	1.26E-3	5.05E-6	3.18E-6

- At this point, you have your report documenting details for the analysis and the results of the analysis.

  But, the analysis is not yet complete. We still need to;

  (a) evaluate the resulting cut sets
  (b) review the importance measures
  (c) consider model applicability/completeness
  (d) use engineering experience along with PRA results for decision making, etc.

8.6 Workshop

9. CONDITION ASSESSMENT using ECA

Section 9 contains a description of how to perform a condition assessment using Events and Conditions Assessment (ECA) in SAPHIRE.

Conditions are those events that cannot be modeled as initiating events, but degrade the ability of the plant to respond to initiating events. Examples are equipment failures that do not cause a plant trip, or any event or operating condition that was not predicted or accounted for in the design basis.

Learning Objectives

- Demonstrate a proficiency with ECA Workspace by performing the workshop exercises related to a condition type of event evaluation.

Section 9 Topics

9.1 Introduction

This section demonstrates how to use the ECA Workspace to evaluate events that involve component failures.

- ◊ Conditions are defined as operational occurrences (both real and hypothetical) that do not involve the occurrence of initiating events. Instead, a condition exists over a period of time that degrades the ability of the plant to respond to upsets.

- As an example of a condition assessment we will walk through the evaluation of a diesel generator unavailability event at the Generic PWR plant. Topics to be covered will be:
  - ◊ A discussion of the event to be modeled.
  - ◊ A discussion of the preliminary steps to analyze the event.
  - ◊ A demonstration of ECA Workspace to evaluate the event.
- The basic approach to the condition type of evaluation will be to determine the CCDP for the event occurring during the period in which the diesel was disabled.
  - ◊ We will then compare this CCDP with the CDP for the same period had the diesel been in its nominal state.
  - ◊ The difference in these two probabilities is a quantity that we will refer to as the *event importance*.
- The ECA Workspace will handle most of the calculational details of the analysis.
  - ◊ The analyst must
    - Determine the basic events in the PRA model that have to be modified to map the event into the model
    - Enter these changes through the GEM Condition Analysis interface

9.2 Event Description

In our example a diesel generator has failed a periodic functional test. When repair crews investigated, they found that the diesel generator (DG A) in division 1A of ac power had a plugged fuel filter. Some other relevant facts are:

- Investigation showed that the machine had been non-functional for 100 hours.
- The other diesel generator (DG B) was also checked, but the plugging was found only in Diesel Generator A.
    - ◊ We are going to assume that a common cause failure was still *possible*. Declaring the failure to be independent requires much more evidence than we have at hand.
- There was no evidence that, had there been a diesel demand during this period, recovery of the diesels would have been affected by other (non-filter) issues.
    - ◊ We are going to leave the diesel recovery events in the SPAR model at their nominal values.
    - ◊ We are going to assume that recovery of the other components (if applicable) are left at their nominal values.

9.3 Preliminary Steps for Condition Assessment

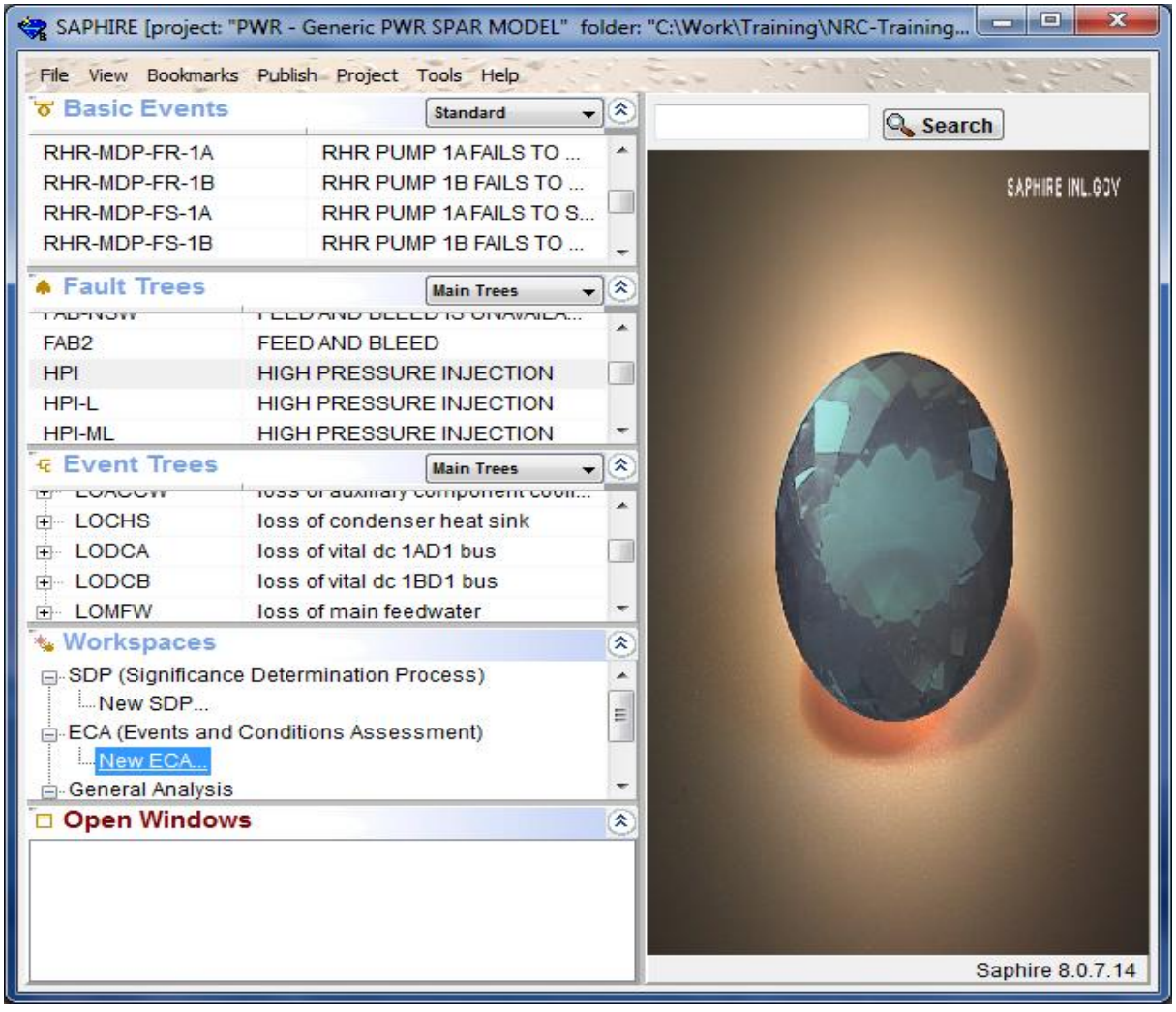
Before we start the ECA Workspace and enter data we should know what model modifications we intend to make. From the event description we know that Diesel Generator A was failed for 100 hours, and that the potential for common cause could not be ruled out.

- For this analysis, we will use the Generic PWR model.
- The same diesel generator related events may appear in many fault trees since it is a support system and, consequently, transfers emergency power dependency to many front-line trees.
- From the EPS fault trees, we decide that we can map this event into the model by setting the basic event EPS-DGN-FS-DGA to **TRUE**. By recognizing that the Unit 1 diesels are a CCCG of size two, we know that we must also set EPS-DGN-CF-1ABRUN to FALSE.
- There is also one diesel generator at Unit 2 that appear in the EPS fault tree. Note that there is another CCCG consisting of all three diesels, represented by events EPS-DGN-CF-DG1ABUN2S and EPS-DGN-CF- DG1ABUN2R. To ensure that the values for these events are adjusted properly, we must also set the event representing the unobserved failure mode (EPS-DGN-FR-DGA) to 1.0.
- We can now start the ECA Workspace and enter our data.

9.4 ECA Workspace Walk-Through

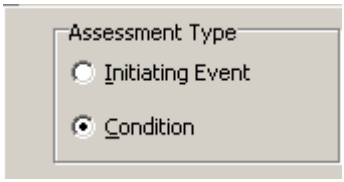
This section will provide a step-by-step guide to performing an event evaluation for the condition described in the preceding section.

- Start the ECA workspace by double-clicking the **New ECA**… option in the Workspaces list panel.



This example uses the Generic PWR SPAR model. Make sure this project is opened (i.e., currently working project).

- From the main screen, select the **Condition** radio button and select the **Next** button.

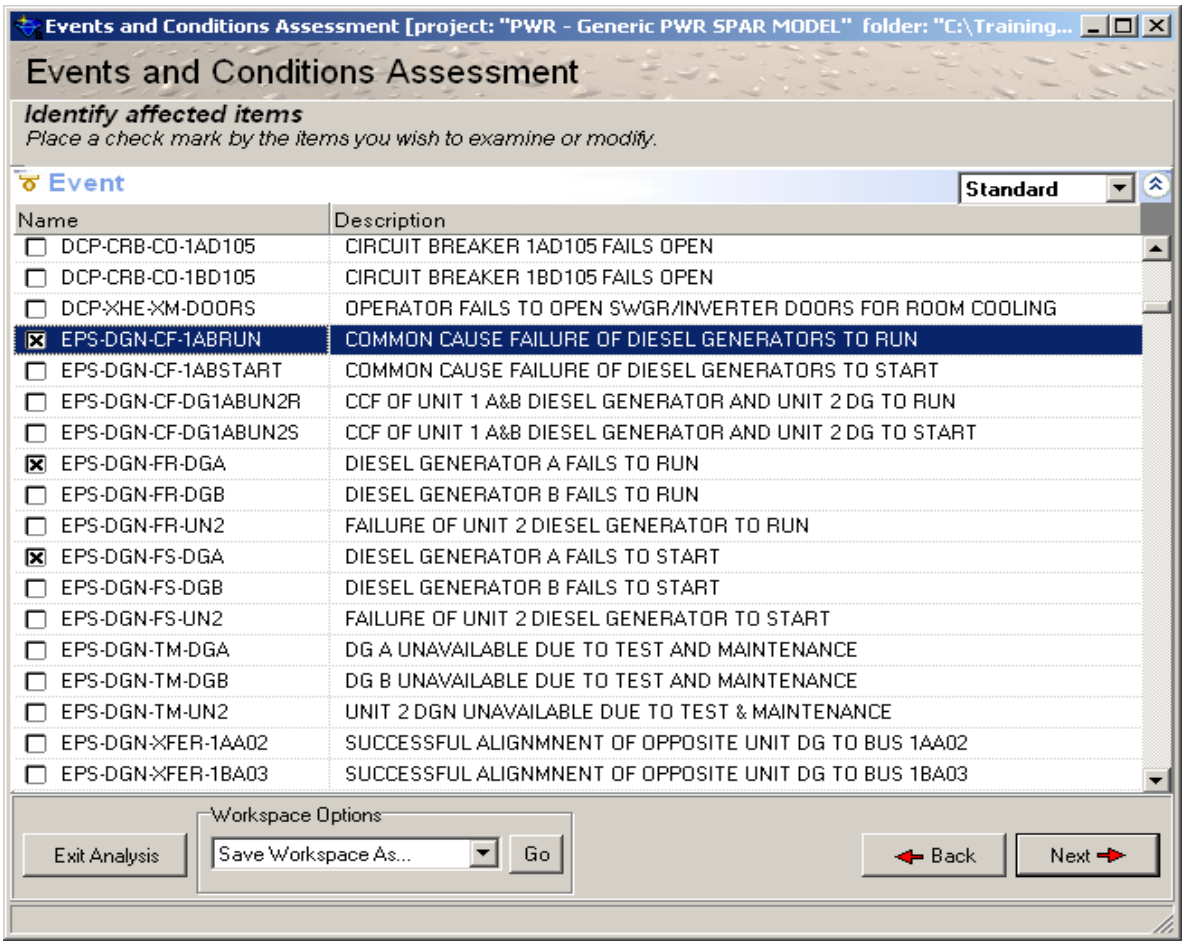


- The steps we are going to go through are:

1. Make a blank analysis record in the database (a place to do the analysis)
2. Add any required event modifications
3. Process the analysis
4. Specify the duration of the condition
5. Review the results

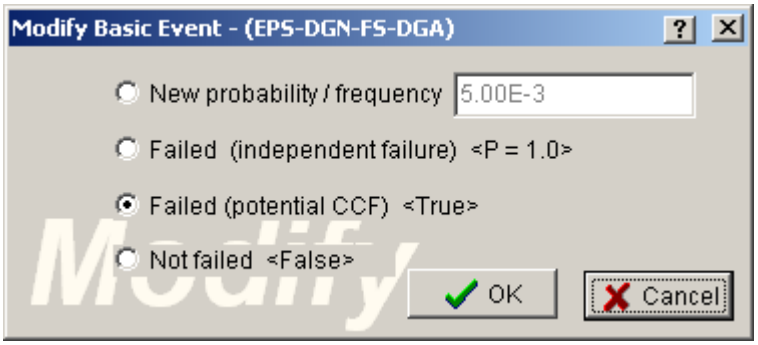
- The ECA workshop will display the "identify affected items" screen, which lists all the basic events that are in the model. From the list of basic events, select the ones that match the assessment, by **clicking** the check box next to them.

- The "Identify affected items" screen allows the analyst to select those basic events that need to be modified based on the analysis, by **clicking** the check box next to them.

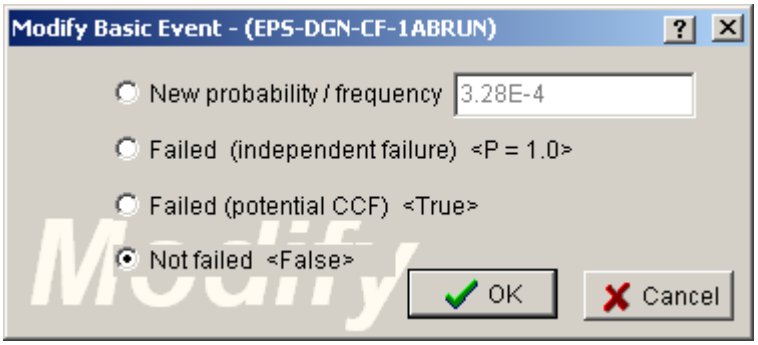


- The basic events that need to be included for this condition assessment are located by scrolling down the list and checking the check box. The basic events are EPS-DGN-CF-1ABRUN, EPS-DGN-FR-DGA, and EPS-DGN-FS-DGA.

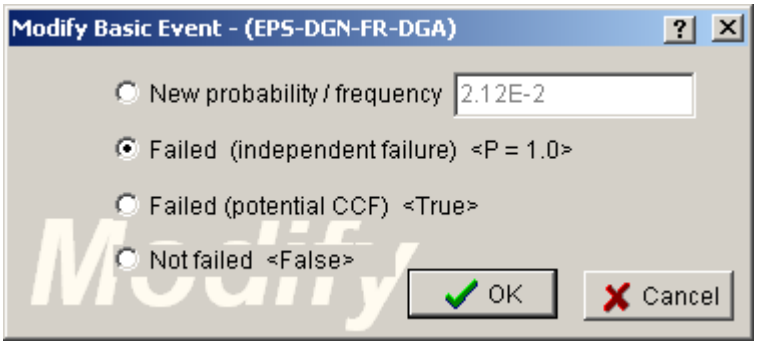
- Set **EPS-DGN-FS-DGA** to TRUE.



- Set **EPS-DGN-CF-1ABRUN** to FALSE.

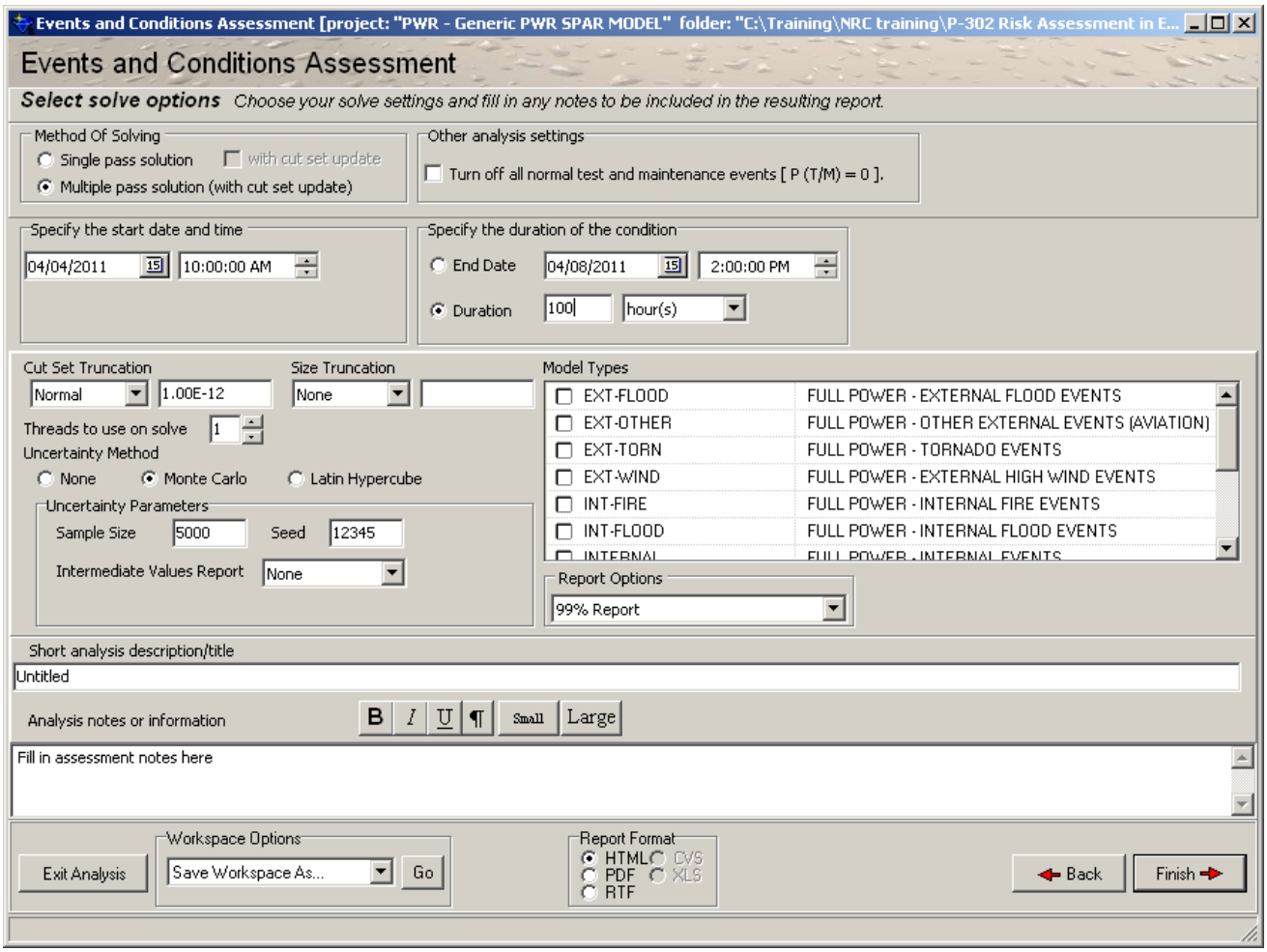


- Set **EPS-DGN-FR-DGA** to 1.0.

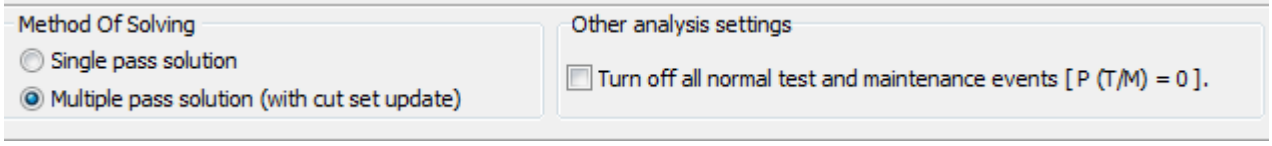


- Once the the basic events have been adjusted select the **Next** button.

The following evaluation screen will appear. Each section will be discussed.



Method of Solving

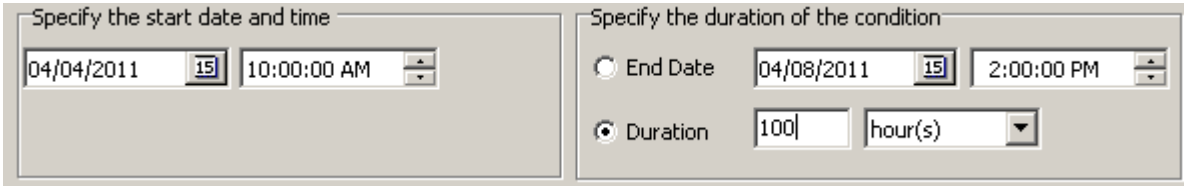


The difference between the single pass with cut set update and the multi-pass routines are:

- The multiple pass solution algorithm will ensure that all sequence post-processing rules are applied even when basic events in the model are specified as a logical "True." The "single pass with cut set update option" does not.
- The multiple pass algorithm will remove non-minimal cut sets (if generated from a post-processing rule) by automatically performing a cut set update.
- SAPHIRE 8 performs the "base case" and the "new case" solving at the same truncation level for both algorithms.

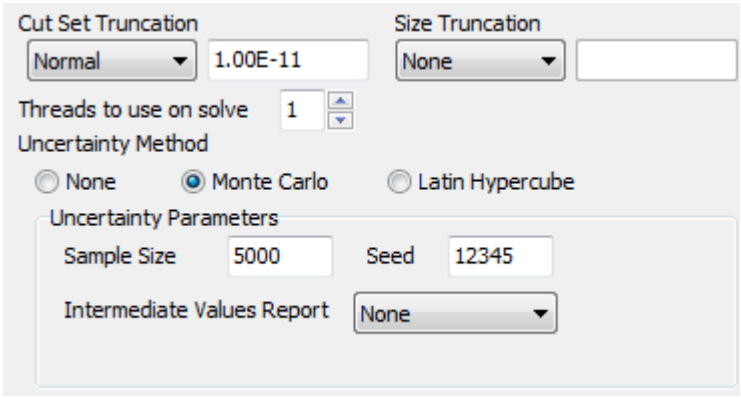
- The "Turn off all T&M events will set all test and maintenance events to 0.0 and then resolve the model, prior to evaluation.

Specify Duration



- The duration of the event can be specified by entering the start of the event (both day and time) and the end of the event (both day and time) or the number of hours the event lasted. In this case, the duration of 100 hours was specified.

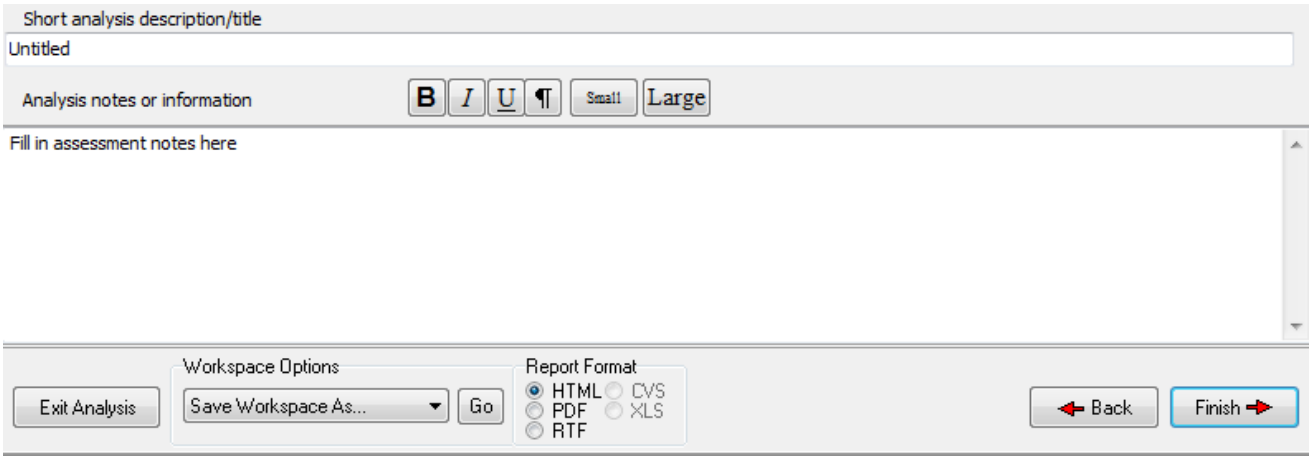
Cut Set Truncation



- The nominal truncation will solve all sequences at this truncation (it defaults to the model's default).

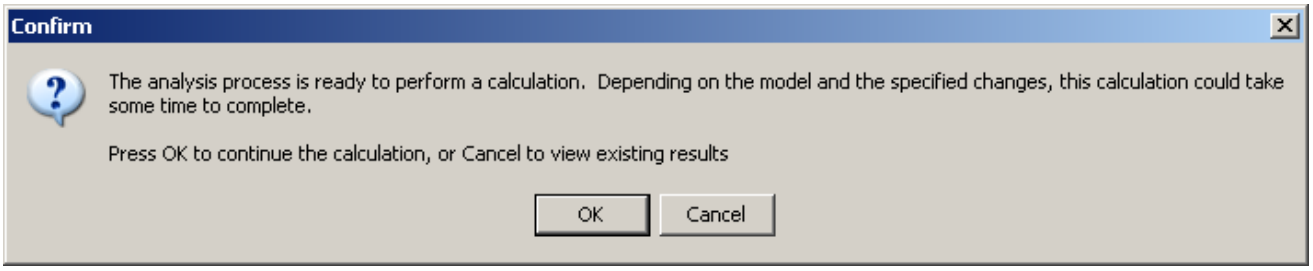
- Uncertainty will be evaluated when solving the model (see NUREG/CR-7039, Volume 5, Section2.7).

Description



A title can be specified to identify the type of assessment being performed. Also, a description of the event and the components that were affected can be described in the analysis notes block.

- Once all of the information has been selected, click the Finish button and SAPHIRE will process the analysis. The following screen just cautions the analyst that the evaluation may take extra time depending upon the complexity of the model.



- When finished, SAPHIRE will display the Event Assessment screen. The Δ**CCDP** for the event will also be displayed.

- Once the evaluation is complete SAPHIRE will provide a summary report of the evaluation. Each of the pieces of the output will be discussed.

The first part is the overall result.

Condition Assessment Summary

Event Date	4/4/2011 10:00:00 AM to 4/8/2011 2:00:00 PM
Duration	100 hours
CCDP	8.75E-7
CDP	5.02E-7
Δ CDP	**3.74E-7**

Solve Settings

Solve Settings

Cut set Truncation	Normal 1.00E-12
Size Truncation	None
Solve Method	Multiple Pass

Summary of Events Changed

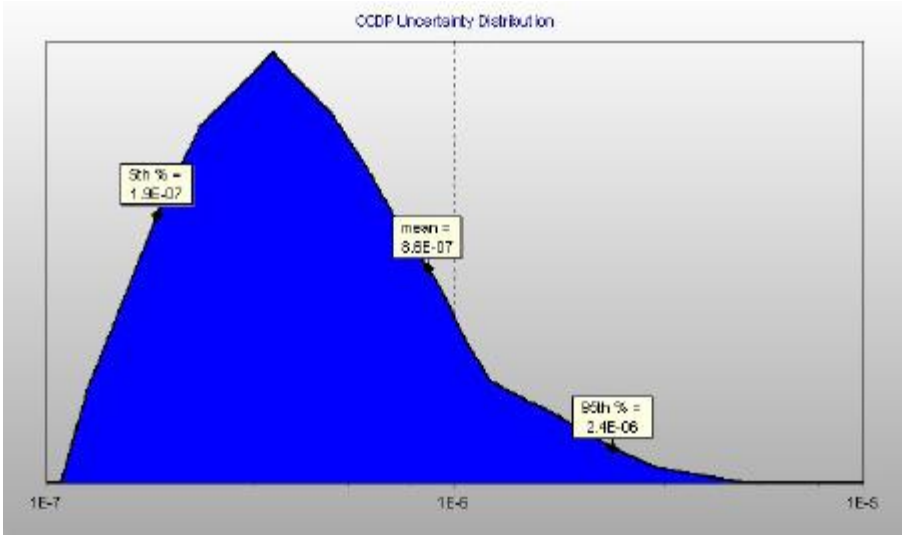
Summary of Conditional Event Changes

Event	Description	Cond Type	Cond Value	Nominal Type	Nominal Value
EPS-DGN-CF-1ABRUN	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO RUN	F	False	C	3.28E-4
EPS-DGN-FR-DGA	DIESEL GENERATOR A FAILS TO RUN	C	1.00E+0	C	2.12E-2
EPS-DGN-FS-DGA	DIESEL GENERATOR A FAILS TO START	T	True	1	5.00E-3
EPS-DGN-CF-1ABSTART	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO START	C	1.15E-2	C	5.75E-5
EPS-DGN-CF-1ABRUN	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO RUN	F	False	C	3.28E-4
EPS-DGN-CF-DG1ABUN2	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO RUN	C	6.66E-4	C	1.21E-4
EPS-DGN-CF-DG1ABUN2	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO START	C	3.72E-3	C	1.86E-5

Uncertainty Analysis (if performed)

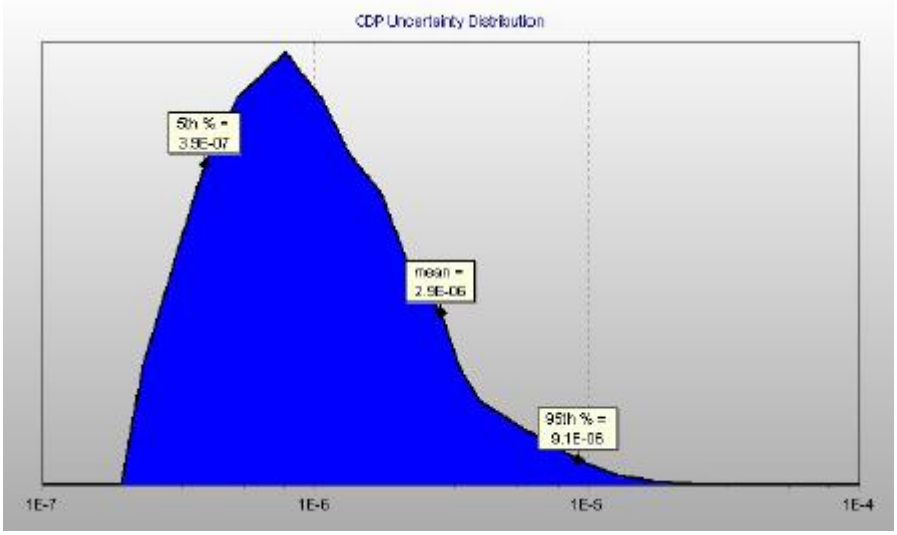
CCDP Uncertainty Distribution

5%	Median	Point Estimate	Mean	95%	Seed	Sample Size	Method
1.87E-7	6.05E-7	8.75E-7	8.63E-7	2.42E-6	12345	5000	Monte Carlo



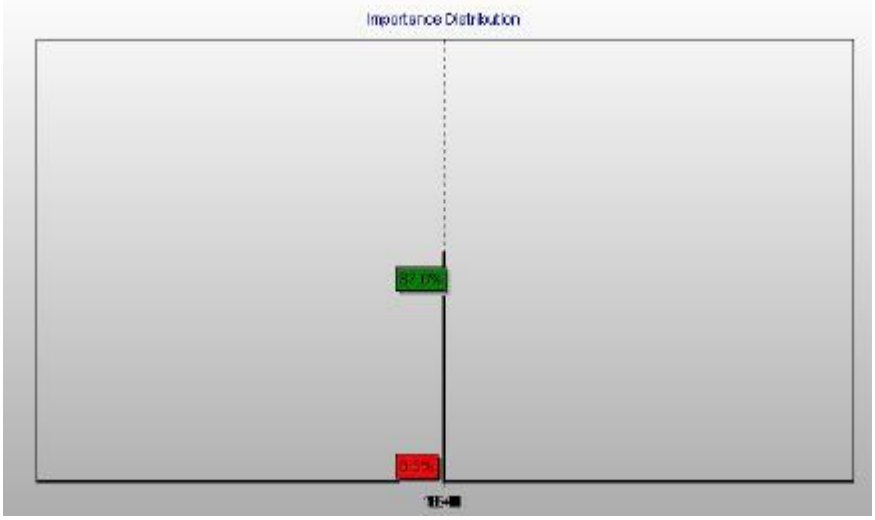
CDP Uncertainty Distribution

5%	Median	Point Estimate	Mean	95%	Seed	Sample Size	Method
3.93E-7	1.76E-6	9.89E-6	2.90E-6	9.15E-6	12345	5000	Monte Carlo



Importance Distribution

5%	Median	Point Estimate	Mean	95%	Seed	Sample Size	Method
-7.29E-6	-9.84E-7	-9.02E-6	-2.04E-6	-1.15E-7	12345	5000	Monte Carlo



Results from the evaluation listing the dominant event tree and dominant sequences.

Event Tree Dominant Results

Only items contributing at least 1.0% to the total CCDP are displayed.

Event Tree	CCDP	CDP	Delta CDP	Description
LOOPGR	1.85E-7	8.98E-9	1.76E-7	loss of offsite power (Grid related)
LOOPWR	1.13E-7	4.73E-9	1.08E-7	loss of offsite power (Weather related)
LOOPSC	7.05E-8	3.73E-9	6.67E-8	loss of offsite power (Switchyard centered)
LOOPPC	1.12E-8	6.20E-10	1.06E-8	loss of offsite power (Plant Centered)
TRANS	1.91E-8	9.09E-9	9.99E-9	general transient
Total	**7.67E-5**	**100%**		

Dominant Sequence Results

Only items contributing at least 1.0% to the total CCDP are displayed.

Event Tree	Sequence	CCDP	CDP	Delta CDP	Flagset	Description
LOOPGR	16-03-10	5.05E-8	1.58E-9	4.89E-8	ETF-SBO-GR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, /BP2, OPR-04H, DGR-04H, AFW-MAN, SG-DEP-LT1
LOOPGR	15	4.80E-8	2.70E-9	4.53E-8	ETF-LOOP-GR	/RPS-L, /EPS, AFW-L, FAB-L
LOOPGR	16-06	4.21E-8	1.31E-9	4.07E-8	ETF-SBO-GR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, BP2, OPR-04H, DGR-04H
LOOPWR	16-03-10	4.17E-8	1.42E-9	4.03E-8	ETF-SBO-WR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, /BP2, OPR-04H, DGR-04H, AFW-MAN, SG-DEP-LT1
LOOPWR	16-06	3.47E-8	1.19E-9	3.36E-8	ETF-SBO-WR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, BP2, OPR-04H, DGR-04H
LOOPSC	15	2.68E-8	1.50E-9	2.53E-8	ETF-LOOP-SC	/RPS-L, /EPS, AFW-L, FAB-L
LOOPGR	16-45	1.81E-8	5.45E-10	1.76E-8	ETF-SBO-GR	/RPS-L, EPS, AFW-B, OPR-01H, DGR-01H
LOOPSC	16-03-10	1.45E-8	4.53E-10	1.41E-8	ETF-SBO-SC	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, /BP2, OPR-04H, DGR-04H, AFW-MAN, SG-DEP-LT1
LOOPWR	15	1.24E-8	6.93E-10	1.17E-8	ETF-LOOP-WR	/RPS-L, /EPS, AFW-L, FAB-L
LOOPSC	16-06	1.21E-8	3.77E-10	1.17E-8	ETF-SBO-SC	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, BP2, OPR-04H, DGR-04H
LOOPGR	02-05	9.89E-9	1.26E-9	8.63E-9	ETF-LOOP-GR	/RPS-L, /EPS, /AFW-L, /PORV-L, LOSC-L, /RSD-L, /BP1, BP2, OPR-02H, HPI-L
LOOPWR	16-03-04	8.29E-9	2.81E-10	8.01E-9	ETF-SBO-WR	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, /BP1, /BP2, OPR-04H, DGR-04H, /AFW-MAN, /CST-REFILL-LT1, SG-DEP-LT2, PWR-REC-24H
LOOPGR	16-10-2	8.21E-9	4.00E-10	7.81E-9	ETF-LOOPGR-MLOCA	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, BP1, BP2, /OPR-02H, /HPI, /SSC, LPR
TRANS	02-02-09	7.33E-9	3.56E-10	6.97E-9	ETF-TRANS-SLOCA	/RPS, /AFW, /PORV, LOSC, /RCPT, /RSD, /BP1, BP2, HPI, /SSC1, LPI
LOOPWR	16-45	6.26E-9	2.00E-10	6.06E-9	ETF-SBO-WR	/RPS-L, EPS, AFW-B, OPR-01H, DGR-01H
LOOPSC	16-45	6.20E-9	1.83E-10	6.01E-9	ETF-SBO-SC	/RPS-L, EPS, AFW-B, OPR-01H, DGR-01H
LOOPPC	15	5.33E-9	2.93E-10	5.04E-9	ETF-LOOP-PC	/RPS-L, /EPS, AFW-L, FAB-L
LOOPSC	16-10-2	4.59E-9	2.23E-10	4.37E-9	ETF-LOOPSC-MLOCA	/RPS-L, EPS, /AFW-B, /PORV-B, /RSD-B, BP1, BP2, /OPR-02H, /HPI, /SSC, LPR
Total		**7.67E-5**	**100%**			

A report of the top 1% dominant cut sets for each dominant sequence is provided. (Just the cut sets for sequence LOOPGR 16-03-10 will be illustrated.)

Cut Set Report - LOOPGR 16-03-10

#	Prob/Freq	Total %	Cut Set
	4.42E-6	100	Displaying 369 of 369 Cut Sets.
1	1.05E-6	23.7	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-TM-DGB,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
2	1.01E-6	22.7	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-CF-1ABSTART,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
3	4.37E-7	9.88	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-FS-DGB,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
4	4.33E-7	9.8	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-FR-DGB,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,OEP-XHE-XX-NR04HGR1,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
5	3.25E-7	7.36	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-CF-DG1ABUN2S,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
6	2.62E-7	5.93	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DUAL-UNITLOOP,EPS-SEQ-FC-DGB,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
7	2.18E-7	4.94	IE-LOOPGR,ACP-CRB-CC-BA30,AFW-XHE-XM-TDPBD,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
8	1.70E-7	3.84	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DGN-FR-DGB,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,OEP-XHE-XL-NR04HGR,OEP-XHE-XX-NR04HGR2,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
9	1.21E-7	2.75	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,NSW-MDP-TM-TRNB,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
10	8.74E-8	1.98	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,NSW-MOV-CC-1669A,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2
11	5.97E-8	1.35	IE-LOOPGR,AFW-XHE-XM-TDPBD,EPS-DUAL-UNITLOOP,EPS-WILSON-SWYD,EPS-XHE-XL-NR04H,EPS-XHE-XM-DGUN2,NSW-FAN-TM-TRNB,OEP-XHE-XL-NR04HGR,/RCS-MDP-LK-BP1,/RCS-MDP-LK-BP2

Referenced Events- lists all of the basic events that part of the cut sets generated from the analysis.

Event	Description	Probability
ACP-CRB-CC-BA30	FAILURE OF SWITCHYARD AC BREAKER BA30 TO OPEN	2.50E-3
ACP-TAC-FC-SWYRD	FAILURE OF SWITCHYARD AC POWER TO BUSES	7.97E-5
ACP-XHE-XM-WILNLP	OPERATOR FAILS TO ALIGN PLANT WILSON GIVEN NON-LOOP IE	1.00E-1
ACW-P1-RUNNING	ACW PUMP P1 RUNNING	5.00E-1
ACW-P2-RUNNING	ACW PUMP P2 RUNNING	5.00E-1
AFW-MDP-FR-4002	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS TO RUN	5.38E-4
AFW-MDP-FS-4002	AFW MOTOR-DRIVEN PUMP P4-4002 FAILS TO START	1.50E-3
AFW-MDP-TM-4002	AFW MDP P4-4002 UNAVAILABLE DUE TO TEST AND MAINTENANCE	4.00E-3
AFW-MOV-CC-HV5106	STEAM SUPPLY MOV HV5106 FAILS TO OPEN	1.00E-3
AFW-MOV-OO-FV5154	FAILURE OF AFW MDP B MINFLOW MOV 5154 TO CLOSE	1.00E-3
AFW-TDP-FR-4001	TURBINE DRIVEN FEED PUMP P4-001 FAILS TO RUN	4.10E-3
AFW-TDP-FS-4001	TURBINE DRIVEN FEED PUMP P4-001 FAILS TO START	7.00E-3
AFW-TDP-TM-4001	AFW TDP PUMP P4-001 IS IN TEST OR MAINTENANCE	5.00E-3
AFW-XHE-XM-TDPBD	OPERATOR FAILS TO CONTROL AFW TDP AFTER BATTERY DEPLETION	3.00E-1
AFW-XHE-XM-TDPBD3	OPERATOR FAILS TO CONTROL AFW TDP AFTER BATTERY DEPLETION; NON SBO	1.00E-1
EPS-DGN-CF-1ABSTART	COMMON CAUSE FAILURE OF DIESEL GENERATORS TO START	1.15E-2
EPS-DGN-CF-	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO RUN	6.66E-4

Event	Description	Probability
DG1ABUN2R		
EPS-DGN-CF-DG1ABUN2S	CCF OF UNIT 1 A&B DIESEL GENERATOR AND UNIT 2 DG TO START	3.72E-3
EPS-DGN-FR-DGB	DIESEL GENERATOR B FAILS TO RUN	2.12E-2
EPS-DGN-FS-DGB	DIESEL GENERATOR B FAILS TO START	5.00E-3
EPS-DGN-TM-DGB	DG B UNAVAILABLE DUE TO TEST AND MAINTENANCE	1.20E-2
EPS-DUAL-UNITLOOP	DUAL UNIT LOOP	5.79E-1
EPS-SEQ-FC-DGB	DGB Sequencer FailsTo Operate	3.00E-3
EPS-WILSON-SWYD	PLANT WILSON UNAVAIL. DUE TO GRID RELATED LOOP	4.00E-1
EPS-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER EMERGENCY DIESEL IN 1 HOUR	7.86E-1
EPS-XHE-XL-NR04H	OPERATOR FAILS TO RECOVER EMERGENCY DIESEL IN 4 HOURS	5.57E-1
EPS-XHE-XL-NR24H4	OPERATOR FAILS TO RECOVER EMERGENCY DIESEL IN 24 HOURS (GIVEN FAILURE AT 4)	2.84E-1
EPS-XHE-XM-DGUN2	OPERATOR FAILS TO CROSS-TIE UNIT 2 DIESEL GENERATOR	1.00E+0
IE-LOOPGR	LOSS OF OFFSITE POWER INITIATOR (GRID-RELATED)	1.86E-2
IE-LOOPPC	LOSS OF OFFSITE POWER INITIATOR (PLANT-CENTERED)	2.07E-3
IE-LOOPSC	LOSS OF OFFSITE POWER INITIATOR (SWITCHYARD-RELATED)	1.04E-2
IE-LOOPWR	LOSS OF OFFSITE POWER INITIATOR (WEATHER-RELATED)	4.83E-3
IE-TRANS	TRANSIENT	8.00E-1
NSW-FAN-TM-TRNB	NSCW TRAIN B TOWER FANS Test & Maint(PSA value)	6.83E-4
NSW-MDP-TM-TRNB	NSW TRAIN B MDPS UNAVAILABLE DUE MAINTENANCE (PSA PROB)	1.39E-3
NSW-MOV-CC-1669A	NSW TRAIN B MOV 1669A TO CT FAILS TO OPEN	1.00E-3
NSW-MOV-CF-16689A	NSW TRAIN A/B MOV 1668A/1669A TO CT CCF TO OPEN	2.28E-5
NSW-P1P3R-P5ST	P001, P003 RUN AND P005 STANDBY	3.33E-1
NSW-P1P5R-P3ST	P001, P005 RUN AND P003 STANDBY	3.33E-1
NSW-P2P4R-P6ST	P002, P004 RUN AND P006 STANDBY	3.33E-1
NSW-P2P6R-P4ST	P002, P006 RUN AND P004 STANDBY	3.33E-1
NSW-P3P5R-P1ST	P003, P005 RUN AND P001 STANDBY	3.33E-1
NSW-P4P6R-P2ST	P004, P006 RUN AND P002 STANDBY	3.33E-1
OEP-XHE-XL-NR01H	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR	5.30E-1
OEP-XHE-XL-NR01HGR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR (GRID-RELATED)	6.11E-1
OEP-XHE-XL-NR01HSC	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR (SWITCHYARD)	3.78E-1
OEP-XHE-XL-NR01HWR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 1 HOUR (WEATHER-RELATED)	6.56E-1
OEP-XHE-XL-NR02HGR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 2 HOURS (GRID-RELATED)	3.56E-1
OEP-XHE-XL-NR04HGR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 4 HOURS (GRID-RELATED)	1.54E-1
OEP-XHE-XL-NR04HSC	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 4 HOURS (SWITCHYARD)	7.86E-2
OEP-XHE-XL-NR04HWR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 4 HOURS (WEATHER-RELATED)	3.82E-1
OEP-XHE-XL-NR24H4WR	OPERATOR FAILS TO RECOVER OFFSITE POWER IN 24 HOURS (FAIL @ 4) (WEATHER-RELATE D)	2.99E-1
OEP-XHE-XX-NR01HGR1	CONVOLUTION FACTOR FOR 1FTR-OPR (1HR-GR AVAIL)	1.75E-1
OEP-XHE-XX-NR01HGR2	CONVOLUTION FACTOR FOR 2FTR-OPR (1HR-GR AVAIL)	5.25E-2
OEP-XHE-XX-NR01HSC1	CONVOLUTION FACTOR FOR 1FTR-OPR (1HR-SC AVAIL)	1.58E-1
OEP-XHE-XX-NR01HWR1	CONVOLUTION FACTOR FOR 1FTR-OPR (1HR-WR AVAIL)	4.08E-1
OEP-XHE-XX-NR01HWR2	CONVOLUTION FACTOR FOR 2FTR-OPR (1HR-WR AVAIL)	2.80E-1
OEP-XHE-XX-NR04HGR1	CONVOLUTION FACTOR FOR 1FTR-OPR (4HR-GR AVAIL)	2.34E-1
OEP-XHE-XX-NR04HGR2	CONVOLUTION FACTOR FOR 2FTR-OPR (4HR-GR AVAIL)	9.18E-2
OEP-XHE-XX-NR04HSC1	CONVOLUTION FACTOR FOR 1FTR-OPR (4HR-SC AVAIL)	2.40E-1
OEP-XHE-XX-NR04HSC2	CONVOLUTION FACTOR FOR 2FTR-OPR (4HR-SC AVAIL)	9.91E-2
OEP-XHE-XX-NR04HWR1	CONVOLUTION FACTOR FOR 1FTR-OPR (4HR-WR AVAIL)	5.28E-1
OEP-XHE-XX-NR04HWR2	CONVOLUTION FACTOR FOR 2FTR-OPR (4HR-WR AVAIL)	4.05E-1
RCS-MDP-LK-BP1	RCP SEAL STAGE 1 INTEGRITY (BINDING/POPPING OPEN) FAILS	1.25E-2
RCS-MDP-LK-BP2	RCP SEAL STAGE 2 INTEGRITY (BINDING/POPPING OPEN) FAILS	2.00E-1

Lastly, the report provides event importance measures from the analysis. The importance measures list only those events that are greater than a predefined truncation.

RIR > 2.00E+00 (> 50 for illustration)
Event Tree Importance

Group

Event	Occur.	Prob.	FV	RIR	RRR	Bb	RII	RRI	Uncert.
IE-XLOCA	1	1.00E-7	1.31E-3	1.31E+4	1.00E+0	1.00E+0	1.00E+0	1.00E-7	1.83E-7
NSW-MDP-CF-RUN	214	2.76E-8	8.20E-5	2.68E+3	1.00E+0	2.05E-1	2.05E-1	6.27E-9	1.96E-8
RPS-ROD-CF-RCCAS	320	1.21E-6	3.33E-3	2.53E+3	1.00E+0	1.93E-1	1.93E-1	2.54E-7	2.49E-7
RPS-BME-CF-RTBAB	158	1.61E-6	4.07E-3	2.34E+3	1.00E+0	1.79E-1	1.79E-1	3.11E-7	8.24E-7
IE-ISL-RHR	3	5.62E-6	1.03E-2	1.82E+3	1.01E+0	1.39E-1	1.39E-1	7.84E-7	0.00E+0
RPS-TXX-CF-6OF8	151	2.70E-6	3.39E-3	1.21E+3	1.00E+0	9.24E-2	9.24E-2	2.59E-7	1.04E-6
IE-LONSW	1409	4.00E-4	3.71E-1	9.28E+2	1.59E+0	7.10E-2	7.09E-2	2.84E-5	4.01E-5
AFW-PMP-CF-RUN	105	1.31E-7	9.89E-5	7.41E+2	1.00E+0	5.66E-2	5.66E-2	7.56E-9	1.64E-8
AFW-CKV-CF-125678	94	1.12E-7	8.42E-5	7.40E+2	1.00E+0	5.65E-2	5.65E-2	6.43E-9	1.50E-8
AFW-CKV-CF-113456	94	1.15E-7	8.66E-5	7.40E+2	1.00E+0	5.65E-2	5.65E-2	6.62E-9	1.38E-8
AFW-CKV-CF-001214	72	5.80E-8	4.35E-5	7.37E+2	1.00E+0	5.63E-2	5.63E-2	3.32E-9	1.06E-8
AFW-CKV-CF-0331358	72	5.80E-8	4.35E-5	7.37E+2	1.00E+0	5.63E-2	5.63E-2	3.32E-9	1.06E-8
AFW-TNK-FC-CST1	70	4.80E-8	3.60E-5	7.37E+2	1.00E+0	5.63E-2	5.63E-2	2.75E-9	4.93E-9
ACP-TAC-FC-SWYRD	7138	7.97E-5	1.52E-2	1.90E+2	1.02E+0	1.44E-2	1.44E-2	1.16E-6	1.63E-6
IE-ISL-LPI	3	3.27E-6	6.13E-4	1.89E+2	1.00E+0	1.44E-2	1.44E-2	4.69E-8	0.00E+0
NSW-MDP-CF-START	1481	1.40E-5	2.43E-3	1.47E+2	1.00E+0	1.12E-2	1.12E-2	1.86E-7	2.32E-7
DCP-BAT-CF-ALL	6	6.43E-8	7.05E-6	1.10E+2	1.00E+0	8.37E-3	8.37E-3	5.38E-10	2.31E-9
IE-LLOCA	148	2.50E-6	2.61E-4	1.06E+2	1.00E+0	7.99E-3	7.99E-3	2.00E-8	3.65E-8
NSW-FAN-CF-FSALL	229	4.00E-6	3.67E-4	9.05E+1	1.00E+0	6.84E-3	6.84E-3	2.80E-8	6.08E-8
NSW-FAN-CF-FRALL	42	2.64E-7	2.37E-5	8.86E+1	1.00E+0	6.70E-3	6.70E-3	1.81E-9	2.55E-9
ACP-BAC-LP-1BA03	543	9.60E-6	7.51E-4	6.54E+1	1.00E+0	4.93E-3	4.93E-3	5.74E-8	6.69E-8
HPI-TNK-FC-RWST	7	4.80E-8	3.13E-6	6.47E+1	1.00E+0	4.87E-3	4.87E-3	2.40E-10	4.27E-10

FV > 5.00E-03 (>0.1 for illustration)
Event Tree Importance

Group

Event	Occur.	Prob.	FV	RIR	RRR	Bb	RII	RRI	Uncert.
RCS-MDP-LK-BP2	27783	2.00E-1	5.47E-1	2.82E+0	2.02E+0	1.78E-4	1.39E-4	3.86E-5	2.15E-5
EPS-WILSON-SWYD	31945	4.00E-1	4.38E-1	1.66E+0	1.78E+0	8.37E-5	5.02E-5	3.35E-5	1.34E-5
EPS-DUAL-UNITLOOP	25999	5.79E-1	4.23E-1	1.31E+0	1.73E+0	5.59E-5	2.35E-5	3.24E-5	1.38E-5
IE-LONSW	1409	4.00E-4	3.71E-1	9.28E+2	1.59E+0	7.10E-2	7.09E-2	2.84E-5	4.01E-5
NSW-XHE-XL-NOREC	1404	3.40E-1	3.71E-1	1.65E+0	1.59E+0	7.83E-5	4.99E-5	2.84E-5	1.27E-5
EPS-XHE-XM-DGUN2	11463	1.00E+0	3.64E-1	1.00E+0	1.57E+0	2.78E-5	0.00E+0	2.78E-5	0.00E+0
EPS-XHE-XL-NR04H	4641	5.57E-1	2.41E-1	1.19E+0	1.32E+0	3.31E-5	1.47E-5	1.84E-5	2.24E-6
IE-LOOPGR	11976	1.86E-2	2.11E-1	1.22E+1	1.27E+0	8.69E-4	8.53E-4	1.62E-5	2.29E-5
AFW-XHE-XM-TDPBD3	3204	1.00E-1	1.79E-1	2.61E+0	1.22E+0	1.37E-4	1.23E-4	1.37E-5	0.00E+0
NSW-P2P4R-P6ST	3704	3.33E-1	1.45E-1	1.27E+0	1.16E+0	3.15E-5	2.08E-5	1.06E-5	0.00E+0
NSW-P2P6R-P4ST	3704	3.33E-1	1.45E-1	1.27E+0	1.16E+0	3.15E-5	2.08E-5	1.06E-5	0.00E+0
NSW-P4P6R-P2ST	3704	3.33E-1	1.45E-1	1.27E+0	1.16E+0	3.15E-5	2.08E-5	1.06E-5	0.00E+0
NSW-P1P3R-P5ST	3208	3.33E-1	1.42E-1	1.26E+0	1.16E+0	3.06E-5	2.03E-5	1.04E-5	0.00E+0
NSW-P1P5R-P3ST	3208	3.33E-1	1.42E-1	1.26E+0	1.16E+0	3.06E-5	2.03E-5	1.04E-5	0.00E+0
NSW-P3P5R-P1ST	3208	3.33E-1	1.42E-1	1.26E+0	1.16E+0	3.06E-5	2.03E-5	1.04E-5	0.00E+0
ACP-XHE-XM-	1736	1.00E+0	1.39E-1	1.00E+0	1.16E+0	1.06E-5	0.00E+0	1.06E-5	0.00E+0

Event	Occur.	Prob.	FV	RIR	RRR	Bb	RII	RRI	Uncert.
REC4160A									
IE-LOACA	1736	9.00E-3	1.39E-1	1.63E+1	1.16E+0	1.18E-3	1.17E-3	1.06E-5	3.76E-6
IE-LOOPWR	7492	4.83E-3	1.29E-1	2.76E+1	1.15E+0	2.04E-3	2.03E-3	9.86E-6	1.39E-5
AFW-XHE-XM-TDPBD	3532	3.00E-1	1.26E-1	1.28E+0	1.14E+0	3.08E-5	2.15E-5	9.24E-6	7.18E-6
AFW-MDP-TM-4002	1210	4.00E-3	1.13E-1	2.88E+1	1.13E+0	2.13E-3	2.12E-3	8.63E-6	5.38E-6
OEP-XHE-XL-NR04HGR	3711	1.54E-1	1.08E-1	1.59E+0	1.12E+0	5.34E-5	4.52E-5	8.22E-6	4.29E-6

- At this point, you have your report documenting details for the analysis and the results of the analysis.
-

But, again, the analysis is just beginning…

- Evaluate the resulting cut sets.
- Review the importance measures.
- Consider model applicability/completeness.
- Use engineering experience along with PRA results.

9.5 Workshop

10. CONSIDERATIONS OF UNCERTAINTY

Section 10 describes uncertainty analysis utilized in the ECA Workspace. An overview of uncertainty methods, parameter uncertainty, model uncertainty, steps required to perform an uncertainty evaluation, and an example uncertainty analysis will be presented.

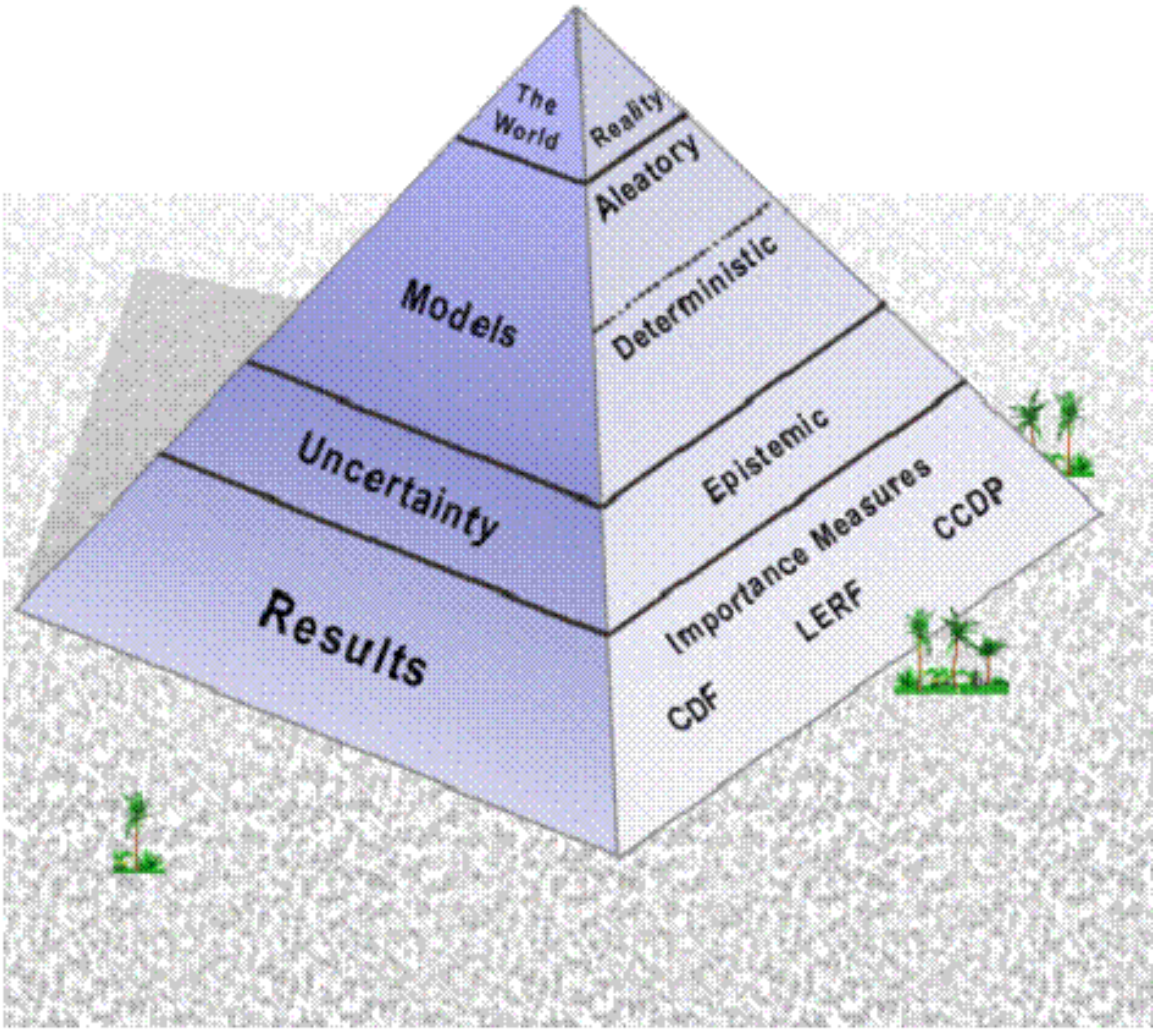
Learning Objectives

- Describe the difference between aleatory and epistemic uncertainty.
- Indicate the two Monte Carlo uncertainty analysis techniques available in the ECA Workspace.
- Describe the major topic areas that need to be addressed to incorporate parameter uncertainty.
- Outline the steps to perform an uncertainty evaluation within the ECA Workspace.

Section 10 Topics

10.1 Overview of Uncertainty

- Uncertainty analysis estimates the variability of the event analysis results (e.g., CCDP, $\text{Importance}_{\text{event}}$) resulting from uncertainties in:
  - ◊ Basic event probabilities
  - ◊ Initiating event frequency
  - ◊ Model structure
  - ◊ Analysis assumptions.
- In general, a PRA has two parts to it.
  - ◊ ***Deterministic***. For example, the thermal-hydraulic calculations that support the event tree structure and the fault tree success criteria are based upon deterministic equations.
  - ◊ ***Aleatory*** (think random). For example, the "fails to run" model for a diesel generator is based upon a Poisson process which is used to yield a probability of failure. The actual time that a diesel generator operates before failing is stochastic.
  - ◊ Each of these two parts has uncertainty associated with it. For example, in a thermal-hydraulic calculation, the temperature and pressure for a particular accident sequence spans a range. For the diesel generator, we may collect data on operation time to determine a failure rate, but we do not know the rate exactly (even if we collect a large amount of data). Further, the models we select for the deterministic or aleatory analysis are abstract representations of reality, thus indicating that we have model uncertainty.
    - These sources of uncertainty are called ***epistemic***.
- When dealing with stochastic events, we do not know when the event will happen. This uncertainty is called **aleatory** uncertainty.
  - ◊ Aleatory models represent a random process; an example of this process would be the time until a light bulb burns out. Other examples are the time that a pump runs (until it fails) or the number of times a diesel generator starts (before a failure occurs).



◊ In all cases, aleatory models have, as inputs, parameters characterizing key elements (or assumptions) about the model.

- For example, when we talk about the "pump fails to run" aleatory model, a parameter of this model is typically a failure rate for "the pump to run."

- In real problems, we are never given the exact failure rate of components. We generally know their failure rates only up to a certain degree, based on the amount of data available.

◊ This "state of knowledge" uncertainty is referred to as **epistemic** uncertainty.

- This type of epistemic uncertainty is frequently called "parameter uncertainty."

- When someone indicates that they have done an uncertainty analysis in PRA, they generally mean that they only evaluated the epistemic parameter uncertainty for just the aleatory portion of the PRA.

- To evaluate the epistemic uncertainty, SAPHIRE provides two (closely related) Monte Carlo uncertainty analysis techniques:

    1. Simple Monte Carlo sampling

        - Repeatedly quantifies the system, event tree sequence, or project cut sets. Each basic event is sampled from its epistemic uncertainty distribution.

        - Generally requires more samples than Latin Hypercube sampling for the same degree of accuracy, but today's computers can handle thousands of iterations.

    2. Latin Hypercube sampling

        - A stratified sampling technique, with the basic event's epistemic distribution divided into equal probability subintervals.

        - Within each subinterval, SAPHIRE randomly samples and then "shuffles" the resulting values to ensure randomness.

        - May require fewer samples than simple Monte Carlo for similar accuracy; however, it may take longer to generate a random subinterval and subsequent shuffle than for a simple Monte Carlo sample.

    Summary:

    Computers and software are sufficiently fast that either uncertainty method is fine. Make sure that you check for convergence by varying the number of samples (e.g., 2,000; 4,000; 6,000) and comparing the answers at the end of each run.

The Rev. 3+ SPAR models contain both aleatory and epistemic uncertainty. Basic events are in the model that have "random" failure models (i.e., aleatory) such as fails-to-run and fails-to-start. For these models, the parameters that are uncertain have epistemic uncertainty distributions assigned to them.

10.2 Other Uncertainty Considerations

- Many steps that are taken during an event evaluation could introduce additional uncertainty into the overall results of the analysis.
  - ◊ The term "modeling uncertainty" represents the uncertainty directly associated with the PRA models (but not including the epistemic uncertainty). This uncertainty includes:
    - Limitations built into the SPAR models.
    - Potential information and interpretation deficiencies that arise during the accident event information gathering step.

- Performing the event evaluation requires several intermediate steps.
  - ◊ Interpret the circumstances regarding the operational event or decide on the situation for a hypothetical event.
  - ◊ Decide which inputs to the PRA model must be modified and how the inputs should be modified.
  - ◊ Modify the SPAR model and perform the evaluation using SAPHIRE/GEM.
  - ◊ Report and evaluate the newly generated results for the event analysis.
    - Each step above has the potential to introduce uncertainty into the event evaluation process.

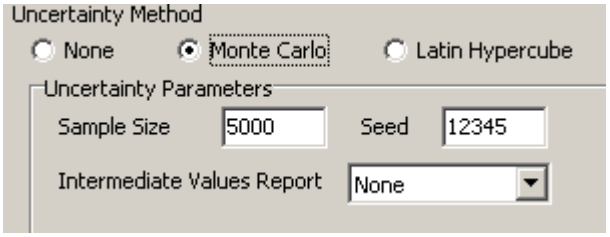
- In general, a formal (mathematical) evaluation of the model uncertainty is not performed.
  - ◊ The review or "reality check" after an analysis helps to scope the potential model uncertainties that may be important for the particular analysis.

10.3 Steps in Performing an Epistemic Uncertainty Evaluation

- The type of event (either "initiating" or "condition") is evaluated prior to performing an uncertainty analysis on the sequences.

- After the event has been evaluated, the ECA Workspace will perform an uncertainty analysis on the resulting cut sets.
  - ◊ The changed sequences had a change in either the initiating event or in basic events in the minimal cut sets.
  - ◊ These changed sequences are noted in the analysis results.

- To perform the uncertainty analysis, the analyst clicks the radio button specifying the type of uncertainty analysis sampling to be performed. (If no uncertainty analysis is to be performed, click the None radio button.)



- Then, you will need to define the uncertainty options.
  - ◊ Choose either Latin Hypercube or Monte Carlo
  - ◊ The number of samples to be used must be specified.
    - A sample size of 5,000 (or more) is generally adequate.
  - ◊ The random number generator seed can be specified or left as zero.

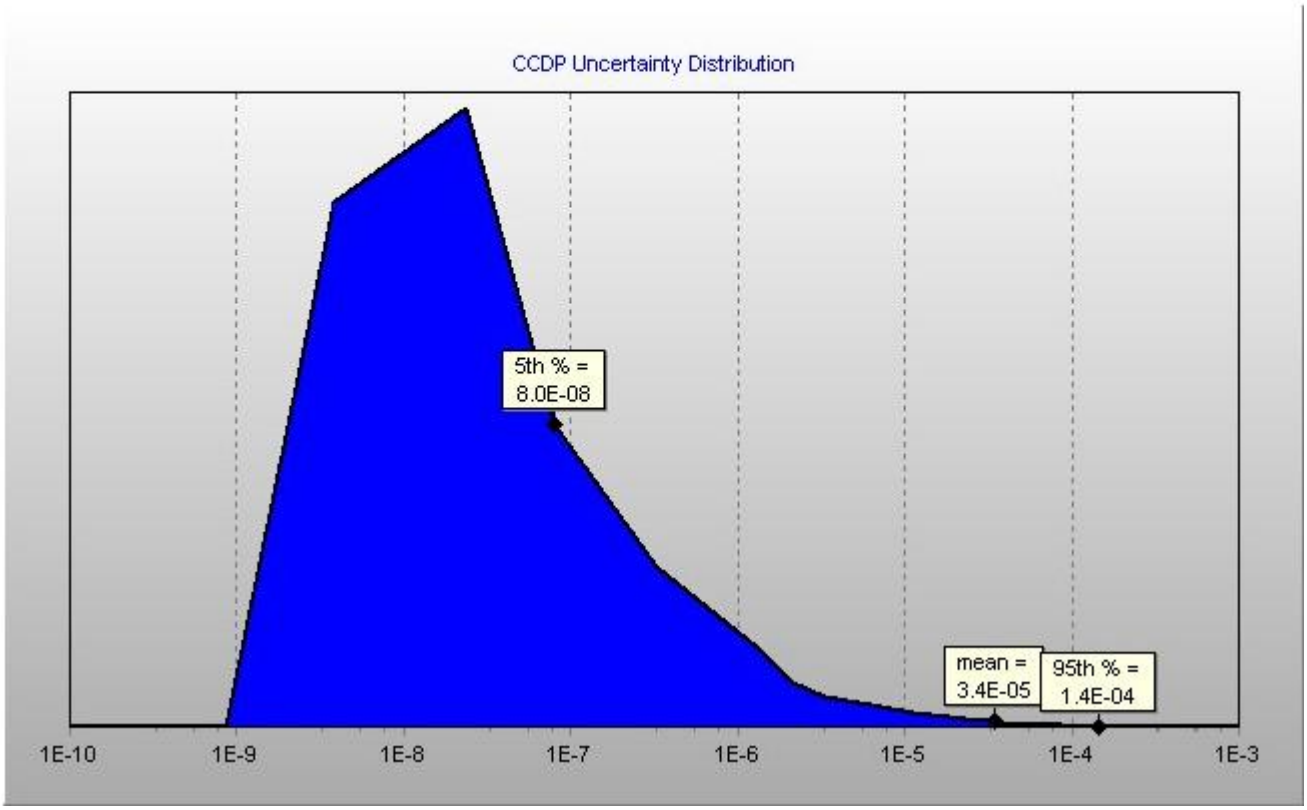
10.4 Example Uncertainty Analysis

- To demonstrate the uncertainty analysis process and results, an initiating event evaluation will be performed using the Generic PWR model.
- A switchyard-related LOOP with no components failed was evaluated along with an uncertainty analysis.
- The LOOP initiator was selected ("switchyard" related).
  - ◊ It was assumed that no components were failed.
    - This calculation gives the CCDP given that a switchyard-related LOOP occurred.
  - ◊ The results of "processing" the analysis are shown.
    - The total CCDP is 3.18E-5. This value is a *point estimate*.
- Since the point estimate does not reflect the uncertainties in the basic events, we need to perform an uncertainty analysis.
  - ◊ The results of the uncertainty analysis are shown for Monte Carlo, 5000 samples.
    - The mean value for the CCDP was found to be 3.45E-5.

- The 95th percentile for the CCDP was found to be 1.43E-4.

CCDP Uncertainty Distribution

5%	Median	Point Estimate	Mean	95%	Seed	Sample Size	Method
7.99E-8	1.12E-5	3.18E-5	3.45E-5	1.43E-4	12345	5000	Monte Carlo



10.5 Workshop

11. EVENT EVALUATION CASE STUDIES

Section 11 contains event reports for two incidents that occurred at operating U.S. nuclear power plants. These incidents will be the focus of the case studies that will be evaluated and discussed. Checklists are provided to assist the reader in determining the important steps to follow in order to complete the event evaluations.

Learning Objectives

- Demonstrate a proficiency with GEM by performing the exercises corresponding to the event reports in this section.

Section 11 Topics

11.1 Introduction

Incidents at nuclear power plants occur at many different times and under a variety of situations. Even the most modern, well run plants may experience events that are precursors to core damage.

The U.S. Nuclear Regulatory Commission evaluates a variety of such events through activities such as its Accident Sequence Precursor program. In this program, a conditional core damage probability is calculated that represents the plant configuration observed during an initiating event situation or during the duration of an unplanned equipment outage. This calculation is called an "event evaluation."

This section provides information about two incidents that happened at nuclear power plants. This information is provided by way of excerpts from the plant LER about the events. You are asked to review the reports in order to gain an understanding of what took place during the event. Then, with this knowledge, you will be asked to perform an event evaluation for the incident.

To assist in the evaluation, a simple checklist has been provided. This checklist is intended to cover the major items that need to be addressed during any event evaluation.

11.2 Case Study 1

CASE STUDY #1, LER FOR GENERIC PWR PLANT

Read the attached LER for the first case study. Using the checklist below, evaluate the event using the ECA Workspace, the Generic PWR SPAR model, and the supplied documentation.

#	Item	Result
1	Is the event an initiating event or condition assessment?	Initiating ☐ Condition ☐ Both ☐
2	If the event is a condition assessment, what is the duration?	hours
3	If the event is an initiating event, is the initiator recoverable? (Note that the ECA Workspace will adjust the non-recovery probabilities for you automatically)	Yes ☐ No ☐
4	Were any systems, structures, or components (SSCs) inoperable during the event.	Yes ☐ No ☐
5	If the answer to Question 4 was *yes*, identify the SSCs by finding its associated basic event(s) from the PRA model. Only identify "independent failure" related events (e.g., no common-cause yet).	
6	For those basic events identified in Question 5, determine the SSC's non-recovery probability (if it is recoverable from the failure).	
7	Are there any basic events identified in Question 5 that have associated common-cause failure events?	Yes ☐ No ☐
8	For each event had a yes answer to Question 7, determine the type of SSC failure. Options are: (a) Independent failures (b) Common-cause failures (c) Testing/Maintenance Refer to Section 6 for additional information.	

#	Item	Result
9	List the common-cause basic events that were identified from Question 7. Note that since you are using the Rev. 3+ SPAR model, you *will not* need to adjust these events (they are automatically modified by the software).	
10	You will need to specify in the ECA Workspace how to modify each basic event identified in Question 8. From Question 8, if the SSC is an independent failure or testing/maintenance outage, set the event to a probability of 1.0. Otherwise, set it to TRUE.	
11	For those SSCs that were identified in Question 6 and do not have an associated common-cause event, set the SSCs to its non-recovery probability in the ECA Workspace.	
12	Process the analysis using the modifications identified in Questions 1 - 11. Record your results of the analysis.	

FACILITY NAME: Generic PWR PAGE: 1 OF 5

TITLE: 'A' Standby Diesel Generator Output Breaker Failure to Close

EVENT DATE: 09/16/93 LER #: REPORT DATE: 10/18/93

OTHER FACILITIES INVOLVED: None

OPERATING MODE: 1 POWER LEVEL: 100%

THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR SECTION:
50.73(a)(2)(i)
50.73(a)(2)(v)

COMPONENT FAILURE DESCRIPTION:
CAUSE: SYSTEM: COMPONENT: MANUFACTURER:
REPORTABLE NPRDS: YES

SUPPLEMENTAL REPORT EXPECTED: No

ABSTRACT:

On September 16, 1993, the 'A' Standby Diesel Generator (SBDG) output breaker, 1A411, failed to close during the performance of the Loss of Offsite Power-Loss of Coolant Accident (LOOP-LOCA) surveillance test. The cause was an improper clearance between the breaker plunger and the switchgear stationary auxiliary switch mechanism on the Standby Transformer feeder breaker, 1A201, to essential bus 1AA02. This improper clearance disabled one of the closure permissives for 1A211.

The corrective actions included readjusting the gap between the breaker plunger and the stationary auxiliary switch to within the specifications intended by the breaker vendor and testing.

TEXT PAGE 2 OF 5

I. DESCRIPTION OF EVENT:

On September 16, 1993, with the plant operating, the 'A' SBDG output breaker, 1A211, failed to close during the performance of the LOOP-LOCA surveillance test.

Troubleshooting conducted by the plant Electrical Maintenance and Systems Engineering groups pinpointed the source of the problem to the 7-8 contacts on the stationary auxiliary switch mechanism in the switchgear cubicle for the Standby Transformer feeder breaker to essential bus 1AA02. The stationary auxiliary switch is operated by a plunger on the breaker that causes the 'a' switch contacts to close when the breaker is closed and causes the 'b' contacts to close when the breaker is open. Contacts 7-8 are 'b' contacts and should have closed during the LOOP-LOCA test when 1A201 opened to provide a signal to the logic that bus 1A2 was disconnected from the Standby Transformer and that the 'B' SBDG output breaker could safely close on the bus. In situ testing of contacts 7-8 indicated that continuity existed between them but that they failed to pass sufficient current to energize one of the logic's relay coils. The switch was removed, its contacts were burnished, and the switch was reinstalled. When the LOOP-LOCA test was rerun on September 22, breaker 1A211 again failed to close. At that time it was discovered that, with breaker 1A201 racked in and open, the breaker plunger was depressing the stationary auxiliary switch operating rod approximately 3/16 inches. This caused enough rotation in the switch mechanism to cause contacts 7-8 to be partially open and maintain poor contact as identified during testing described above.

A review of plant records revealed that during the performance of periodic maintenance on breaker 1A201 on **July 21, 1993,** a spacer had been added to raise the plunger. The addition of the spacer restored one of the breaker's dimensions to within the vendor's specifications, but caused the relationship between the breaker plunger and the auxiliary switch operating rod gap to fall outside acceptable limits. The breaker plunger was readjusted and the LOOP-LOCA test was successfully completed on **September 24.**

TEXT PAGE 3 OF 5

II. CAUSE OF THE EVENT

The cause of this event was procedural inadequacy. The maintenance manual for circuit breakers states, under Auxiliary Devices-Plunger Interlock, that the distance from the top of the plunger bolt to the bottom of the lifting rail should be 11-7/32 to 11-11/32 inches with the breaker closed. The manual also states that washers should be added or removed from the plunger as necessary to achieve this dimension. This dimension assures that the 'a' contacts on the auxiliary switch will close when the breaker is closed and also establishes uniformity between individual breakers to make them interchangeable. This maintenance procedure is based largely on other practices and it was this dimension that was being restored when the washer was added to the plunger on 1A201 on July 21.

In addition, the maintenance manual for Metal Clad switchgear states that, with the breaker racked in and open, that the gap between the breaker plunger and the operating rod on the stationary auxiliary switch mechanism should be from 0 to 1/8 inches and that any adjustment in this dimension must be made on the auxiliary switch setting. This measurement is a final check to make sure that the plunger and auxiliary switch perform as intended. However, the auxiliary switch is pinned in place and is not adjustable. It was stated that removing this pin is inappropriate. Establishing this gap can only be accomplished by adding or removing washers from the plunger.

III. ANALYSIS OF EVENT

Two Technical Specification violations resulted from the inoperability of the 'A' SBDG output breaker for the period from July 21 to September 24.
The period from July 21 to September 24 (when the plant was shutdown for a refueling outage) was longer than the seven day Limiting Condition for Operation allowed and was a violation of Technical Specification 3.5.G.1.
The second violation (Technical Specification 3.9.D) occurred during a four day period (**July 31 through August 4**) with the 'B' SBDG also inoperable for maintenance.

TEXT PAGE 4 OF 5

In the event a Loss of Offsite Power event would have occurred between July 21, 1993 and September 24, the 'A' SBDG output breaker, 1A211 would have failed to close automatically on essential bus 1AA02. However, plant procedures would have directed control room operators to perform the steps necessary to allow breaker 1A411 to be closed manually from the control room.

A probabilistic risk assessment (PRA) of the core damage frequency (CDF) was performed for the period from July 21 when maintenance was performed on 1A201 until September 24 when the plant was placed in cold shutdown for its 12th refueling outage. The analysis conservatively assumed that the control room operators would be unable to close the 'A' SBDG output breaker and determined that the instantaneous CDF for this period was 6.00E-05/year. This was a 21-fold increase but was still below the Proposed Safety Goal CDF of 1.00E-04/year.

The Safety Analysis Group also evaluated the plant shutdown risk for the period from September 24 to September 28 to determine the effect on the reactor core boiling frequency. This time frame includes a four day period when fuel was being moved out of the reactor vessel at the same time the 'B' Standby Diesel Generator was inoperable for maintenance. Again assuming no operator action to manually close breaker 1A211, the frequency of core boiling was increased 2% for the most limiting 24 hour period. This increase is considered minimal. A refueling accident, combined with a loss of offsite power event would have resulted in appropriate Reactor Building ventilation isolations. Manual operator action would have been necessary to ensure proper Standby Gas Treatment and Standby Filter Unit systems operation by restoring electrical power to essential busses. Throughout this period, offsite power sources were available.

IV. CORRECTIVE ACTIONS

1. The proper gap between the 1A201 auxiliary switch operating rod and the breaker plunger was established on September 23 and the LOOP-LOCA surveillance test was successfully completed on September 24.

2. Plant procedures have been revised to address the need to establish the auxiliary switch - breaker plunger gap.

TEXT PAGE 5 OF 5

3. A review was completed on all of the stationary auxiliary contacts in the essential busses and RPT breakers to identify those contacts with functions important to plant safety. All such contacts were either tested or verified to have been tested since the last time the breaker plunger had been adjusted. No failures were identified.

4. Measurements were taken on all essential and nonessential 4160 volt switchgear to assess conformance to vendor acceptance criteria. In thirteen of the essential breakers, the gap fell outside the vendor's criteria. Of the 13, the stationary auxiliary contacts on three of these breakers perform no safety related or significant plant functions and were not reworked prior to plant startup. The remaining 10 were adjusted to within vendor specifications. If a breaker plunger was adjusted downward (spacers removed), its 'a' contacts were functionally tested after the adjustments were made.

5. Six non-essential 4160 volt breakers with functions important to plant operation were also adjusted to within specification and were functionally tested if spacers were removed.

6. Special Order 93-48 was issued due to the concerns over 4160 volt breakers. The Special Order requires the Electrical Maintenance Supervisor or his designee to authorize and witness any exchanges between 4160 volt breakers. Any exchange will be documented on a Corrective Maintenance Action Request (CMAR) describing the condition which necessitates the exchange and the serial numbers of the breakers involved.

11.3 Case Study 2

CASE STUDY #2, LER FOR GENERIC PWR SPAR MODEL

Read the attached LER for the second case study. Using the checklist below, evaluate the event using the ECA Workspace, the Generic SPAR model, and the supplied documentation.

#	Item	Result	
1	Is the event an initiating event or condition assessment?	Initiating	☐
		Condition	☐
		Both	☐
2	If the event is a condition assessment, what is the duration?	Hours	
3	If the event is an initiating event, is the initiator recoverable? (Note that the ECA Workspace will adjust the non-recovery probabilities for you automatically)	Yes	☐
		No	☐
4	Were any systems, structures, or components (SSCs) inoperable during the event.	Yes	☐
		No	☐
5	If the answer to Question 4 was *yes*, identify the SSCs by finding its associated basic event(s) from the PRA model. Only identify "independent failure" related events (e.g., no common-cause yet).		
6	For those basic events identified in Question 5, determine the SSC's non-recovery probability (if it is recoverable from the failure).		
7	Are there any basic events identified in Question 5 that have associated common-cause failure events?	Yes	☐
		No	☐

#	Item	Result
8	For each event had a yes answer to Question 7, determine the type of SSC failure. Options are: (a) Independent failures (b) Common-cause failures (c) Testing/Maintenance Refer to Section 6 for additional information.	
9	List the common-cause basic events that were identified from Question 7. Note that since you are using the Rev. 3+ SPAR model, you *will not* need to adjust these events (they are automatically modified by the software).	
10	You will need to specify to the ECA Workspace how to modify each basic event identified in Question 8. From Question 8, if the SSC is an independent failure or testing/maintenance outage, set the event to a probability of 1.0. Otherwise, set it to TRUE.	
11	For those SSCs that were identified in Question 6 and do not have an associated common-cause event, set the SSCs to its non-recovery probability in the ECA Workspace.	
12	Process the analysis using the modifications identified in Questions 1 - 11. Record your results of the analysis.	

FACILITY NAME: XYZ Plant PAGE: 1 OF 9

TITLE: Reactor Trips as a Result of a Switchyard Power Circuit Breaker Fault and a Unit 2 Entry Into Limiting Condition for Operation (LCO) 3.0.3 When A Centrifugal Charging Pump Was Removed From Service

EVENT DATE: 12/31/92 LER #: REPORT DATE: 02/01/93

OTHER FACILITIES INVOLVED: Unit 3

OPERATING MODE: 1 POWER LEVEL: 100

COMPONENT FAILURE DESCRIPTION:
CAUSE: SYSTEM: COMPONENT: MANUFACTURER:
REPORTABLE NPRDS: N

ABSTRACT:

On December 31, 1992, at approximately 2148 Eastern standard time (EST), with Units 2 and 3 in power operation at approximately 100 percent, both units received a reactor trip signal because of reactor coolant pump bus undervoltage. The reactor trips were followed by turbine trips. Undervoltage on the 6.9-kV shutdown boards initiated board load stripping, diesel generator (D/G) starts, and D/Gs tying onto their respective shutdown board. Electrical loads were appropriately sequenced back to the boards. Main feedwater isolated and auxiliary feedwater pumps started. Loss of power to a radiation monitor resulted in an auxiliary building isolation. With limited staffing in the Unit 2 main control room, recovery evolutions for Unit 2 resulted in isolation of centrifugal charging pump suction and removal of centrifugal charging pump from service. Unit 2 entered LCO 3.0.3 for approximately one minute until a suction flow path was reestablished. The cause of the event was an internal fault in a **switchyard** power circuit breaker resulting from inappropriate testing methodology, resulting in a loss of offsite power. Corrective actions include strengthening of switchyard controls and increasing minimum Operations control room staffing.

TEXT PAGE 2 OF 9

I. PLANT CONDITIONS

Units 1 and 2 were in power operation at approximately 100 percent power.

II. DESCRIPTION OF EVENT

A. Event

On December 31, 1992, at approximately 2148 Eastern standard time (EST), both units received a reactor trip signal because of reactor coolant pump bus undervoltage (EIIS Code EA). The undervoltage condition resulted from an internal fault in a new switchyard power circuit breaker (PCB) (EIIS Code FK) that had been in service approximately 11 minutes. Before the event, switchyard crews were in the process of placing the PCB in service. The PCB (PCB 5058) was in the 500-kV switchyard to intertie transformer position. Primary protective relays applicable to the PCB had been disabled by opening the associated trip cutout switches to facilitate differential relay circuit phasing.

The reactor trips were followed by turbine trips. Undervoltage on the 6.9-kV shutdown (S/D) boards (EIIS Code EB) initiated diesel generator (D/G) (EIIS Code EK) starts and loading onto their respective S/D boards. The S/D board loads were stripped and upon D/G loading, loads were appropriately sequenced back to the boards with the exception of the thermal barrier booster pumps (TBBPs), which did not restart. Main feedwater isolated and auxiliary feedwater (AFW) (EIIS Code BA) pumps started. Loss of power to a radiation monitor (EIIS Code IL) resulted in an auxiliary building isolation. The fault was cleared within 88 cycles, and offsite power to the start busses was restored. Following the trip the reactor coolant pumps (RCPS) transferred from the unit station service transformer (USST) to the common station service transformer (CSST) as designed; forced reactor coolant flow was maintained.

TEXT PAGE 3 OF 9

During the transient, Unit 2 recovery evolutions resulted in isolation of centrifugal charging pump (EIIS Code CB) suction and pump being removed from service. Unit 2 entered Limiting Condition for Operation (LCO) 3.0.3 for approximately one minute until a suction flow path was reestablished. Normal charging seal flow was not in-service during this time. Approximately 20 seconds into that minute, the TBBPs were manually started to provide RCP seal flow cooling.

B. Inoperable Structures, Components, or Systems That Contributed to the Event

The handswitches for the TBBPs of both units were in the A-Auto position (in accordance with procedure) instead of the AP-Auto position (in accordance with design). The TBBPs were shed following the **loss of offsite power** indication, as designed. However, as a result of the handswitch position, the TBBPs did not reload upon D/G loading.

C. Dates and Approximate Times of Major Occurrences

December 31, 1992 at 2137 EST	Following review and approval of the switching order and testing methodology by the main control room (MCR) staff, PCB 5058 was placed in service to be followed by verification of phasing on the differential relay circuit. The primary trip cut-out switches were placed in the open position and provided no primary relay protection for PCB 5058 during this timeframe. Secondary delayed relay protection was available and did operate after approximately 88 cycles.

TEXT PAGE 4 OF 9

December 31, 1992 PCB 5058 faulted internally, resulting in breaker failure. From the annunciator printout, the first alarms to come in indicated oscillograph operation and opening of PCB 5074 (Plant Bowen line). The condenser circulating water pump motors tripped followed by alarms for overcurrent on Generator 1 exciter field, 161-kV supply voltage failure, station frequency excessive error, and undervoltage on the RCP bus.

Additional events during this first minute included:

1) Opening of the 500-kV switchyard PCBs and the intertie PCBs in the 161-kV switchyard.

2) Undervoltage on the 6.9-kV S/D boards resulted in the appropriate relays stripping the major equipment from the boards. This included the centrifugal charging pumps (CCPs) on both units, which subsequently resulted in letdown isolations.

3) Both units received a reactor trip signal because of RCP bus undervoltage. The reactor trips were followed by turbine trips and 161-kV bus voltage-failure alarms. Automatic transfer from USST to CSST was successful, and the 6.9-kV unit boards remained energized from offsite power. Undervoltage on the four 6.9-kV S/D boards initiated transfer to the D/Gs. The four D/Gs started; feeder breakers closed and energized their respective S/D boards.

TEXT PAGE 5 OF 9

Unit 2 at 2208 EST	Suction to the CCPs swapped over from the volume control tank (VCT) to the refueling water storage tank (RWST) because level in the VCT had decreased to 7 percent. At that time, the ASOS realized that letdown had been previously isolated. The ASOS directed that one CCP be stopped. Since the blackout relays were sealed in, the pump was placed in pull-to-lock (P-T-L).
Unit 2 at 2209 EST	Letdown was reestablished.
Unit 2 at 2211 EST	After the reactor operator (RO) and ASOS verified sufficient VCT level, the VCT outlet valves were opened. The operator then closed the RWST valves. The operator observed that the VCT outlet valves were traveling closed. The second CCP was stopped and letdown automatically isolated. With both CCPs not in service, LCO 3.0.3 was entered. Approximately 20 seconds after the second CCP was stopped, the shift operations supervisor (SOS) started the TBBPs. The Unit 1 TBBPs were then started after the Unit 2 TBBPs.
Unit 2 at 2212 EST	VCT valves were opened, the second CCP was started, and letdown was reestablished. The handswitches for both the VCT and RWST valves were either placed in or verified to be in AP-AUTO position. LCO 3.0.3 was exited.

Unit 2 at at 2313 EST	The 6.9-kV S/D boards were returned to normal offsite power.
January 1, 1993 at 0011 EST	Unit 2 was stabilized in Mode 3.

D. Other Systems or Secondary Functions Affected

The low voltage condition resulted in the Units 1 and 2 condenser circulating water (CCW) pumps tripping. The loss of these pumps is not considered abnormal for this event. The unit boards sustained a voltage drop that would cause a drop in excitation voltage and result in a speed deviation trip or a power-factor deviation trip. CCW flow is necessary to maintain condenser vacuum and to provide an enable signal for steam dump.

E. Operator Actions

The operators promptly diagnosed the plant conditions and took actions necessary to stabilize the units in the hot standby condition (Mode 3).

Unit 2 MCR personnel (one ASOS and one RO) proceeded through the actions described by the emergency procedure. With only one RO, securing of the secondary side was delayed. The RO took manual control of the TDAFWP and reduced its speed to minimum. The MDAFWP LCVs were left in the auto position resulting in twice the AFW flow of that in Unit 1, resulting in a greater cooldown rate. With blowdown isolated, feedwater pumps tripped, main turbine tripped, and steam dumps not available, the effect of the higher AFW flow caused Unit 2 to cooldown to about 537 degrees F. The ASOS recognized that RCS boration was required if T sub avg was less than 540 degrees F and made the decision to leave the MDAFWP LCVs in auto and borate first. The ASOS and RO discussed which flow path was to be used. The normal boration path was chosen because it was considered to require less operator intervention and monitoring than the emergency path. The ASOS made the decision to borate through the blender and directed the RO to initiate 135 gallons of high concentration (20,000 parts per minute) boration at

greater than 10 gpm. The ASOS did not read the procedure and believed that the procedure allowed boration through the path chosen. The procedure required boration through the emergency boration path. The normal boration path was allowed only if flow could not be achieved through the emergency boration path. The decision to borate through the normal rather than emergency path, as required by the procedure, set up the sequence of events ultimately leading to the loss of both CCPs and charging RCP seal injection.

The ASOS had noted early in the transient that the component cooling system (CCS) TBBPs did not automatically start after the D/Gs energized the S/D boards. The ASOS did not direct manual starting of the TBBPs at that time because he did not have the resources available to evaluate the impact on D/G loading.

At the time of the reactor trip, the undervoltage condition had resulted in load stripping of the 6.9-kV S/D boards. The load shedding tripped off the running CCP. With no CCPs running, a letdown isolation automatically occurred. After the ASOS initiated boration and manual control of the MDAFP LCVs, an automatic swapover from the VCT to the RWST occurred as the level in the VCT reached 7 percent. At this time, the ASOS realized that letdown was isolated, and normal boration was only providing approximately 10 gpm makeup. After swapover, the ASOS directed the operator to stop the one CCP.

TEXT PAGE 8 OF 9

At this point, the RO recalled the RWST valves being closed and the VCT valves being open. The RO stated that as he looked away from the handswitches, he noticed green and red lights on the VCT valves, indicating the valves traveling closed. The RWST valves remained closed with green lights. With the RWST valve handswitches left in the A-Auto rather than the AP-Auto position, automatic transfer back to the RWST did not occur when the VCT valves traveled closed. The RO called out the condition to the ASOS. Not knowing whether the VCT valves were partly closed or almost fully closed, the RO prepared to stop the running A CCP. With concern for potential imminent failure of the CCP on loss of suction, the ASOS directed the RO to stop the A CCP. The RO held the pump handswitch in the STOP position (not in P-T-L). When told by the ASOS that the second CCP was being stopped, the SOS manually started the TBBPs approximately 20 seconds after the A CCP was stopped. The VCT outlet valves were reopened and remained open, the handswitch for the 2A-A CCP was released, and the pump restarted approximately one minute after being stopped. Letdown was reestablished and the system stabilized.

The normal feeder to the 6.9-kV S/D boards is designed to open when its undervoltage relays sense less than 80 percent voltage for more than 0.5 seconds. After the 6.9-kV S/D board voltage had decreased to less than 70 percent undervoltage, a D/G start signal was generated. The load shedding occurred as expected. After each D/G reached the appropriate speed and voltage, the breaker that connects each D/G to the S/D board closed, and the load sequencing timers started. Loads were then automatically reconnected for a nonaccident loading sequence. During this event, the load shed/load sequence logic functioned as designed on the four S/D boards, with the exception of the TBBPS.

TEXT PAGE 9 OF 9

The TBBPs failed to start following S/D board reloading. The SOS took manual action to restart the TBBPS. Further investigations into the failure to start revealed that the handswitches for the pumps had been placed in the A-Auto position in accordance with procedure. With the handswitch in this position, the pumps will not start upon actuation of the blackout relays. The handswitch position described by procedure was found to be incorrect relative to design.

During the time that the S/D boards were without power, a control power alarm was received on D/G 1A and a low lube oil pressure alarm was received on the four D/Gs. The low lube oil pressure alarm was expected for the event and was cleared. The control power alarm was reviewed and found to be the result of the test pushbutton being depressed or momentarily shorted. This condition was evaluated and no D/G operability concerns were identified.

12. TEST REVIEW

Section 12 presents elements for review prior to the comprehensive event evaluation test. Alternatively, this section can be used to provide additional workshop material.

Learning Objectives

- Demonstrate a proficiency with the Event Evaluation course material by performing the exercises in this section.

Section 12 Topics

12.1 Example Problems

12.1 Example Problems

Problem 1. Assume that the minimal cut sets for core damage are:

CD = IE1·MOV-B + IE2·MOV-A·DG-A + IE2·DG-B

where "·" indicates a logical AND operation while "+" indicates a logical OR operation.

a. If the component represented by MOV-B is failed (i.e., a TRUE house), what are the new minimal cut sets for core damage?

b. Calculate the conditional core damage probability (CCDP) given that the initiating event IE2 occurred while nothing was failed. Assume the following probabilities:

P(MOV-A) = P(MOV-B) = P(DG-A) = P(DG-B) = 0.01.

Problem 2. An LER is given to you by a coworker who asks you to perform an event assessment for the event. The LER reads as follows:

Facility: Plant XYZ	Notification: 6/10/2000	Event #: 21343
Emergency Class: Not applicable 10 CFR Section:ARPS 50.72(b) (2) (ii)		Notification: G.W. Operator
Unit 2: Reactor critical	100% power initially	0% power currently
DEGRADATION OF AFW CONDENSATE STORAGE TANK During surveillance testing of the AFW, it was found that the AFW Condensate Storage Tank was valved shut (and locked) preventing its operation. Investigations indicated that this tank was inoperable since the last AFW maintenance 4 days ago.		

a. In the Generic PWR SPAR model, what is the name(s) of the basic event(s) that need to be adjusted in order to map the LER into the PRA?

b. Using the ECA Workspace, map the LER event into the model. Print out a hardcopy of the analysis report. Record the overall results below.

$\text{Importance}_{\text{event}}$ = _____

CCDP = _____

CDP = _____

NOTES

Appendix A

Thoughts on Calculating CCDPs

The calculation of an operational risk measure attempts to create a risk profile, over time, conditional upon the component outages and plant initiating events that actually occurred during the period of interest. The conditional core damage probability (CCDP) is believed to be the best measure as a basis for this risk profile since it has many desirable features. But, what is *not* being calculated for the risk profile is the probability that severe core damage *did* happen. If we look at the operation during the last 12 months for any nuclear power plant in the U.S. and ask "what is the probability that severe core damage did happen," the resulting probability is zero. While a zero probability for severe core damage is of great interest for the plant owners and operators, this particular probability question in itself is of little interest. Instead, the risk profile that deserves attention asks the question:

> What could happen (i.e., what is the probability of core damage) if the conditions and events that existed over the duration of interest were realized at a later time?

Thus, the CCDP that is part of the risk profile measures the likelihood of core damage conditional upon the plant configuration and operating status at a point in time during the duration of interest. In addition, the conditionality that is imposed only reflects impacts on the measure of interest (e.g., core damage). Such impacts include the scenarios that have been discussed (e.g., a component outage or the occurrence of an initiating event). Situations where a component *operates* are not factored into the CCDP calculation. The fact that a particular component operated at a point in time is not important to the calculation. What is important is the question concerning the probability that the operating component *could* have failed. At first glance it may appear that the CCDP calculation is performed using the "relative frequency" statistical framework since the notion of a repeatable plant configuration is implied (i.e., if the plant were in this configuration 100 times, how many times would the operating component fail?). But, the CCDP calculation is still performed using the subjective (or Bayesian) framework that forms the foundation of modern PRAs. Nonetheless, the notion of a repeatable configuration may help the reader conceptualize the philosophy behind operational risk profile calculations.

To illustrate the philosophy backing the CCDP calculation, a non-nuclear power plant example will be utilized. To motivate this example, assume that an audience will see a particular magic show. In this show, the magician performs a special magic trick, using a length of rope, that incurs great risk and the potential for death. This trick is performed only once a month, every month of the year. Unfortunately, the type of rope used by the magician varies from one performance to another, depending on the available rope supply. It is known, from collecting rope usage data, that on any given performance, the probability of one type of rope being used during the performance is:

P(best rope | performance) = 0.5
P(good rope | performance) = 0.4
P(bad rope | performance) = 0.1 .

Further, it has been estimated that the probability of the magician dying during the performance varies from 0.1 to 0.001, depending on the type of rope that is used. Specifically, the probability of death is:

P(death | best rope is used) = 0.001
P(death | good rope is used) = 0.01
P(death | bad rope is used) = 0.1 .

The magician insists that "the show must go on" irrelevant of what type of rope is available for a particular performance. Knowing this, one could estimate the probability of death for a given, upcoming performance by the equation:

$$P(\text{death} \mid \text{performance}) = \sum P(\text{death} \mid \text{rope type X is used}) \times P(\text{rope type X is used} \mid \text{performance})$$

Evaluating this expression for the three rope types yields:

$$P(\text{death} \mid \text{performance}) = [0.001 \times 0.5] + [0.01 \times 0.4] + [0.1 \times 0.1]$$
$$= 0.0005 + 0.004 + 0.01 = 0.0145 .$$

where it can be seen that using the "bad" rope incurs the greatest amount of risk. Using the bad rope gives a probability of death more than two times that of the good rope and 20 times that of the best rope. While this risk calculation is adequate to determine the risk differences between using the three types of rope, it does not indicate what the risk was for a particular pattern of performances (say over the last 12 months). Instead, what is needed to determine the risk over a specified period of time is a risk profile calculation.

To perform this risk profile calculation, the actual rope type used for each of the last 12 shows is needed and are shown below.

Show	1	2	3	4	5	6	7	8	9	10	11	12
Type	good	best	best	best	good	bad	best	good	best	best	good	best

From the previous calculation, the probability of death, given usage of a particular type of rope, is known for each rope type. These probabilities are: P(death | best rope) = 0.001, P(death | good rope) = 0.01, and P(death | bad rope) = 0.1. Plotting these probabilities for each performance over the last 12 months gives Figure A-1. If these conditional probabilities are summed over the last twelve performances, a cumulative probability risk profile is constructed. An example of a cumulative risk profile is shown in Figure A-2.

The plots shown in Figures A-1 and A-2 are representations of risk profiles. These risk profiles demonstrate the probability of death that was experienced by the magician for the performances over the last year. The calculation for similar plots will be discussed relevant to the operation of nuclear power plants in the following two sections. First, the issue of component outages, and their impact on the risk profile, is presented. Second, the concern of initiating events and complications to the risk profile calculation is addressed. One important difference between the magician example risk profile and that of an operating nuclear power plant is that the ordinal axis consists of time and is continuous rather than the discrete case (i.e., per performance) above.

The probability that the magician died over the last 12 performances is zero since the magician successfully completed the last performance. But, based upon the calculated risk profiles that are displayed in Figures A-1 and A-2, we can state that, given the type of ropes used and the number of performances over the year, the probability of death during a performance is about 0.147. As will be demonstrated later, similar statements can be made about the probability of experiencing damage to a nuclear power plant reactor during a component outage or the occurrence of an initiating event.

Figure A-1. Magician's probability of death risk profile.

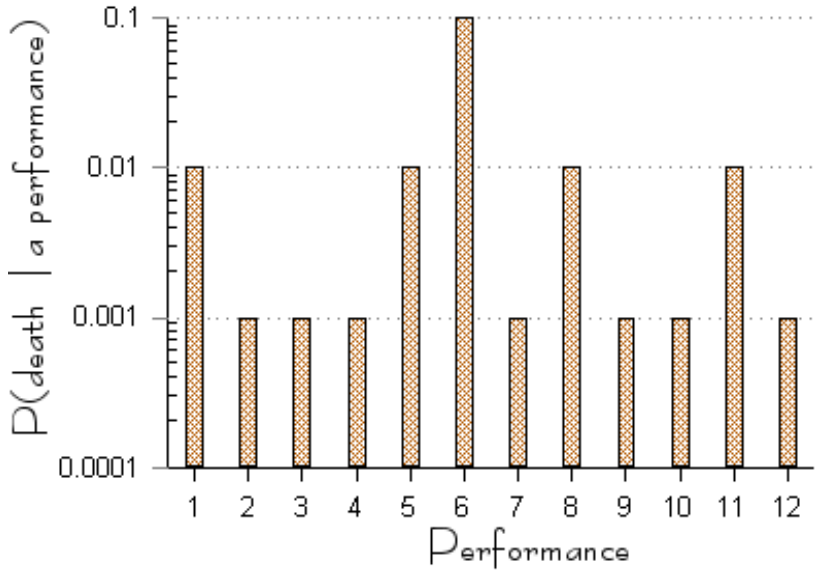


Figure A-2. Magician's cumulative probability of death risk profile.