U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8

Volume 5: Workspaces

Office of Nuclear Regulatory Research

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8

Volume 5: Workspaces

Prepared by
C.L. Smith, S.T. Wood

Idaho National Laboratory
Battelle Energy Alliance
Idaho Falls, ID 83415

D. O'Neal, NRC Project Manager

NRC Job Code N6423

Office of Nuclear Regulatory Research

PREVIOUS REPORTS

S. T. Wood, C. L. Smith, K. J. Kvarfordt, S. T. Beck, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 1 Summary Manual*, NUREG/CR-6952, August 2008.

C. L. Smith, S. T. Wood, W. J. Galyean, J. A. Schroeder, S. T. Beck, M. B. Sattison, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 2 Technical Reference*, NUREG/CR-6952, August 2008.

K. J. Kvarfordt, S. T. Wood, C. L. Smith, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 3 Code Reference*, NUREG/CR-6952, August 2008.

S. T. Beck, S. T. Wood, C. L. Smith, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 4 Tutorial*, NUREG/CR-6952, August 2008.

C. L. Smith, J. Schroeder, S. T. Beck, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 5 GEM Manual*, NUREG/CR-6952, August 2008.

C. L. Smith, R. Nims, K. J. Kvarfordt, C. Wharton, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 6 Quality Assurance Manual*, NUREG/CR-6952, August 2008.

K. J. Kvarfordt, S. T. Wood, C. L. Smith, *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 7 Data Manual*, NUREG/CR-6952, August 2008.

Smith, C. L., et al., *Testing, Verifying, and Validating SAPHIRE Versions 6.0 and 7.0*, NUREG/CR-6688, October 2000.

K. D. Russell, et al. *Systems Analysis Programs for Hands-on Reliability Evaluations (SAPHIRE) Version 6.0 - System Overview Manual*, NUREG/CR-6532, May 1999.

K. D. Russell et al., *Integrated Reliability and Risk Analysis System (IRRAS) Version 5.0, Volume 2 - Reference Manual*, NUREG/CR-6116, EGG-2716, July 1994.

K. D. Russell et al., *Verification and Validation (V&V), Volume 9 – Reference Manual*, NUREG/CR-6116, EGG-2716, July 1994.

K. D. Russell et al., *Integrated Reliability and Risk Analysis System (IRRAS) Version 4.0, Volume 1 - Reference Manual*, NUREG/CR-5813, EGG-2664, January 1992.

K. D. Russell et al., *Integrated Reliability and Risk Analysis System (IRRAS) Version 2.5 Reference Manual*, NUREG/CR-5300, EGG-2613, March 1991.

K. D. Russell, M. B. Sattison, D. M. Rasmuson, *Integrated Reliability and Risk Analysis System (IRRAS) - Version 2.0 User's Guide*, NUREG/CR-5111, EGG-2535, manuscript completed March 1989, published June 1990.

K. D. Russell, D. M. Snider, M. B. Sattison, H. D. Stewart, S.D. Matthews, K. L. Wagner, *Integrated Reliability and Risk Analysis System (IRRAS) User's Guide - Version 1.0 (DRAFT)*, NUREG/CR-4844, EGG-2495, June 1987.

ABSTRACT

The Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8 is a software application developed for performing a complete probabilistic risk assessment using a personal computer running the Microsoft Windows™ operating system. SAPHIRE 8 is funded by the U.S. Nuclear Regulatory Commission (NRC). The role of the Idaho National Laboratory (INL) in this project is that of software developer and tester. In older versions of SAPHIRE, the model creation and analysis functions were intermingled. However, in SAPHIRE 8, the act of creating a model has been separated from the analysis of that model in order to improve the quality of both the model (e.g., by avoiding inadvertent changes) and the analysis. Consequently, in SAPHIRE 8, the analysis of models is performed by using what are called Workspaces. Currently, there are Workspaces for three types of analyses: (1) the Events and Condition Assessment (ECA), (2) the NRC's Significance Determination Process (SDP), and (3) the General Analysis (GA) workspace. Workspaces for each type are created and saved separately from the base model which keeps the original database intact. Workspaces are independent of each other and modifications or calculations made within one workspace will not affect another. In addition, each workspace has a user interface and reports tailored for their intended uses.
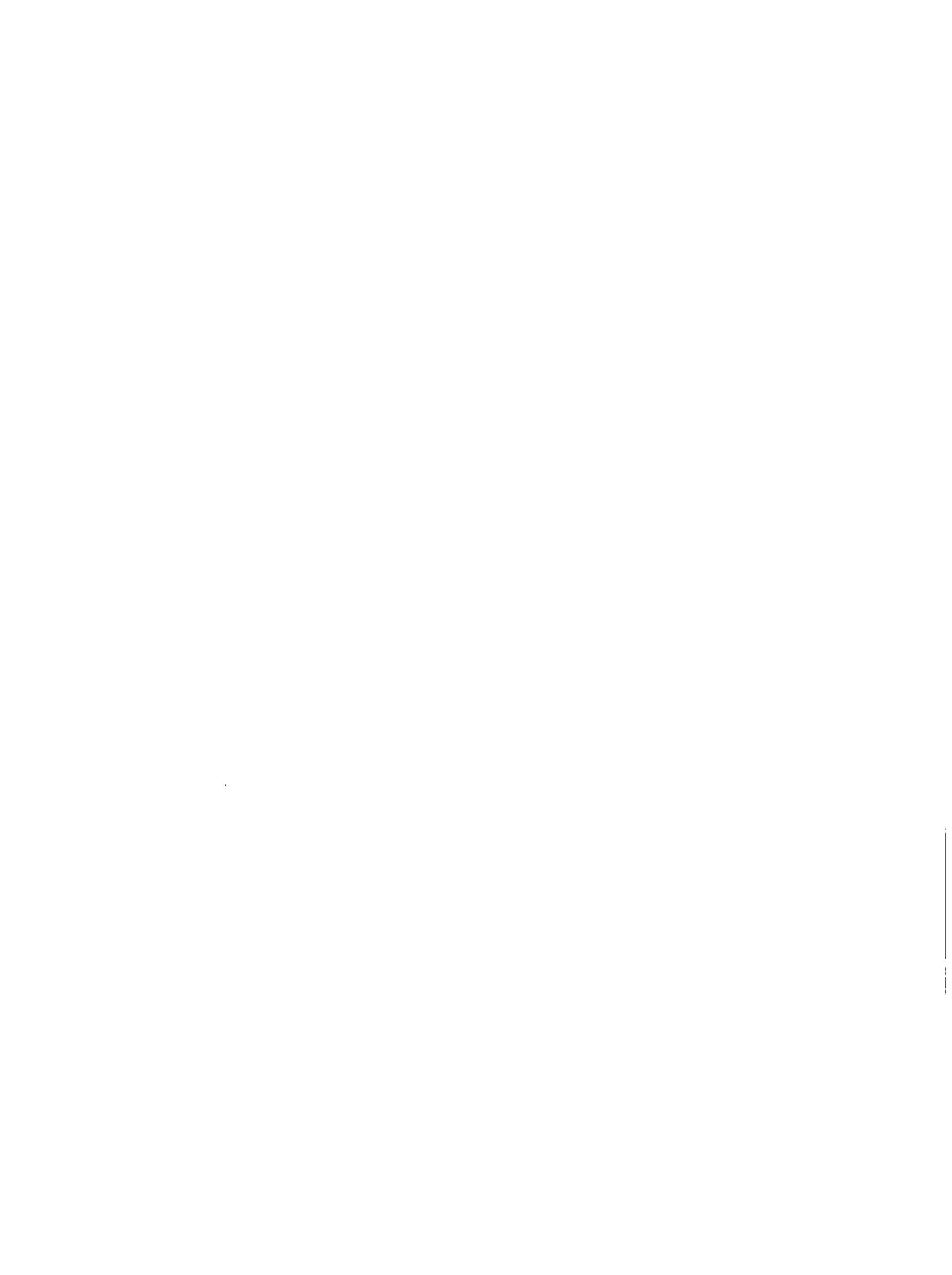
FOREWORD

The U.S. Nuclear Regulatory Commission (NRC) has developed the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software that is used to perform probabilistic risk assessments (PRAs) on a personal computer. SAPHIRE enables users to supply basic event data, create and solve fault and event trees, perform uncertainty analyses, and generate reports. In that way, analysts can perform PRAs for any complex system, facility, or process.

For nuclear power plant PRAs, SAPHIRE can be used to model a plant's response to initiating events, quantify core damage frequencies, and identify important contributors to core damage (Level 1 PRA). The program also can be used to evaluate containment failure and release models for severe accident conditions given that core damage has occurred (Level 2 PRA). In so doing, the analyst could build the PRA model assuming that the reactor is initially at full power, low power, or shutdown. In addition, SAPHIRE can be used to analyze both internal and external events and, in a limited manner, to quantify the frequency of release consequences (Level 3 PRA). Because this software is a very detailed technical tool, users should be familiar with PRA concepts and methods used to perform such analyses.

SAPHIRE has evolved with advances in computer technology and users' needs. Starting with Version 5, SAPHIRE operated in the Microsoft Windows™ environment. Versions 6 and 7 included features and capabilities for developing and using larger, more complex models. SAPHIRE Version 8 includes significant new features and capabilities to meet user needs for NRC risk-informed programs. In general, these include:

Improved user interfaces supporting NRC's Significance Determination Process, event and condition assessments, and more detailed types of PRA analyses.

Development and use of NRC's Standardized Plant Analysis Risk models.

New and improved solving algorithms.

Support features for user-friendliness.

This NUREG-series report comprises seven volumes as outlined below and incorporates new features and capabilities of Version 8.

Volume 1, "Overview and Summary"

Volume 1 provides an overview of the functions and features available in SAPHIRE Version 8 and presents general instructions for using the software.

Volume 2, "Technical Reference"

Volume 2 summarizes the fundamental mathematical concepts of sets and logic, fault trees, and probability. It then describes the algorithms used to construct a fault tree and to obtain the minimal cut sets. This report presents the formulas used to obtain the probability of the top event from the minimal cut sets and the formulas for probabilities that apply for various assumptions concerning reparability and mission time. In addition, it defines the measures of basic event importance that SAPHIRE can calculate. This volume also gives an overview of uncertainty analysis using simple Monte Carlo sampling or Latin Hypercube sampling and states

the algorithms used by this program to generate random basic event probabilities from various distributions. Finally, this report discusses enhanced and new capabilities such as post-processing rules, integrated model solving using model types, and workspace analysis routines.

<u>Volume 3, "Users' Guide"</u>

Volume 3 provides a brief discussion of the purpose and history of the software as well as general information such as installation instructions, starting and stopping the program, and some pointers on how to get around inside the program. Next, it discusses database concepts and structure. The following nine sections (one for each of the menu options on the SAPHIRE main menu) furnish the purpose and general capabilities for each option. Finally, Volume 3 provides the capabilities and limitations of the software.

<u>Volume 4, "Tutorial"</u>

Volume 4 provides a series of lessons that guide the user through basic steps common to most analyses performed with SAPHIRE.

<u>Volume 5, "Workspaces"</u>

Volume 5 describes the functionality and process behind SAPHIRE Version 8 workspaces. Workspaces provide an area in which a PRA model can be analyzed to obtain risk insights for a given initiating event or condition. Workspaces replace the "Graphical Evaluation Module" in earlier SAPHIRE versions.

<u>Volume 6, "Quality Assurance"</u>

Volume 6 is designed to describe how the SAPHIRE software quality assurance (QA) is performed for Version 8, what constitutes its parts, and the limitations of those processes. In addition, this report describes the Independent Verification and Validation that was conducted for Version 8 as part of an overall QA process.

<u>Volume 7, "Data Loading"</u>

Volume 7 is designed to guide the user through the basic procedures necessary to enter PRA data into the SAPHIRE program using SAPHIRE's MAR-D ASCII-text (or "flat file") data formats. In addition, this manual covers loading data through the new Accident Sequence Matrix and discusses the Project Integrate interfaces with SAPHIRE.

Christiana H. Lui, Director

Division of Risk Analysis

Office of Nuclear Regulatory Research

U.S. Nuclear Regulatory Commission

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

SAPHIRE can be used to model incidents at facilities such as nuclear power plants, where these events can occur at different times and under a variety of conditions. Analysts perform a probabilistic risk assessment (PRA) of the situation as well as a variety of "what if" types of analysis. To perform these evaluations, SAPHIRE 8 contains Workspaces in order to use a PRA model to obtain a risk measure that is conditional on the situation that is modeled as part of the analysis.

Currently, there are Workspaces for three types of analyses:

1. The Events and Condition Assessment (ECA)

2. The NRC's Significance Determination Process (SDP)

3. The General Analysis (GA) workspace

The ECA Workspace performs two types of analyses on the PRA model. The first type is an initiating event assessment. This type of assessment is designed to analyze the PRA model given the initiating event occurred. The results are a condition core damage probability (CCDP), since the PRA model is solved with the specific initiating event set to 1.0. The other assessment type is a conditional assessment. This type of assessment is based on a component(s) being failed or potentially unavailable to perform its safety function for some duration. The results from this analysis are also a CCDP.

The SDP Workspace is designed to analyze models to obtain results that represent the annualized change in core damage frequency (CDF). The increase in annualized CDF is determined by taking the nominal core damage probability (CDP) (which accounts for nominal test and maintenance), and subtracting it from the conditional CCDP to obtain the change in CDP due to the degraded condition alone. This numerical result is then normalized by dividing it by 1 year to arrive at a delta CDF in units of "per year." Models which run in the SDP interface have all of their components and systems specified in order to be recognized by SAPHIRE Version 8. SAPHIRE Version 8 is designed to walk the analyst through the required steps to perform an SDP analysis by way of four steps:

1. Indicate which component(s) are affected

2. Specify the affect

3. Modify analysis boundary conditions

4. Perform the analysis

The General Analysis user interface allows for a more general analysis option. This option provides the user the flexibility to set up an analysis that is saved for future analyses and modifications. As part of this analysis, SAPHIRE Version 8 allows the user to select what parts of the model will be affected by the analysis by checking the applicable selection boxes.

ACKNOWLEDGEMENTS

ACRONYMS

ASP   Accident Sequence Precursor

CCDP   conditional core damage probability

CCF   common cause failures

CDP   core damage probability

GEM   Graphical Evaluation Module

INL   Idaho National Laboratory

IRRAS   Integrated Reliability and Risk Analysis System

LERF   large early release frequency

LOSP   loss-of-offsite power

LPI   low pressure injection

NRC   Nuclear Regulatory Commission

PC   personal computer

PRA   Probabilistic Risk Analysis

RAW   Risk Achievement Worth

SAPHIRE   Systems Analysis Programs for Hands-on Integrated Reliability Evaluations

SPAR   Standardized Plant Analysis Risk

Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8

Volume 5 Workspaces

1. INTRODUCTION

1.1 Background

The U.S. Nuclear Regulatory Commission (NRC) has developed a powerful personal computer (PC) software application for performing probabilistic risk assessments (PRAs), called Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8.

Using SAPHIRE 8 on a PC, an analyst can perform a PRA for any complex system, facility, or process. Regarding nuclear power plants, SAPHIRE can be used to model a plant's response to initiating events, quantify associated core damage frequencies, and identify important contributors to core damage (Level 1 PRA). It can also be used to evaluate containment failure and release models for severe accident conditions, given that core damage has occurred (Level 2 PRA). It can be used for a PRA assuming that the reactor is at full power, at low power, or at shutdown conditions. Furthermore, it can be used to analyze both internal and external initiating events, and it has special features for transforming models built for internal event analysis to models for external event analysis. It can also be used in a limited manner to quantify risk for release consequences to both the public and the environment (Level 3 PRA). For all of these models, SAPHIRE can evaluate the uncertainty inherent in the probabilistic models.

SAPHIRE development and maintenance has been undertaken by the Idaho National Laboratory (INL). The INL began development of a PRA software application on a PC in the mid 1980s when the enormous potential of PC applications started being recognized. The initial version, Integrated Risk and Reliability Analysis System (IRRAS), was released by the Idaho National Engineering Laboratory (now Idaho National Laboratory) in February 1987. IRRAS was an immediate success, because it clearly demonstrated the feasibility of performing reliability and risk assessments on a PC and because of its tremendous need (Russell 1987). Development of IRRAS continued over the following years. However, limitations to the state of the-art during those initial stages led to the development of several independent modules to complement IRRAS capabilities (Russell 1990; 1991; 1992; 1994). These modules were known as Models and Results Database (MAR-D), System Analysis and Risk Assessment (SARA), and Fault Tree, Event Tree, and Piping and Instrumentation Diagram (FEP).

IRRAS was developed primarily for performing a Level 1 PRA. It contained functions for creating event trees and fault trees, defining accident sequences and basic event failure data, solving system fault trees and accident sequence event trees, quantifying cut sets, performing sensitivity and uncertainty analyses, documenting the results, and generating reports.

MAR-D provided the means for loading and unloading PRA data from the IRRAS relational database. MAR-D used a simple ASCII data format. This format allowed interchange of data between PRAs performed with different types of software; data of PRAs performed by different codes could be converted into the data format appropriate for IRRAS, and vice-versa.

Previous versions of SAPHIRE consisted of the suite of these modules. Taking advantage of the Windows 95 (or Windows NT) environment, all of these modules were integrated into SAPHIRE Version 6; more features were added; and the user interface was simplified. Additional enhancements and streamlining were made to SAPHIRE Version 7, but the overall graphical user interface remained largely the same as that found in Version 6. Version 8 of SAPHIRE features an entirely new graphical user interface with the intent to simply and, at the same time, provide additional capabilities.

New to SAPHIRE 8 is the concept of Workspaces. SAPHIRE supports performing calculations in workspaces. The workspaces are selected within the standard SAPHIRE user interface. From here, any number of workspaces may be selected and saved. For each workspace, custom reports are tailored for the applications of the user interface.

SAPHIRE performs quantification within each Workspace. Since workspaces are independent of each other the quantification within one workspace does not affect quantification within other workspaces. Similarly, quantification in a workspace does not affect calculations performed in the "Standard Analysis" (i.e., the main screen) interface where the base case model resides. However, a new workspace will use the model in the Standard Analysis interface; therefore, saved changes made to the base model in the Standard Analysis interface will be carried along into the new workspace.

Currently, there are Workspaces for three types of analyses:

1. The NRC's Accident Sequence Precursor program, where the workspace is called "Events and Condition Assessment (ECA)"

2. The NRC's Significance Determination Process (SDP)

3. The General Analysis (GA) workspace

This volume describes the functionality and process behind each workspace. In Chapter 2, we review the ECA Workspace and describe the types of evaluations that are provided by that workspace. In Chapter 3, we discuss the SDP Workspace, including a worked example. In Chapter 4, we describe the GA Workspace. Lastly, Chapter 5 provides a list of the references used in this report.

1.2   Accessing a SAPHIRE Workspace

The user interfaces for performing different types of analyses are shown in the workspaces menu on the left side of the main SAPHIRE window (Figure 1).
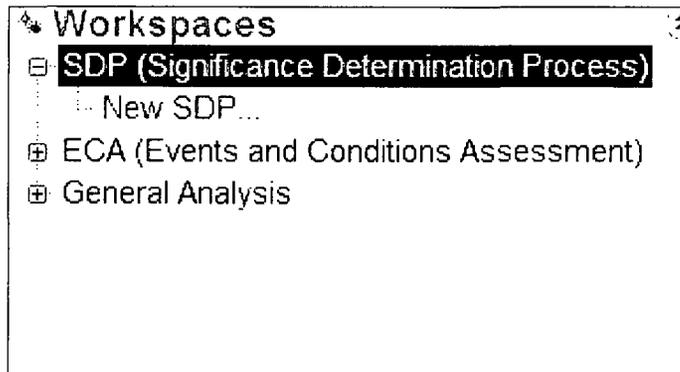
Figure 1. Workspaces selection window

Each SAPHIRE workspace can load and run a PRA model. If a PRA model is not designated as a Standardized Plant Analysis Risk (SPAR) model, then only the General Analysis workspace will be available to be used. If a model is designated as a SPAR model, then the Significance Determination Process and the Events and Conditions Assessment workspaces will also be available to be used. The SPAR models are PRA models used by the NRC. The SPAR models give the risk analysts the ability to quantify the expected risk of a nuclear power plant in terms of core damage frequency and the change in that risk given an event or an anomalous condition or a change in the design of the plant.

Workspaces for each user interface are created and saved separately from the base model which keeps the original database intact. Each workspace created can have multiple analyses performed and saved. Each time the workspace calculation is performed, the changed model becomes the "base case" for the next calculation within that workspace. The logic in the original model is kept unchanged outside of the selected workspace. Workspaces are independent of each other and modifications or calculations made within one workspace will not affect another. Only changes made to the model in the SA user interface (main screen), which is outside of the workspace environment, will overwrite the original database. Each workspace has a user interface and reports tailored for their intended uses.

Change sets are created in the workspaces by checking the desired checkboxes for systems, components, etc. These change sets are defined entirely within the selected workspace. A current limitation of workspaces is that changes sets which are defined in the Standard Analysis

(SA) user interface are not automatically carried over into the workspace when the model is loaded into a workspace from the SA space. If it is desired to apply such change sets, they would need to be mapped manually into the workspace.

2. THE ECA WORKSPACE

2.1 Motivation

The use of a probabilistic risk assessment tool and model to obtain a risk measure or "event evaluation" that is conditional on the situation that existed during an incident is a common analysis practice. To perform event evaluations, the ECA Workspace was developed. The ECA Workspace contains a simplified user interface that relies on the SAPHIRE analysis engine in order to perform analysis related to PRA incidents.

The technique known as "event evaluations" began around 1977 when the NRC Risk Assessment Review Group acknowledged the potential for accident precursor events to contribute to the overall plant operational risk. This Review Group recommended that "potentially significant sequences, and precursors, as they occur, be subjected to the kind of analysis contained in WASH-1400." One of the first full-scope PRAs, WASH-1400 (also known as the "Reactor Safety Study") provided a basis for the recommendations of the Review Group.

Following this initial recommendation in utilizing a PRA to make inference based upon quantified probabilistic models, the NRC formalized the process of using PRAs for event evaluation. In 1982, the first of a series of NUREG/CR reports was published that addressed the Review Group's recommendation. Specifically, NUREG/CR-2497, *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report*, was finished and addressed precursor events from the 1969 to 1979 time period. Following the successful completion of this analysis, other NUREG/CR reports in the series addressed precursor events for subsequent years in order to provide a historical perspective on the operation of nuclear power plants in the U.S. These additional reports are known as the ASP analyses documents.

While these older analyses utilized simplistic PRA models, tools, and evaluation techniques, current analyses (and models) have become much more complex. The development of the ECA Workspace attempted to address the complexities of both simplifying and standardizing the analysis steps required by the analysts performing event evaluations. To perform an event evaluation, several processes must be completed prior to the actual analysis of an incident such as understanding the incident and collecting data related to the analysis. This report does not address these "pre-analysis" issues. However, this section discusses three areas of interest related to the use and understanding of the ECA Workspace when performing event evaluations:

1. A theoretical framework behind event evaluation calculations.

2. Considerations when performing event evaluations using the ECA Workspace.

3. Guidance and examples for performing event evaluations when using the ECA Workspace.

2.2 The General Event Evaluation Framework

An event evaluation is completed using a PRA model to obtain a measure of risk that is conditional on the situation existing during an event or specific situation. A PRA model is modified to account for specific initiators, failures, or conditions that occurred during the event in question. (Smith, 1998)

Two types of event analysis are used for the analysis of events.

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

Examples: 1.   Offsite power was lost during a storm while operating 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 installed improperly and was inoperable for several months.

2.   A generator fuel supply was found empty due to a leak.

Figure 2 illustrates two general steps that take place during the event evaluation: (1) mapping the incident context into the PRA and (2) using PRA to determine the incident-specific risk measure. To complete these steps, gathering detailed information from the event is important. Knowledge of the system design and operation, along with details found in the PRA model, will help to better map the incident into the PRA model.
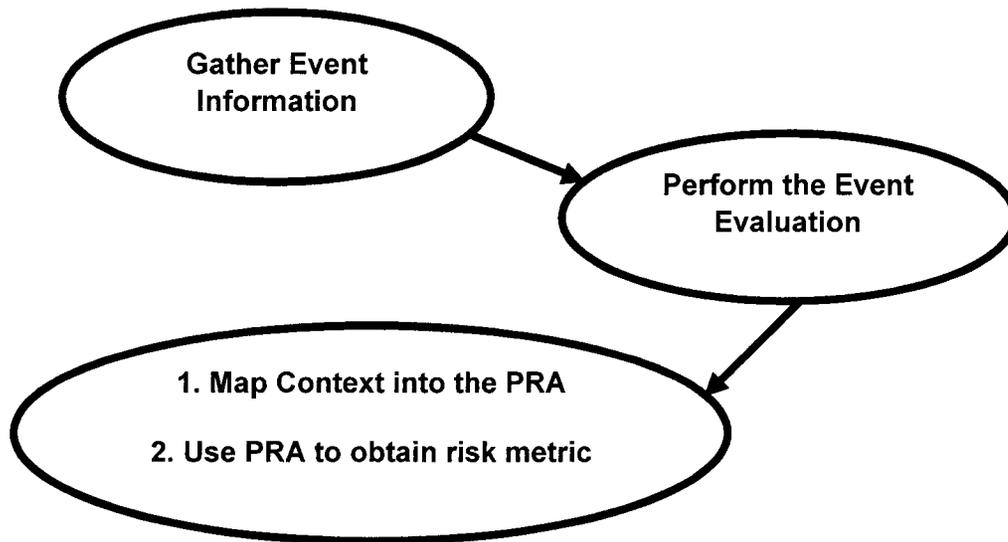
Figure 2. Event evaluation methodology

Questions such as equipment recoverability and the potential for common cause failures 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 unavailabilities (e.g., equipment out for testing)
- Conditions that may have hindered operation.
- Cause of initiating event (if applicable).

"Mapping" the event into the PRA model is a prerequisite to obtaining event evaluation measures. This mapping is the process of structuring the PRA to represent the conditions of the incident (either actual or hypothetical) being modeled. In other words, the context surrounding the incident is imposed on the PRA boundary conditions. Once the PRA model is selected, then the following steps must be performed:

- Adjust the initiating events depending on the type of event being evaluated.
- Determine the impact on system reliability, which potentially include:

7

1.   Model failed, unavailable, or degraded components.

2.   Modify common cause failure probabilities.

3.   Adjust nonrecovery probabilities where needed.

4.   Change 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, if dealing with a nuclear power plant issue, one could find a conditional probability of core damage (CCDP) given a specified initial state.

An event "importance" (or increase) can be found by subtracting the nominal core damage probability (CDP) from the CCDP. Alternatively, the ratio measure of the CCDP divided by the CDP could be used. For these calculations, traditional importance measures can also be obtained for the basic events in the PRA 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.

2.3   Conditional Probability Calculations

Conditional probability calculations estimate the probability of an end state (e.g., core damage) given that an event or condition occurred. For nuclear power plants, the general expression for the CCDP given condition Z existing is

$P(CD|Z) = P(CD \cap Z) / P(Z) = CCDP$

where $P(Z) > 0$ and

$$CD = \bigcup_{i=1}^{n} C_i$$

where C_i is the i'th core damage cut set and U is the union of these cut sets.

As a demonstration of the CCDP calculation, 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. To get core damage (CD), an initiating event (IE) is necessary and then either (1) A and B fail, (2) A and C fail, (3) B and C fail, or (4) D fails. The condition in this model is that

initiator IE occurred while component C was inoperable (and was not recoverable). Thus, it is necessary to calculate

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

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

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, the CD equation can be rewritten as

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

Now, this is effectively the expression for the minimal cut sets that one would obtain using a fault tree/event tree tool like SAPHIRE. When a set of minimal cut sets exists, only those cut sets need to be quantified to obtain results. In general, there are many ways to quantify the union of minimal cut sets. However, in PRA, it is standard to use one of three methods, which include:

1.   Rare event approximation.

This calculation approximates the probability of the union of minimal cut sets. The equation for the rare event approximation is

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

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. The equation for the minimal cut set upper bound is

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

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.

9

There are various methods of determining the exact probability given a set of cut sets. The most common approach is commonly referred by the name "inclusion-exclusion." Others include solutions via binary decision diagrams.

For this example, the nominal (unconditional) equation must first be quantified and then evaluated using both the rare event approximation and the minimal cut set upperbound.

Rare event approximation:

$$P = \sum_{i=1}^{4} C_i = P(IE \cdot A \cdot B) + P(IE \cdot A \cdot C) + P(IE \cdot B \cdot C) + P(IE \cdot D)$$

Minimal cut set upper bound:

$$P = 1 - \prod_{i=1}^{4} (1 - C_i) = 1 - [1 - P(IE \cdot A \cdot B)][1 - P(IE \cdot A \cdot C)][1 - P(IE \cdot B \cdot C)][1 - P(IE \cdot D)]$$

The condition for this example was that the evaluation of initiator IE occur while component C is inoperable (and was not recoverable). Thus, the CCDP is:

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

Rare event approximation:

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

Minimal cut set upper bound:

$$= \ 1 - [1 - P(A)][1 - P(B)][1 - P(D)] \ = 1 - (1 - a)(1 - b)(1 - d) \ .$$

To calculate the CCDP, the values for the event probabilities are needed. For this example, assume:

P(IE| IE occurred) = 1

$P(A) = 1 \times 10^{-1}$

$P(B) = 2 \times 10^{-1}$

$P(C) = 5 \times 10^{-2}$

$P(D) = 5 \times 10^{-3}$.

10

The CCDP using the assumed probability values is:

Rare event approximation:

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

$$= 0.305 .$$

Minimal cut set upper bound:

$$P(CD| IE=True, C=True) = 1 - (1 - a)(1 - b)(1 - d)$$

$$= 1 - (1 - 0.1)(1 - 0.2)(1 - 0.005)$$

$$= 0.284 .$$

Thus, the conditional core damage probability, or CCDP, given that initiator IE occurs while component C is inoperable (and is not recoverable) is about 0.28.

2.4   Event Importance Calculations

Event importance calculations attempt to estimate the change of the probability given that an event or condition occurred. The ECA Workspace is designed to automatically perform this calculation. The definition of this event importance calculation is (where component Z fails):

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

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

Note that the $Importance_{event}$ calculation is a difference of two probabilities, and, as such, is not a probability (hence the name "Importance"). For example, the CCDP could be lower than the CDP (if a hypothetical design improvement is being proposed), thereby resulting in a negative $Importance_{event}$ value. However, the $Importance_{event}$ gives a sense of the relative differences between the two probabilities.

11

2.5 Initiating Event Assessments

Components or systems that are inoperable at the time the initiator occurs increase the overall risk of the event. The CDP can be calculated that is conditional upon the initiator occurring and the initial conditions of the event. Some typical initiating events modeled in nuclear power plant PRAs include:

- Reactor trip.
- Loss of offsite power.
- Steam generator tube rupture.
- Small, medium, or large break loss-of-coolant accident (LOCA).
- Inadvertent/stuck open relief valve.

For an initiating event analysis, the ECA Workspace will allow the analyst to model the scenario where an initiating event, such as the above, has occurred. The CCDP that is quantified is representative of a instantaneous risk increase for the event. To measure this risk from a PRA, it is important to note that the results of the PRA model may be described by two parts:

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

Knowing these two parts, any type of event assessment can be performed by adjusting the relevant portions of the PRA. For example, the product $\lambda(t) \approx \Phi(t)$ is the core damage frequency. However, the CCDP for initiating event assessment is simply $\Phi(t)$ conditional on the initiator that occurred and any complicating conditions.

2.5.1 Treatment of Initiating Events for Initiating Event Assessments

For initiating event assessments, the initiating events in a model must be modified to reflect the event in question. First, for those initiators that **did not** occur, they are set to a FALSE house event. Since initiating events are ANDed with the sequence cut set basic events, sequences with a FALSE house event in every cut set will not show up in the results. In other words, the other initiators did not happen. Second, for the initiator that **did** occur, its numeric value should be modified depending on the type of initiator, either (a) non-recoverable or (b) recoverable.

- Non-recoverable Initiators – Set the initiating event to a TRUE house event (or probability of 1.0). For example, in the case where offsite power is lost (LOSP), *and if* there is no chance of recovering offsite power, the initiating event should be set to a TRUE house event.

- 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 nonrecovery probability.

For initiating event assessment, the initiating events should be modified according to the flow diagram below in Figure 3.
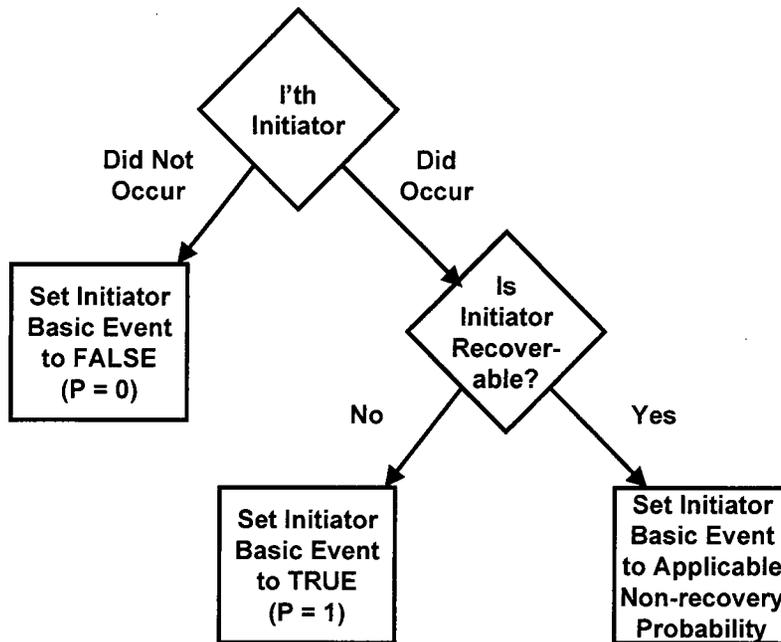
Figure 3. Modification of initiating events during an initiating event assessment

2.5.2 Treatment of Component Recovery for Initiating Event Assessments

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. 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 (in the time available) component failure
- Harsh environment (e.g., high radiation, high temperature)
- Location (e.g., inside containment versus outside)
- Timing/staffing limitations

13

If a component or system **is** recoverable, its nonrecovery basic event should be set to an appropriate nonrecovery probability. If a nonrecovery event is not present, then set the component event to an appropriate nonrecovery probability.

In summary, the component-level nonrecovery should be incorporated into the PRA according to the flow diagram below in Figure 3. When using this process, one should be aware that setting a component to TRUE may affect how the "recovery rules" are applied (for more on recovery rules, refer to the Technical Reference, Volume 2).
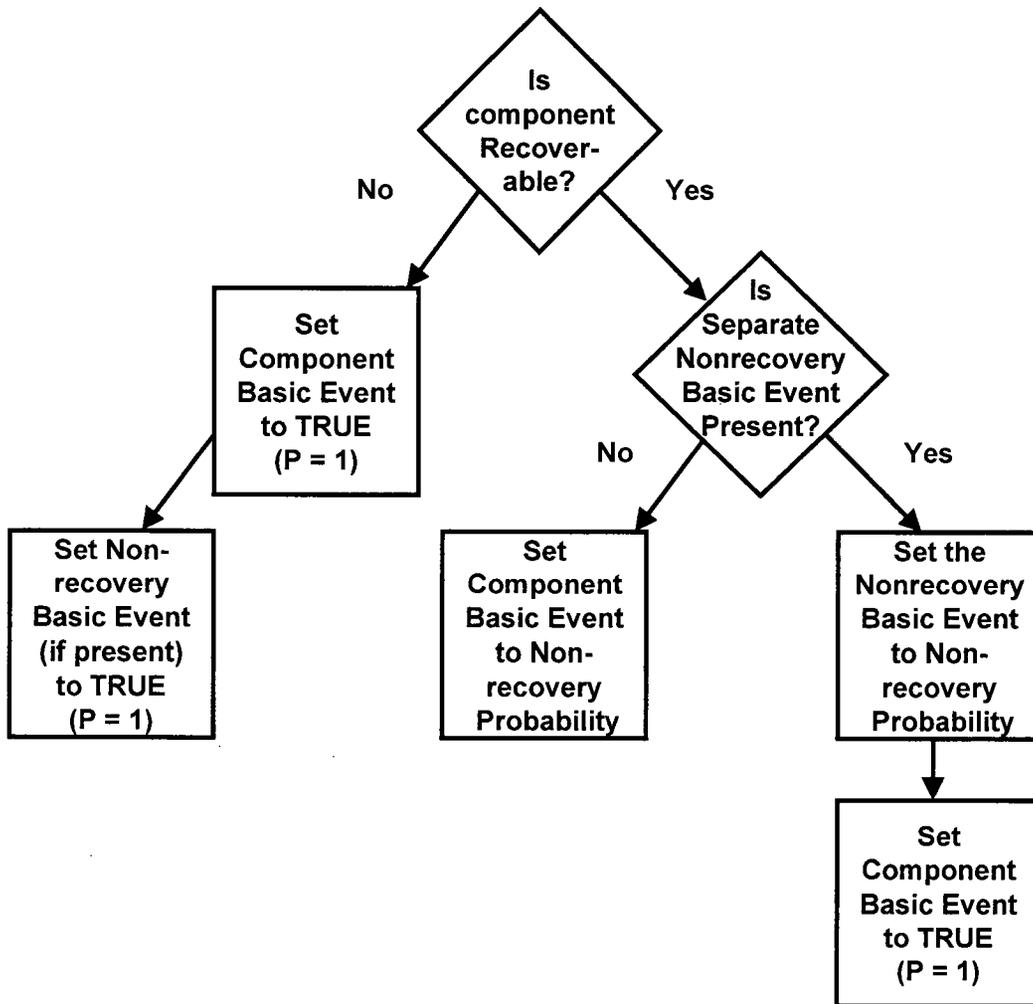
Figure 4. Modification of component non-recovery events during an initiating event assessment

2.5.3 Treatment of Common Cause Failures for Initiating Event Assessments

Many PRA models have common cause failures (CCF) included in the fault tree logic. These CCF events are generally either train-level or component-level events. 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. However, during an event evaluation, SAPHIRE will 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. The ECA Workspace uses the CCF adjustments as described by Rasmuson and Kelly. [2008]

The CCF module that makes adjustments uses Boolean reduction to realize combinations of CCF basic events, and removes approximations made in the conditional CCF probability modeling for events assessment as a result of setting components' failure modes to 1, TRUE, 0, or FALSE. The RASP common cause method is a new calculation type in SAPHIRE. The RASP CCF method provides a way to evaluate nominal and conditional CCF probabilities. When using the RASP CCF method, the user will select a specific type of failure:

- Component is failed (unknown type)
- Component is failed (dependent type)
- Component is failed (independently)

2.5.4 Appropriate Risk Measure for Initiating Event Assessments

In the ECA Workspace, 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) and the component, train, or system that are inoperable at the time the initiator occurs. An event importance (i.e., Importance$_{event}$) is not generally calculated for initiating event assessments since the determination of the CDP may not be obvious (e.g., is instantaneous probability or the probability over a short duration needed?).

2.6   Condition Assessments

An event assessment analyses is 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 inoperable for a certain length of time and no initiator actually occurred during this time. The "length of time" is the duration over which the risk is measured. This duration of increased risk is shown in Figure 5. In this figure, $\lambda(t)$ is the initiating event hazard rate and $\Phi(t)$ is the conditional probability of core damage given an initiating event.

15

Conditional Core Damage Hazard Rate
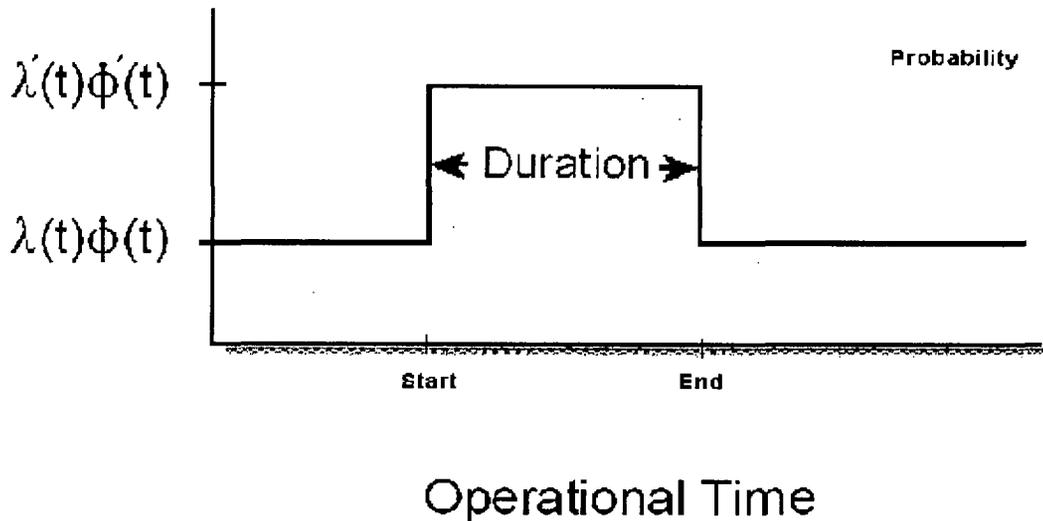
Figure 5. Example of the increase in risk during the duration of a component outage

For component outages, the ECA Workspace assumes that the risk is assumed constant over the duration of the event. This constant (the λ' Φ' from Figure 5) is the *conditional* risk result given by the PRA model. If the configuration changes (say due to maintenance, testing, or other failures), then there is a new risk level.

2.6.1 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, the Workspace calculation will 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. Assuming that the arrival of an initiating event can be modeled as a standard Poisson process, the probability of core damage is expressed as

$$P(core\ damage) = 1 - e^{-\lambda' \phi' T}$$

where: λ is the arrival rate of the initiating event (with units of inverse time)

Φ is the probability of the accident sequence cut sets

T is the duration (with units of time).

This calculation assumes the λ and Φ are constant over time T.

2.6.2 Treatment of Components and Common Cause 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. For this evaluation step, the treatment of components for condition assessments is identical to that presented for initiating event assessment (Section 2.5.2). The treatment of common cause failures is the same as that in the initiating event assessment section (Section 2.5.3).

2.6.3 Appropriate Risk Measure for Condition Assessments

In the ECA Workspace, the risk measure that is used for **condition assessments** is the "event importance" (i.e., Importance$_{event}$). The event importance for core damage models is

Importance$_{event}$ = CCDP - 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 and components, trains, or systems that are inoperable for the duration of the event. However, while the Importance$_{event}$ is the primary risk measure used, the ECA Workspace calculates both the CCDP and CDP and provides these as part of the results.

Below, Table 1 compares the two types of event evaluations, showing the unique identifying attributes for the two types of event assessments, how initiators are treated, how component events are modified, and the applicable risk metrics.

17

Table 1. Overview of the important attributes of initiating and condition assessments.

Item	Assessment Type	
	Initiating Event Assessment	Condition Assessment
Unique Attributes	Initiating event happens (a point in time)	One (or more) component is unavailable for some duration of time (t1 → t2) Initiating event did not occur
Treatment of Initiating Events	Set initiator to 1.0 (or non-recovery probability) for the initiating event that occurred. Others initiators are set to zero.	$CCDP = 1-exp[-\Sigma (\lambda i \, \Phi i) \, T]$ where, λi = i'th initiator frequency $\Phi i = P(CD \mid i'th\ initiator)$ T = duration of condition
Treatment of Components	Failed components → TRUE (or nonrecovery probability) and adjust CCF. Non-failed components → leave at their nominal failure probabilities	Failed components → TRUE (or nonrecovery probability) and adjust CCF. Non-failed components → leave at their nominal failure probabilities
Risk Metric	CCDP	Ie = CCDP - CDP

2.7 Events and Condition Assessment Uncertainty Analysis

Two general calculation types are performed, initiating event assessment and condition assessment. For the former, a single metric, the CCDP, is calculated. This metric is used in an absolute sense in that its numerical value is not subtracted from a nominal value to obtain an increase in risk. However, the condition assessment calculation requires two metrics, a CCDP and a CDP. In this calculation, the risk increase (over the time of the condition) is calculated.

Historically, only a point estimate value was calculated for the condition assessment CCDP and CDP. These two values were then subtracted to find the risk increase. However, a variety of complications arise when this approach is used, specifically on the change in risk measure, or "event importance" (Ie) which is given by the relationship

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

where:

CCDP = the conditional core damage frequency (CCDF) duration of the condition

CDP = the core damage frequency (CDF) duration of the condition

The uncertainty results are based on sampling from the component's variability and then solving for the CCDF and CDF based on the sampled probability. SAPHIRE then subtracts CDF from CCDF to obtain a sampled ΔCCDF, which is multiplied by the duration. SAPHIRE stores this calculated value and continues this process for the number of samples noted. Once SAPHIRE has performed the number of specified samples, it orders the ΔCCDP values and pulls out the 5th, 50th, and 95th, then calculates the mean by summing up the ΔCCDPs and divides it by the number of samples.

The algorithm used to determine the uncertainty on the Ie using either Monte Carlo or Latin Hypercube sampling is given below:

1. Solve all cut sets (to the project truncation level) for all sequences. Two lists are solved and stored, one for the nominal CDP case and one for the condition CCDP case.

2. Create a list of all basic events appearing in cut sets for either the nominal or condition cut sets. There will be a total of J number of basic events.

3. Start the uncertainty sampling loop.

    For I = 1 to N, where N is the total number of iterations specified by the user.

    a. Go through the list of J events. For each event, obtain a random sample. If events are correlated, obtain a single value for all events in that correlation group. If an event is modified for the condition case, it will appear in the list twice, once to be used for the nominal (CDP) case and once for the condition (CCDP) case, with its values set for the respective case.

19

b. Calculate CDP_I, where $CDP = 1 - \exp(-\lambda_{CDF} * Duration)$. The λ_{CDF} is the value of the core damage frequency from the nominal case cut sets quantified using the samples obtained in Step 3a.

c. Calculate $CCDP_I$, where $CCDP = 1 - \exp(-\lambda_{CCDF} * Duration)$. The λ_{CCDF} is the value of the core damage frequency from the condition case cut sets quantified using the samples obtained in Step 3a.

d. Calculate Ie, where Ie = CCDPI - CDPI.

e. Store Ie, $CCDP_I$, and CDP_I into their own respective array, where each array is N elements long.

Repeat the **I loop** N times.

4. Once the I loop is complete and the three results arrays (Ie, CCDP, and CDP) are populated, sort each array.

5. From each result array, determine the moments and percentiles.

This uncertainty analysis is performed in SAPHIRE Version 8. The graph of the uncertainty analysis, as shown in the Figure 6, is available in the ECA Workspace reports. It color codes the percentages of the probability distribution function between the orders of magnitudes.
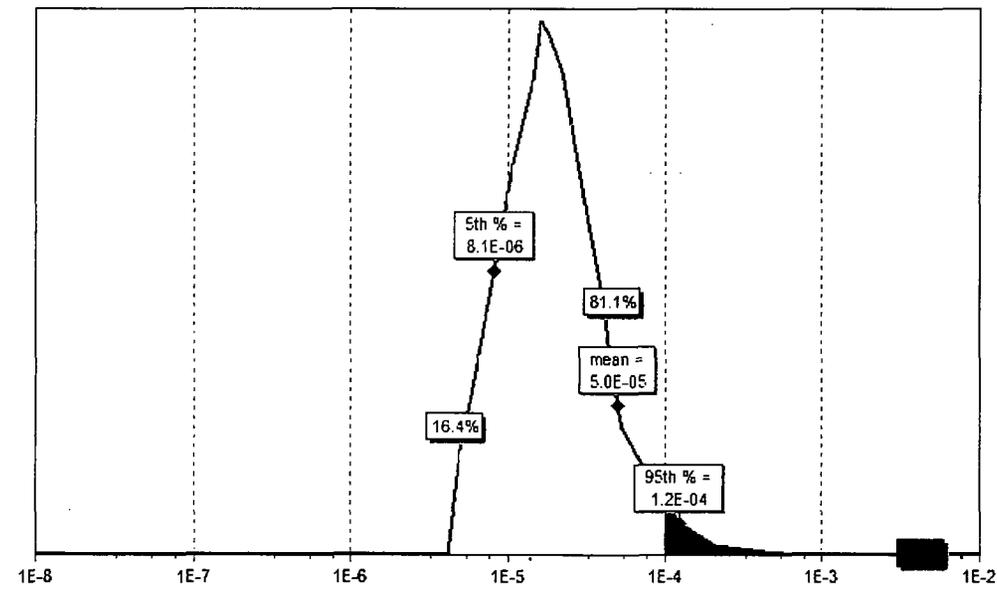
Figure 6. Graph of uncertainty analysis results

2.8   Performing an Initiating Event Assessment

To start the event assessment process, the analyst selects the "ECA (Events and Conditions Assessment)" option from the Workspaces menu option (Figure 7).
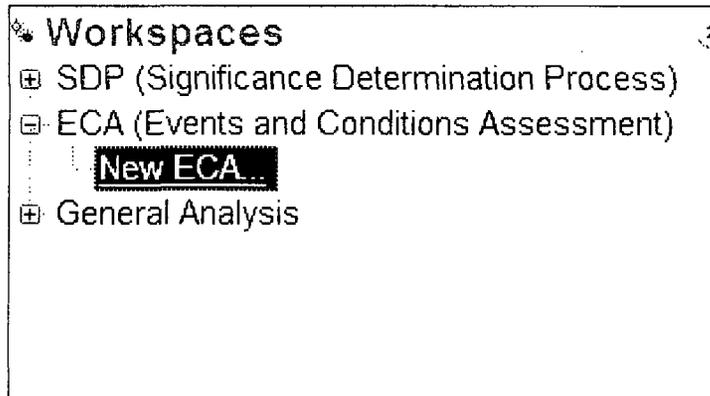
Figure 7. Events and Conditions Assessment workspace option

This option requires a double click and then SAPHIRE copies all of the information from the project into a new workspace. By making this copy, any modifications will only be saved for this particular analysis and the original model will not be affected. SAPHIRE Version 8 then loads the Events and Conditions Assessment Type analysis screen, which allows the analyst to select the type of assessment by selecting the appropriate radio button to start mapping the event into the PRA model (Figure 7).
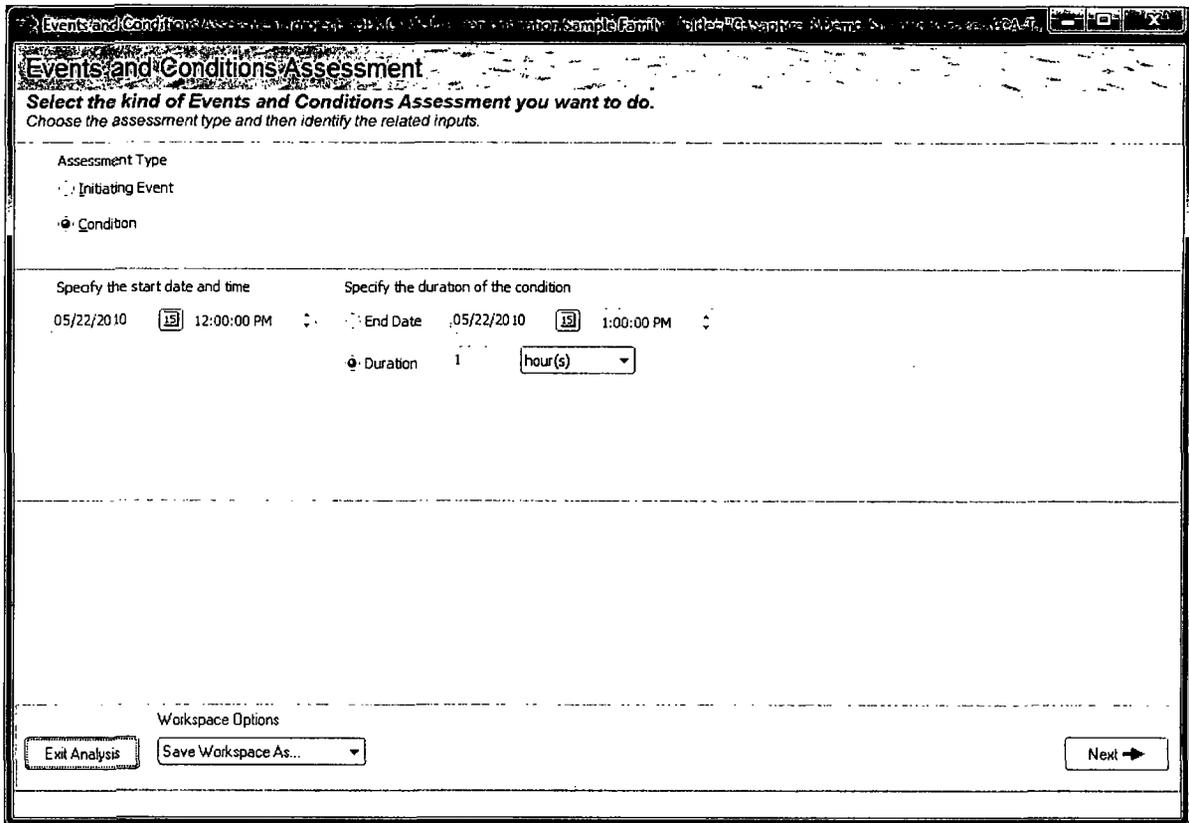
Figure 8. ECA analysis screen

Once the Initiating Event assessment type radio button is selected, SAPHIRE loads up all of the initiating events developed in the PRA model (Figure 9). The analyst then selects the initiating event that occurred and selects the Next button. Note that in the simple demonstration project shown, only a single initiating event is used in the project.
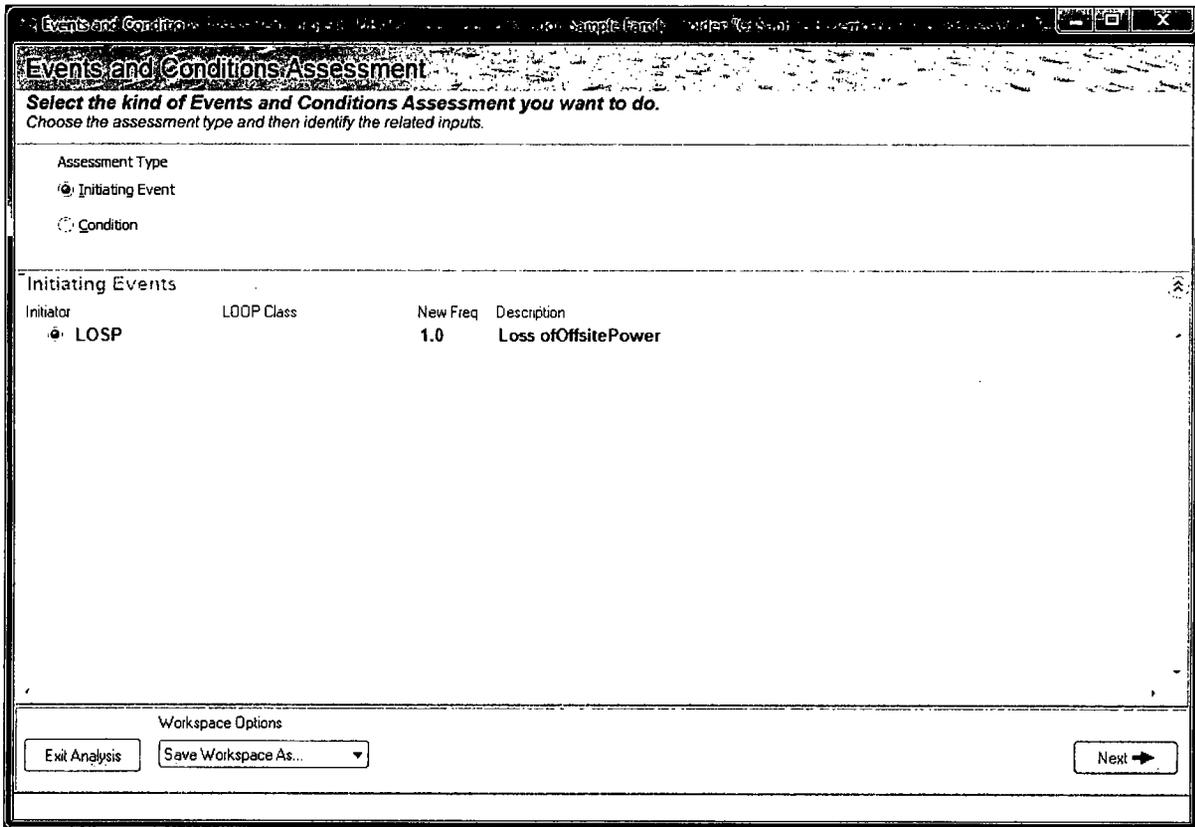
Figure 9. ECA Initiating Events selection screen

SAPHIRE now displays a screen that contains all of the basic events found in the project. This list is used to finalize the assessment by selecting those component(s) that failed or could potentially fail if required during the mission time (Figure 10). After all of the affected components have been selected, the Next button is clicked to continue the assessment process.
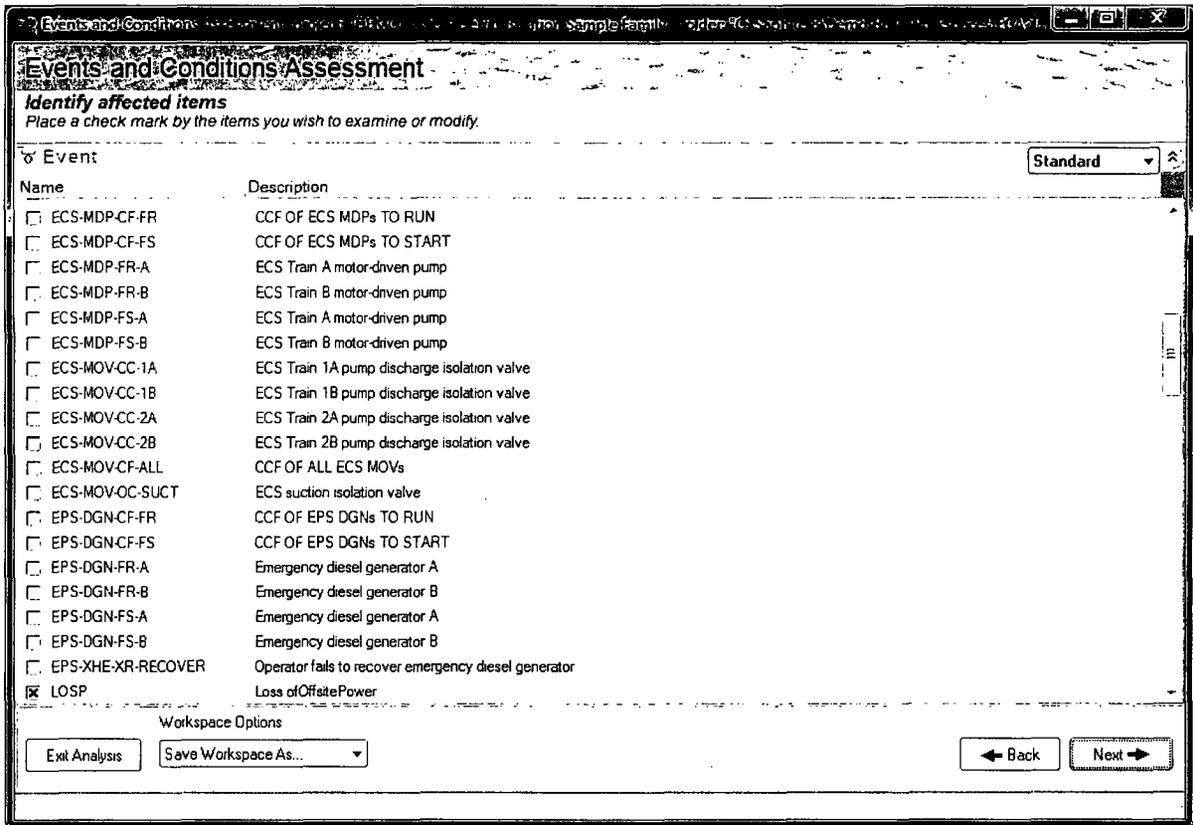
Figure 10. ECA Basic Events selection screen

The next screen is designed to make the probability modifications to the selected component(s). There are four probability options that can be selected for the component(s), as shown in Figure 11.

Events and Conditions Assessment

Modify the items identified in the previous step.
Further instructions here.

☞ Event

Event	Modification Type	New Prob/Freq	Nominal Prob/Freq
⊟ CCS-MOV-CC-1A	CCS Train 1A pump discharge isolation valve		
Edit	Edit	5.000E-3	5.000E-3
⊞ LOSP	Loss of Offsite Power		
Edit	Edit	1.0	4.000E-2/year

Modify Basic Event - (CCS-MOV-CC-1A)

⦿ New probability / frequency 5.000E-3

○ Failed (Independent failure) <P = 1.0>

○ Failed (potential CCF) <True>

○ Not failed <False>

✔ OK   ✘ Cancel

Workspace Options

Exit Analysis   Save Workspace As... ▼ Go   ◆ Back   Next ◆

Figure 11. ECA Basic Event modification screen

The first option allows for the component's probability to be changed from its nominal probability to some other value. This value could be any value between 0.0 and 1.0. The next option tells SAPHIRE that the component failed but its failure was an independent failure. This means that the mechanism that caused the component to fail will not cause any similar components to fail the same way (i.e., no common mode failure). The next radio button sets the component to a True house event, which tells SAPHIRE that the component(s) failed due to a potential common cause; therefore, SAPHIRE will automatically adjust the component's common cause failure probability. The last radio button tells SAPHIRE that the component cannot fail, house event False.

Once the component's probabilities have been modified, the Next button is selected. The next screen provides the analyst with solve options (Figure 12).

The analyst can select whether a single or multiple pass solution is required. The single pass option will only solve the model and apply the recovery rules. The multiple pass will solve the model, apply the recovery rules, and perform a cut set update to remove any potential non-minimal cut sets that could have been created from the recovery rules.

- The specification of the truncation level to be used is specified along with the uncertainty information (number of samples, seed number, and type).

25

- Option to perform a zero test and maintenance calculation.

- Selection of model types to solve (model types other than "Random" can be solved in the ECA interface).

- Option to turn off the uncertainty analysis.

- Report options, including output format types (e.g., .html, .pdf).

Lastly, a title for the analysis along with a description of the event can be input into their appropriate spots. This will keep all of the information together.

Figure 12. ECA Solve options screen for Initiating Event assessment.

Now that all of the information has been specified, click the Finish button to analyze the event. SAPHIRE will provide an output of the assessment on the last screen.

2.9   Performing a Condition Assessment

To start the event assessment process, the analyst selects the "ECA (Events and Conditions Assessment)" option from the Workspaces menu option. This option requires a double click (on New Analysis...) and then SAPHIRE copies all of the information from the project into a new workspace. By making this copy, any modifications will only be saved for this particular analysis and the original model will not be affected. SAPHIRE Version 8 then loads the Events and Conditions Assessment Type analysis screen, which allows the analyst to select the condition assessment by selecting its radio button to start mapping the event into the PRA model.

Once the condition assessment type radio button is selected, SAPHIRE loads up the condition duration screen (Figure 13). This screen is used in the final calculation of the conditional core damage probability. (For condition assessments, the results are Importance$_{ECA}$ = CCDF*duration – CDF*duration, where the CCDF is the results of the mapped event in the PRA and the CDF is nominal frequency of the PRA.) The analyst then specifies the duration of the event in hours, days, weeks, months or years, and selects the Next button.

Figure 13. ECA condition duration screen.

SAPHIRE now displays a screen that contains all of the basic events found in the project. This list is used to finalize the assessment by selecting those component(s) that failed or could potentially fail if required during the mission time. After all of the affected components have been selected, the Next button is clicked to continue the assessment process.

The "solve options" screen (Figure 14) is designed to make the probability modifications to the selected component(s). There are four probability options that can be selected for the component(s). These have been discussed in the initiating event assessment section.

Once the component's probabilities have been modified, the Next button is selected. The next screen provides the analyst with solve options. The options are the same as discussed for the Initiating Events analysis.

Figure 14. ECA Solve options screen for Condition Assessment

Now that all of the information has been specified, click the Finish button to analyze the event. SAPHIRE will provide an output of the assessment.

2.10 The Multi-pass versus Single Pass Option

SAPHIRE Version 8 has two options when solving a model in a Workspace:

- Single pass with cut set update option
- Multi-pass

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. In older versions of SAPHIRE, it is possible that these two cases could be solved at different sequence truncation levels resulting in calculating a delta between results truncated at different levels.

These two algorithms are outlined below, where the single-pass solution is listed in Table 2 and the multi-pass solution is listed in Table 3.

Table 2. Steps for the "single-pass" solution.

Step	Processes
1	Recalculate the "nominal case" to be able to determine the increase in risk. a. Generate basic event data with no change sets marked. If the no test/maintenance option is used, all T&M events will be set to zero. b. Solve all sequence cut sets using a predetermined (but low) truncation. c. Apply recovery rules to all sequence cut sets. d. If identified in the project constants, perform a cut set update to ensure non-minimal cut sets are removed. e. Re-quantify the cut sets. f. Store the cut set results via a base case update.
2	Calculate the risk increase. a. Generate basic event data with SDP changes indicated by the analyst. If the no test/maintenance option is used, all T&M events will be set to zero. b. Solve sequence cut sets using the same truncation for the "nominal" case. c. Apply recovery rules to all sequence cut sets. d. If identified in the project constants, perform a cut set update to ensure non-minimal cut sets are removed. e. Re-quantify the cut sets. f. Store the cut set results for use in determining the SDP annualized CDF.

Table 3. Steps for the "multi-pass" solution.

Step	Processes
1	Recalculate the "nominal case" to be able to determine the increase in risk. a. Generate basic event data with no change sets marked. If the no test/maintenance option is used, all T&M events will be set to zero. b. Solve all sequence cut sets using a predetermined (but low) truncation. c. Apply recovery rules to all sequence cut sets. d. If identified in the project constants, perform a cut set update to ensure non-minimal cut sets are removed. e. Re-quantify the cut sets. f. Store the cut set results via a base case update.
2	Calculate the risk increase. a. Generate basic event data with SDP changes indicated by the analyst and store these values for use in Step 2g. If the no test/maintenance option is used, all T&M events will be set to zero. b. Change TRUE events to 1.0 events (to ensure application of recovery rules). c. Solve sequence cut sets using the same truncation for the "nominal" case. d. Apply recovery rules to all sequence cut sets. e. Change events having a probability of 1.0 to TRUE events (to ensure that non-minimal cut sets will be removed during the next step). f. Perform a cut set update to ensure non-minimal cut sets are removed. g. Re-quantify the cut sets so they have the proper values stored from step 2a. h. Store the cut set results for use in determining the SDP annualized CDF.

2.11 ECA Workspace Reports

Reports of varying detail are selectable, and include:

- Model information

- CCDP, CDP, and ΔCDP

- Solve settings

- Uncertainty distribution graph on the importance ΔCDP for condition assessments, or, uncertainty distribution graph on the CCDP for initiating event assessments. The graphs are colored by order of magnitude intervals and display the point estimate, mean, and quantiles.

- Event tree dominant results

- Dominant sequence results

- Referenced fault trees

- Sequence importance measures

- Referenced events

3. THE SDP WORKSPACE

The SDP workspace within SAPHIRE 8 has been developed to aid analysts perform inspection finding evaluations. The SDP workspace automates the analysis process and provides result reports.

The SDP workspace calculates the increase in CDF based on the inspection finding. The SDP risk measure is called "delta CDF" (i.e. ΔCDF). The delta CDF is similar to a calculated conditional core damage probability (CCDP), which is the probability that a core would have gone to a damage state given that (i.e., conditioned on) a specific initiating event occurred and the actual plant equipment and operator responses are accounted for. This "event" use of CCDP represents the remaining probabilistic "margin" (related to defense-in-depth) to core damage at a precise moment in time.

The SDP calculation, in general, is the nominal CDP, which accounts for normal maintenance, subtracted from the CCDP to obtain the change in CDP due to degraded condition(s) (i.e., CCDP - CDP = ΔCCDP, normalized by dividing it by 1 year). The baseline CDF contains test and maintenance practices already in the results; therefore, the SDP evaluation accounts for nominal equipment outages as probabilities at that particular time as part of the degraded equipment or function. The SDP evaluation will also account for the degraded equipment or functions identified during the inspection.

3.1   Starting an SDP Analysis

To begin the SDP evaluation, the appropriate PRA model must be opened within SAPHIRE 8. The initial start up of SAPHIRE 8 allows the opening of the previously worked project or the selection of a new project using the **Browse** option. If the previously loaded project is the appropriate PRA model, then select

- Modify a Reliability or Risk Analysis Project "green arrow" to modify the project, or

- Perform an Analysis "green arrow" with the New Significance Determination Process (SDP) selected in the drop down box to start an SDP analysis.

If the previously loaded project is not the appropriate PRA model, then select the appropriate PRA model by selecting Browse button and scrolling through the folders. Highlight the *.SRA file (or the FAM.DAT file) and click Open button or double click the *SRA file. SAPHIRE will load the selected project.

Note that SAPHIRE 8 may also open compressed (.zip or .exe) files directly if they exist in the project folder. These files (from the compressed file) will overwrite existing files in the folder – however the user will be prompted to confirm opening the compressed file prior to any files being overwritten (as shown in Figure 15).
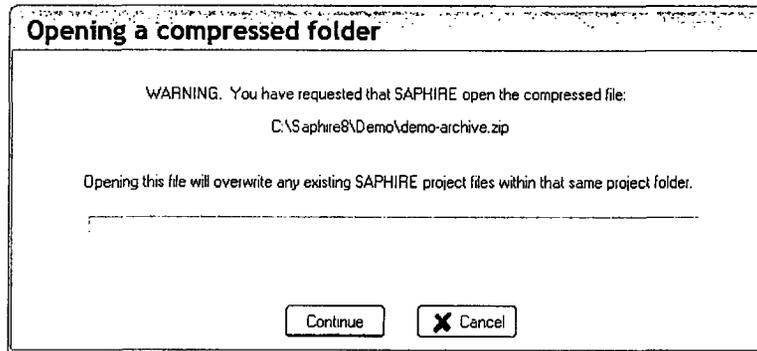
Figure 15. Warning message when opening a compressed project

With the appropriate PRA model loaded, select the "plus box" next to the Significance Determination Process (SDP) located in the Workspaces list. Then, double click the "New SDP..." option to start a new SDP analysis.
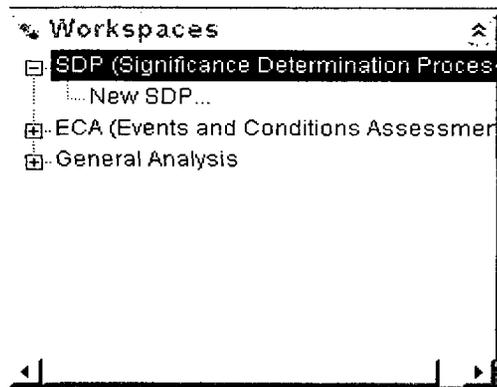
The SDP workspace follows a four step process:

```
┌─────────┐          ◇
│ Select  │         ╱ Identify ╲
│ Plant   ├────────◇  affected   ◇     Step 1
│ Model   │         ╲ initiators ╱
└─────────┘          ╲   and   ╱
                      ◇ components ◇

                      ◇
                     ╱ Modify ╲
                    ◇ affected  ◇      Step 2
                     ╲ initiators ╱
                      ╲   and   ╱
                       components

                      ◇
                     ╱ Provide ╲
                    ◇ analysis  ◇      Step 3
                     ╲ information ╱
                      ◇

                      ◇
                     ╱ Quantify ╲
                    ◇ and view   ◇     Step 4
                     ╲ results  ╱
                      ◇
```
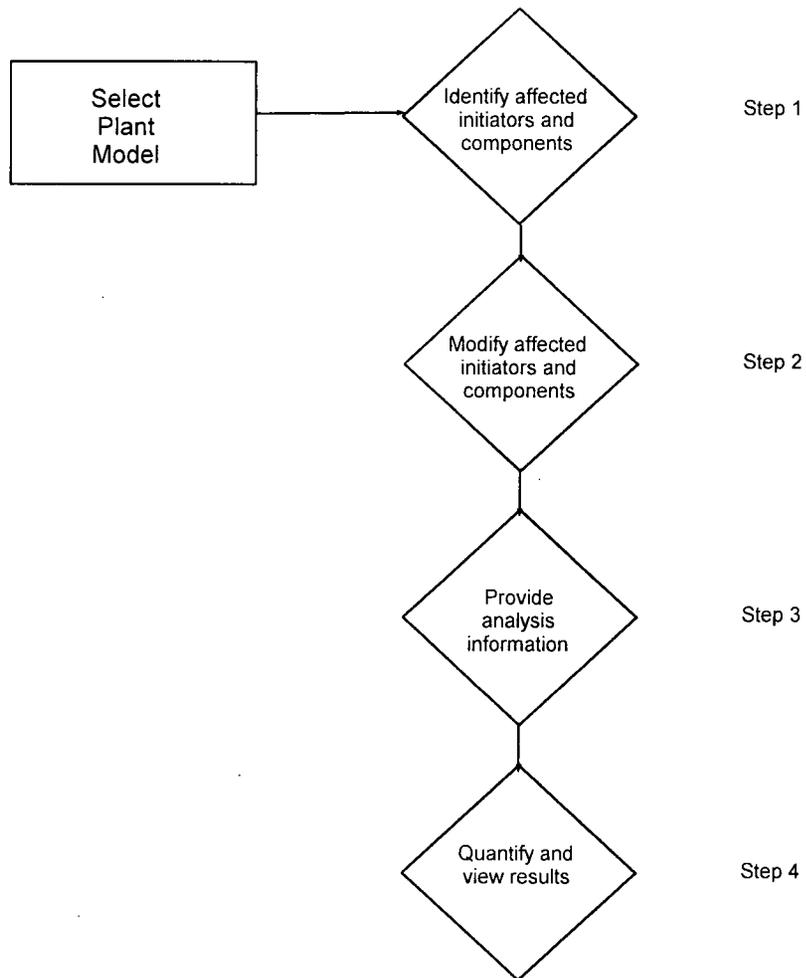
3.2   Identify Affected Items

Step 1 in the SDP evaluation is to select the initiator to adjust and/or the system(s) which have a performance deficiency.

Significance Determination Process

Step 1. Identify affected initiators and components *Select a system on the left to view its associated components. Mark the components/initiators affected by the condition being analyzed.*

| Initiators | Electrical Power System (EPS) |

| Containment Cooling System (CCS) | Safety Injection System (SIS) |

| Emergency Cooling System (ECS) | |

Safety Injection System (SIS)
  ☐ RWST (SIS-TNK)

Related Diagrams

Uncheck All Components

🔍 Search

Workspace Options

Exit Analysis | Save Workspace As... ▾ | Go

Next ➡

All of the identified systems for the plant are listed on this screen. By clicking the system button, the components that make up the system will appear in the empty field to the right. In addition, a button labeled "Initiators" is available on this screen that when clicked, lists all the initiating events indentified in the SPAR model. This button can be used for initiating event assessments.

Also, a search box is available in the bottom-left corner. Enter text related to components or systems in the text box and then click Search. The results of the search will be displayed in the right-hand side of the window.

The "Uncheck All Components" button will uncheck any components or initiators that may be checked (for example, if revisiting an old analysis). If the project has piping and instrumentation diagrams (P&IDs), the P&IDs will be shown in the "Related Diagrams" area at the bottom of the screen (see Figure 16).
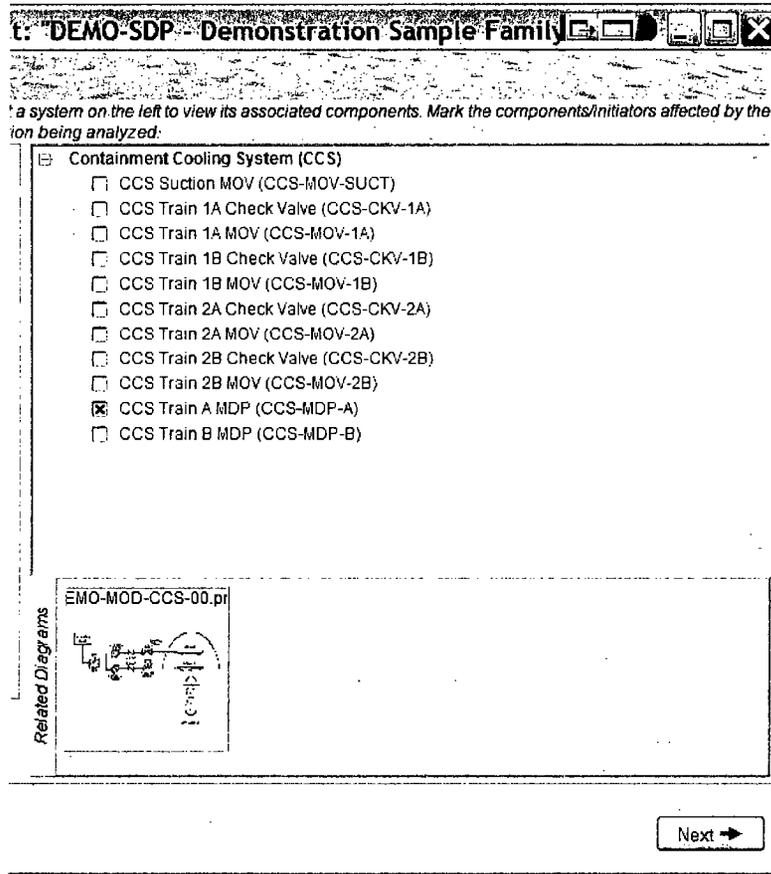
Figure 16. Thumbnail image for the P&IDs related to systems

Clicking on the diagram thumbnail will bring up the P&ID graphic (see Figure 17).
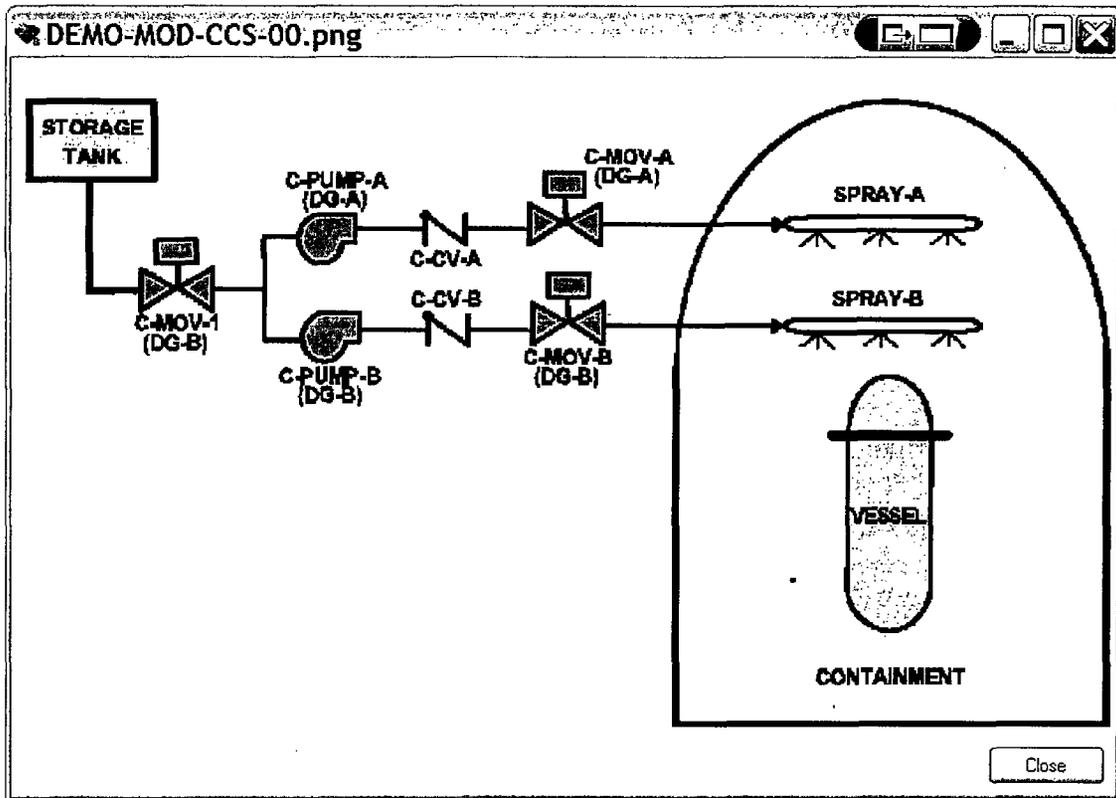
Figure 17. Example P&ID for the CCS system

Note that this P&ID figure is only for display purposes and does not contain links or information specific to any particular component.

By clicking on a system, for example CCS, all of the components in the PRA database that are related to the CCS system show up. Now that for the CCS components that show up in the list, any component can be selected by clicking the check box next to the component name (CCS Train A MDP in Figure 18). Selecting a component indicates that it will be modified for the analysis. Click any additional systems and its relevant components as needed for the analysis.

Once all relevant components from the applicable system(s) have been selected, click the "next" button.
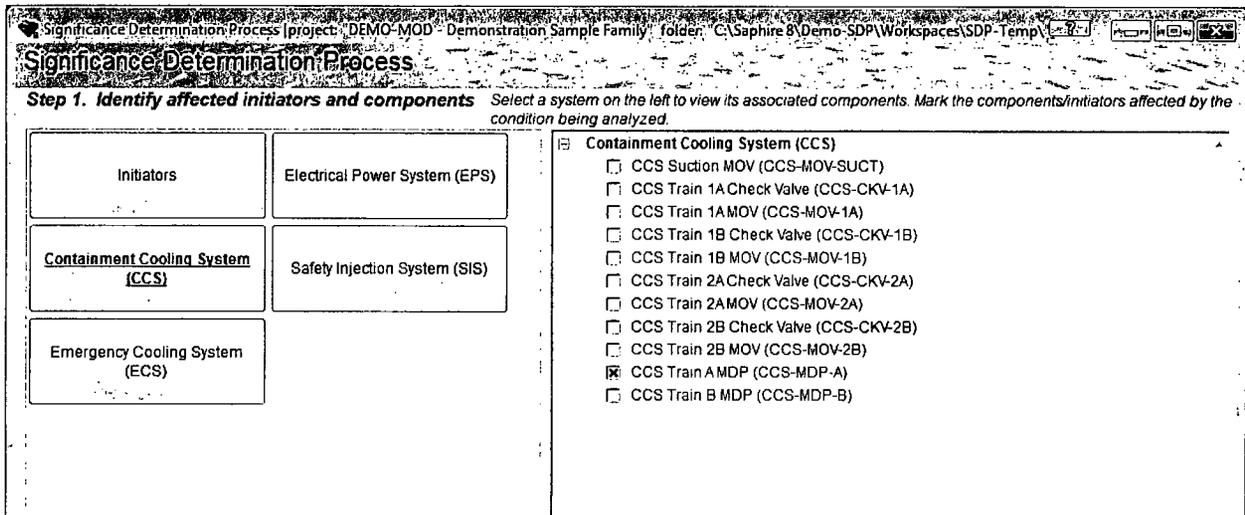
Figure 18. Selection of Train A MDP in the CCS system

3.3   Modify Selected Items

Step 2 in the SDP evaluation is to modify the selected component(s) from Step 1. The component(s) listed should appear and can now be modified. Modifying a component is performed by clicking the text "Default - Leave As Is". This will create a drop down box with a variety of options. In general, there are three different modifications allowed

1. New probability

2. Out for Test & Maintenance (only listed on T&M events)

3. True[1] (Component is Failed)

---

[1] Note that "True" should be used rather than setting a "new probability" to a value of 1.0.

Significance Determination Process

Step 2. Modify Component States   *Indicate the modifications to the applicable failure modes of the components selected on the previous step.*

Component Failure Type	Modification Type	New Failure Probability	Nominal Probability
⊟ **Containment Cooling System (CCS)**			
⊟ CCS Train A MDP (CCS-MDP-A)			
Fails to run (FR)	True (Component Is Failed ▼)	1.000E+0	2.400E-4
Fails to start (FS)	Default - Leave As Is		3.000E-3

Workspace Options

| Exit Analysis | Save Workspace As... ▼ | Go | ◆ Back | Next ◆ |

Note that if a component is failed, SAPHIRE 8 will automatically adjust the associated test and maintenance event (if any) so that the correct cut sets will be generated. Only one failure mode should be adjusted for each component. The failure mode that is observed should be the one modified. The other failure modes should be left as is since SAPHIRE will automatically make the appropriate adjustments to basic events related to that failure mode. For the figure above, "Fails to run (FR)" is highlighted and changed to "True" using the drop down box. Click next to continue.

3.4   Analysis Settings

Step 3 in the evaluation is to provide analysis details and add descriptive text.

On this step insert the start date of the finding. The drop down boxes allow for easy modification. The default is the current date and time from the computer clock. Then, the end date or duration needs to be specified. The duration can be specified in hours, days, weeks, months or years. The default is one day. For this example, we used 45 days, as shown in Figure 19.

40

Figure 19. Analysis options available in the SDP Workspace

A short description can be added about the finding. Also, a blank memo area (labeled "Analysis notes or information") is provided to the analyst in order to add more detailed information about the inspection finding. This information will be carried along and placed in the final report for record keeping. Simple HTML-based formatting (e.g., bold, underline, large fonts) may be applied to the text in the memo area.

The type of report (.HTML or .pdf) should be specified.

The option to evaluate screening LERF results should be check if desired. Note that this option may not be displayed depending on the user settings that are specified in SAPHIRE (under the Main Menu, Project, User Settings options).

The type of model (Full Power, Fire, Flood, etc.) should be indicated as applicable to the analysis. The default is "Random" which indicates that only full-power, internal events will be evaluated.[2]

The option to modify the truncation level may be changed as desired, but should be set to a low enough value. Note that this option may not be displayed depending on the user settings that are specified in SAPHIRE (under the **Main Menu, Project, User Settings** options).

---

[2] The current SDP Workspace has been designed for at-power internal events SDP analyses only.

After the relevant information is added, click the "Finish" button at the bottom of the screen to start the analysis.
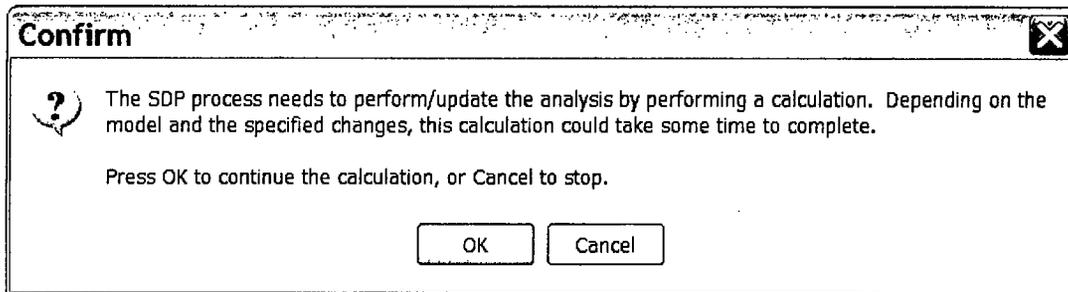
Note: SAPHIRE prompts the analyst about the analysis and the potential time involved. To continue click "OK", or to stop click "Cancel". If "OK" is clicked, a clock will appear to indicate that SAPHIRE is processing the analysis. While the DEMO-SDP model takes only a second or two to perform the SDP calculation, other models may take significantly longer.

3.5   SDP Analysis Results

Step 4 in the SDP evaluation consists of viewing the results. An example of the main output is shown in Figure 20.

Step 4. Analysis Results

Significance Determination Process
May 22, 2010 12:31 PM

Demonstration Sample Family

AFW Train A MDP failed

Increase in Yearly Core Damage Frequency

$$10^{-8} \quad 10^{-7} \quad 10^{-6} \quad 10^{-5} \quad 10^{-4} \quad 10^{-3} \quad 10^{-2}$$

I. Summary **Condition: Green: 5.4E-07/yr**

The given condition duration is 45 days.

Containment Cooling System (CCS) CCS Train A MDP (CCS-MDP-A) had adjustments made to the following failure modes:

- Fails to run (FR) was changed from 2.400E-4 to True (Component Is Failed). This implies that the component was failed for the entire duration.

Multi-pass option with cut set update calculation used.

Used truncation value of 1E-12

Model Version: 0.0

II. Insights

The affected components had only a minor impact on the accident sequences. However, further evaluation for LERF and external events for SDP Phase 2 analysis may be necessary since the increase in the CDF is greater than or equal to 1E-7/yr.

Since the annualized CDF increase is greater than 1E-7/year SDP recovery action credit should be considered if all the recovery action credit questions are answered "yes."

The following accident sequences were most impacted (by total increase):

Event Tree	Sequence	Failed Systems	Increase	(Factor Increase)
LOSP	3	ECS, CCS	5.4E-7	(1.1)

Workspace Options

Exit Analysis   Save Workspace As... ▼ Go

Report Options

Print Report... ▼ Go   ◀ Back

Figure 20. Report of results from the SDP Workspace

The output results are broken down into five sections:

1. Summary

2. Insights

3. Figures

4. Notes

5. SPAR Model Insights

3.5.1 Summary Results

The first section provides a summary that includes a graph illustrating the delta CDF and its risk significance, the duration of the condition, and the component(s) that were unavailable along with its failure setting.

I. Summary   Condition: Green: 5.4E-07/yr

The given condition duration is 45 days.

Containment Cooling System (CCS) CCS Train A MDP (CCS-MDP-A) had adjustments made to the following failure modes:

Fails to run (FR) was changed from 2.400E-4 to True (Component Is Failed). This implies that the component was failed for the entire duration.

Multi-pass option with cut set update calculation used.

Used truncation value of 1E-12

Model Version: 0.0

3.5.2 Insights

The second section provides information about the results. The output listed in this section is based on the final risk significance. Note that the higher the risk significance, the more information that is provided.

II. Insights

> The affected components had only a minor impact on the accident sequences. However, further evaluation for LERF and external events for SDP Phase 2 analysis may be necessary since the increase in the CDF is greater than or equal to 1E-7/yr.
>
> Since the annualized CDF increase is greater than 1E-7/year SDP recovery action credit should be considered if all the recovery action credit questions are answered "yes."
>
> The following accident sequences were most impacted (by total increase):

Event Tree	Sequence	Failed Systems	Increase	(Factor Increase)
LOSP	3	ECS, CCS	5.4E-7	(1.1)

> The following components contribute the most to the delta CDF:

Components	Percent Contribution (FV)	RIR
Diesel Generator B Fails to start	32.0%	16.5
Diesel Generator A Fails to run	30.0%	25.3
Diesel Generator B Fails to run	19.0%	16.7
CCF OF EPS DGNs TO START	19.0%	707.1

> The following operator actions contribute the most to the delta CDF:

Components	Percent Contribution (FV)	RIR
ECS-CKV-CF-ALL-ABCD : (uncategorized event)	< 0.1%	707.1
ECS-MDP-CF-FR-AB : (uncategorized event)	0.3%	707.1

ECS-MDP-CF-FS-AB : (uncategorized event)	9.5%	707.1
ECS-MOV-CF-ALL-ABCD : (uncategorized event)	1.1%	707.1
ECS Suction MOV Normally closed, fail in closed position	0.9%	707.1
CCF OF EPS DGNs TO RUN	15.0%	707.1
CCF OF EPS DGNs TO START	19.0%	707.1
RWST Loss of function	< 0.1%	707.1

The following operator actions contribute the most (by Fussell-Vesely) to the delta CDF :

Operator Actions	Percent Contribution (FV)	RIR
EPS Operator Recovery Fails to recover	10.0%	1.4

The following operator actions contribute the most (by Risk Increase Ratio) to the delta CDF :

Operator Actions	Percent Contribution (FV)	RIR
EPS Operator Recovery Fails to recover	10.0%	1.4

3.5.3 Figures

The third section provides a variety of graphs representing the evaluation.

Figure III-A

The first figure provides a risk profile of the event.
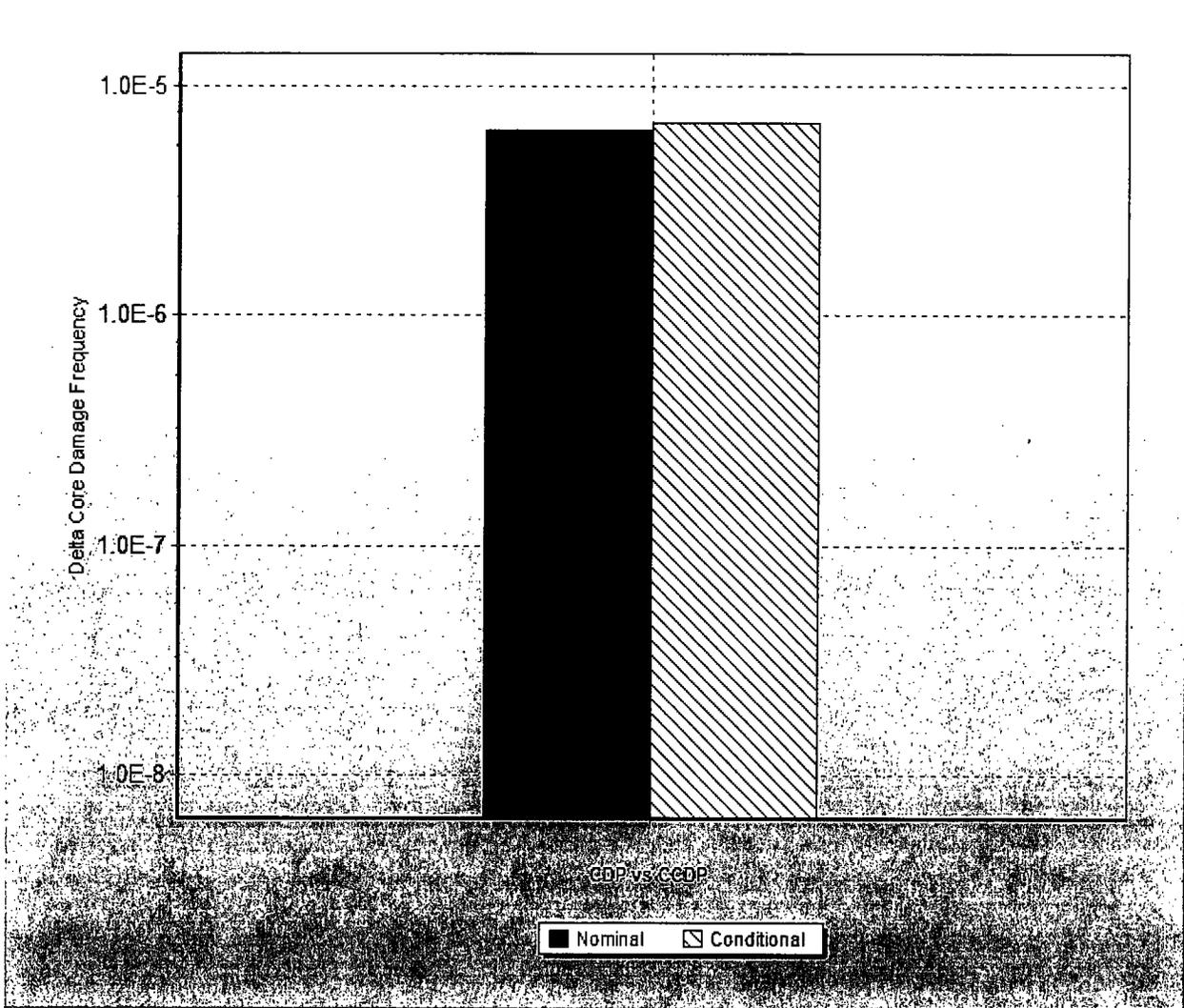
Figure III-B

The second figure provides a pie chart showing the percent contribution to the delta CDF given the condition.
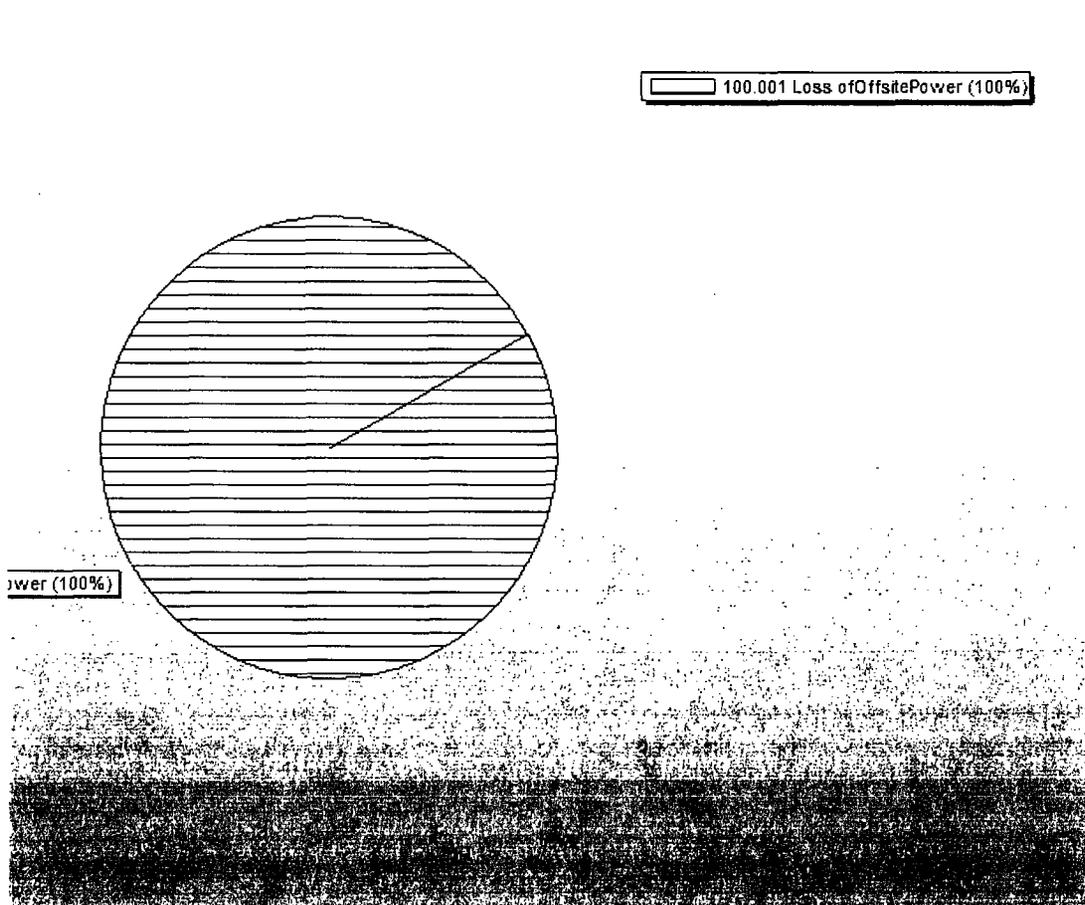
Note that the DEMO project only has a single initiating event (Loss of Offsite Power).

Figure III-C

The third figure shows the relative risk change graphed by the initiating events given the condition.
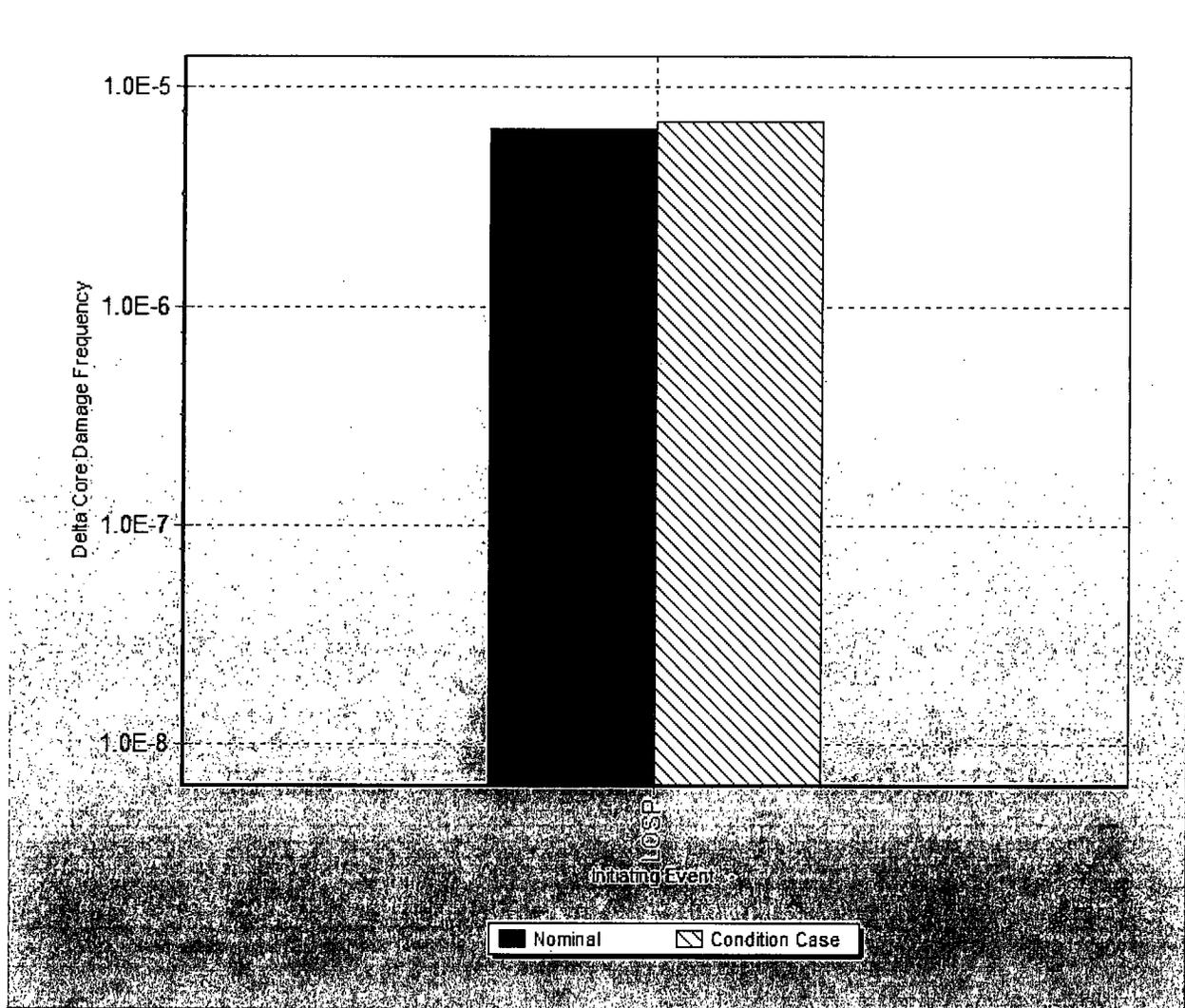
Figure III-D

The fourth figure shows the change in delta CDF as function of duration.
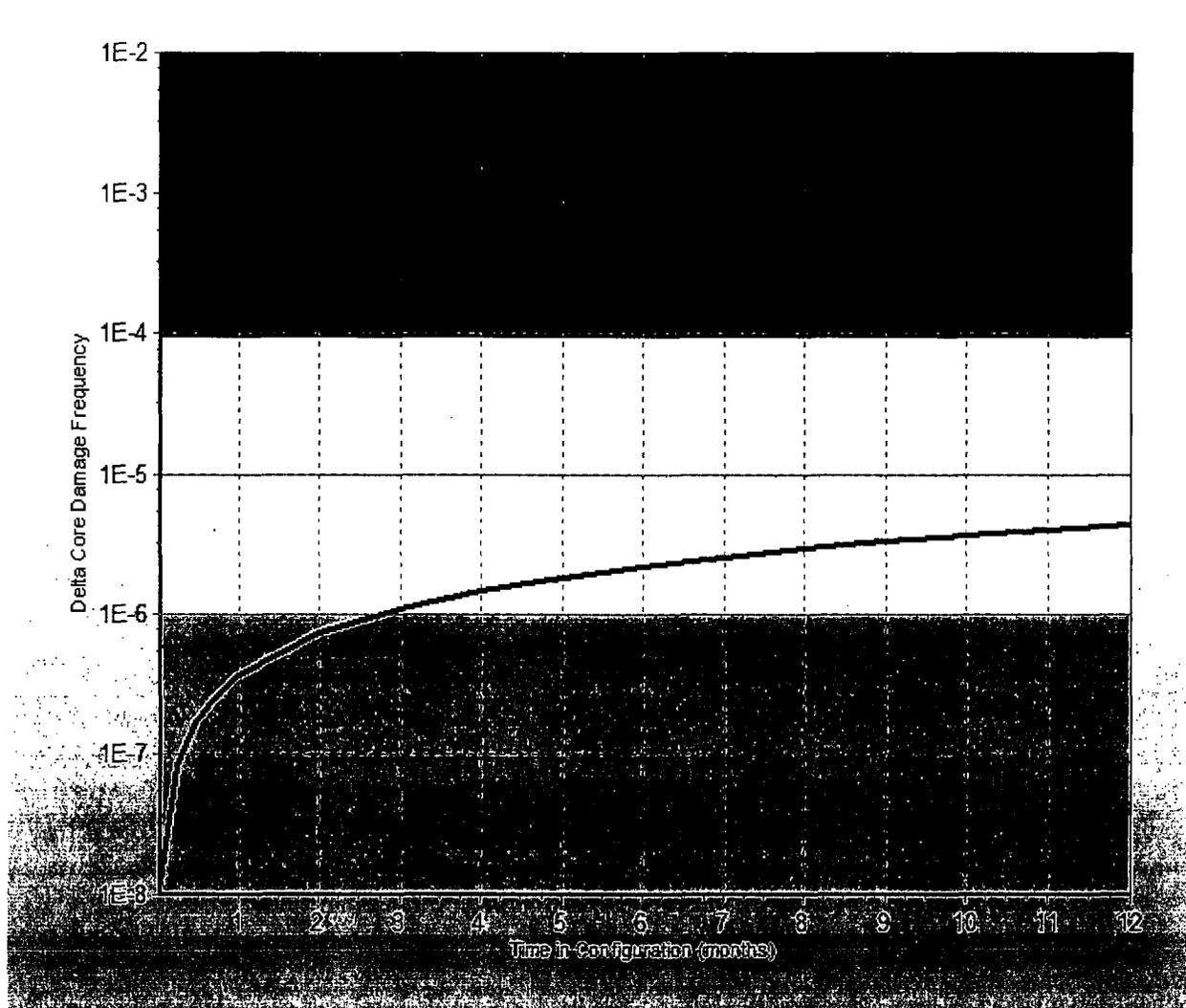
3.5.4 Notes

The fourth section provides the output of the notes the analyst typed into the analysis. By reporting the notes, all of the information is documented and kept together.

3.5.5 SPAR Model Issues

Each SPAR model comes with a disclaimer discussing implications of using the model. Included in the disclaimer are points of contacts related to the models and the SDP software.

3.6 Reports in the SDP Workspace

On the main reporting window, the report itself may be printed via the "Report Options" located in the lower right corner. Select an option and then click the "Go" button.

┌─Report Options──────────────────────────────┐
│ ┌──────────────────────────────┬───┐ ┌────┐ │
│ │ Print Report...   │ ⌄ │ │ Go │ │
│ └──────────────────────────────┴───┘ └────┘ │
└───┘
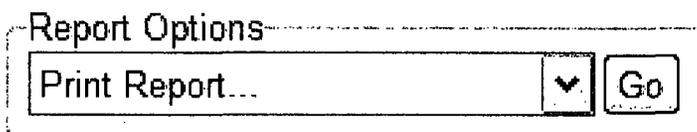
Additional report options include looking at "advanced" reports for different levels of detail (cut sets up to 90%, 99%, or 99.9% of the total results.). The advanced reports contain additional details for the analysis results (see Figure 21).

Significance Determination Process Advanced Report (90.0%)

May 22, 2010 12:39 PM

Demonstration Sample Family

AFW Train A MDP failed

I. Assessment Summary

Duration: 45 days	**Project:**	Demonstration Sample Family	
CCDP: 7.0E-6	**Model Version:**	0.0	
CDP: 6.4E-6	**Model Date:**	--/--/----	
Increase: 5.4E-7 /year	**Saphire Version:**	Version 8.0.7.1	
Color: Green			

II. Changed Basic Events

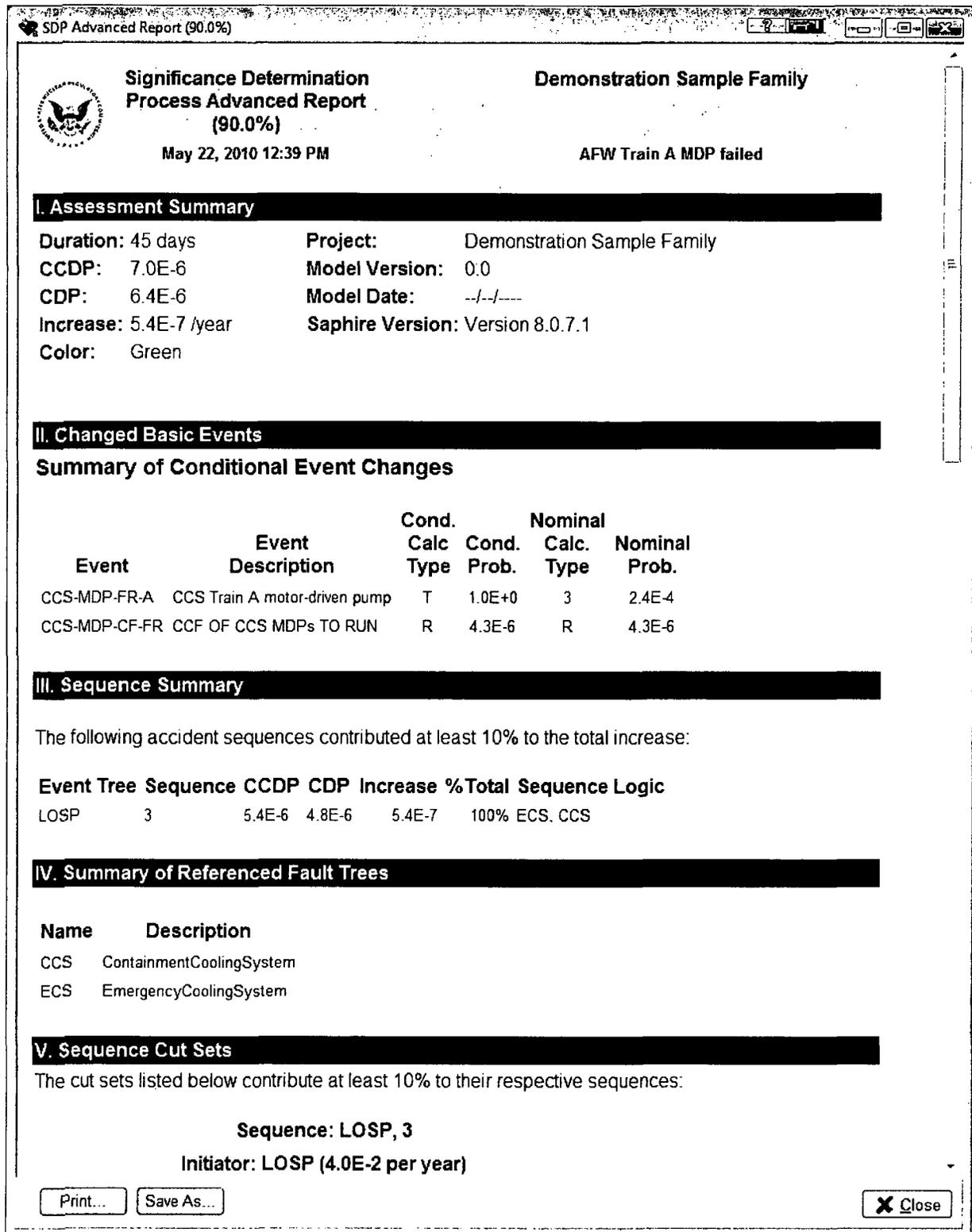### Summary of Conditional Event Changes

Event	Event Description	Cond. Calc Type	Cond. Prob.	Nominal Calc. Type	Nominal Prob.
CCS-MDP-FR-A	CCS Train A motor-driven pump	T	1.0E+0	3	2.4E-4
CCS-MDP-CF-FR	CCF OF CCS MDPs TO RUN	R	4.3E-6	R	4.3E-6

III. Sequence Summary

The following accident sequences contributed at least 10% to the total increase:

Event Tree	Sequence	CCDP	CDP	Increase	%Total	Sequence Logic
LOSP	3	5.4E-6	4.8E-6	5.4E-7	100%	ECS, CCS

IV. Summary of Referenced Fault Trees

Name	Description
CCS	ContainmentCoolingSystem
ECS	EmergencyCoolingSystem

V. Sequence Cut Sets

The cut sets listed below contribute at least 10% to their respective sequences:

Sequence: LOSP, 3

Initiator: LOSP (4.0E-2 per year)

Print... | Save As... | ✗ Close

Figure 21. Advanced 90% SDP report example.

4. THE GENERAL ANALYSIS WORKSPACE

4.1 Performing Analysis

The General Analysis user interface allows for a generic analysis option. This option provides the user the flexibility to set up an analysis that is saved for future analyses and modifications. To start this process, the user selects **General Analysis → New Analysis** from the Workspaces menu option.

```
✦ Workspaces                                        ⟨⟨
 ⊞ SDP (Significance Determination Process)
 ⊞ ECA (Events and Conditions Assessment)
 ⊟ General Analysis
      New Analysis...
```
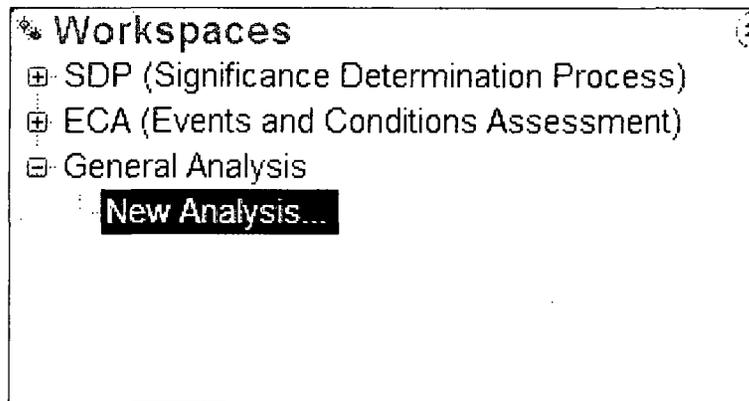
Figure 22. General Analysis workspace option

This option requires a double click and then SAPHIRE copies all of the information from the project into a new workspace. By making this copy, any event tree/fault tree modifications will only be saved for this particular analysis and the original models will not be affected. SAPHIRE Version 8 then loads up a new analysis screen which allows the user to select what parts of the model will be affected by the analysis by checking the applicable boxes.
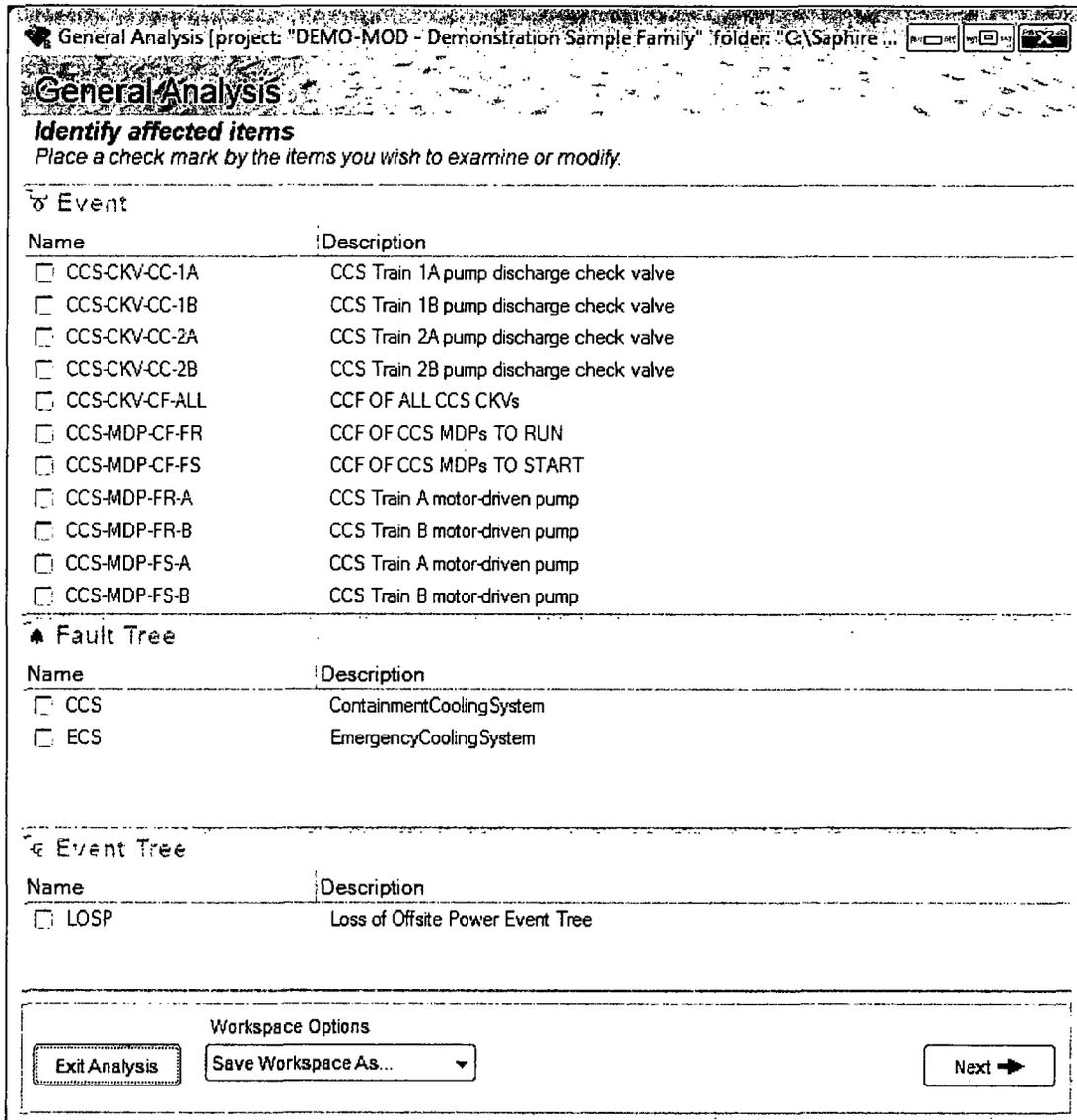
Figure 23. General Analysis start screen

The basic events, fault trees and event trees are checked in order to tell SAPHIRE Version 8 that these parts of the project are going to be affected for this particular analysis. Thus, unlike the SDP and ECA interfaces, the GA interface allows solving specific portions of the model. Once the parts of the model are checked, then the **Next** button is selected.
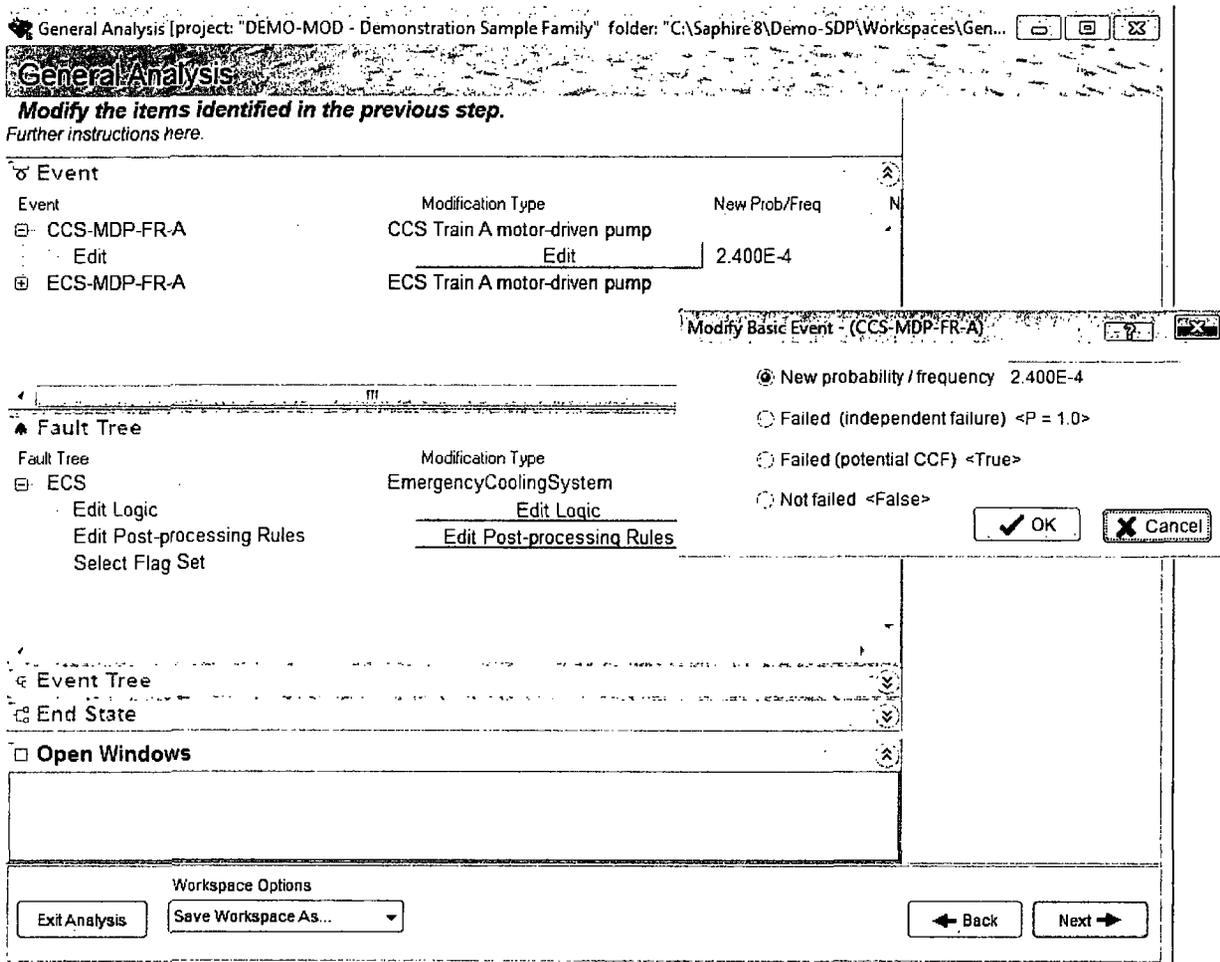
Figure 24. General Analysis modification screen

The checked fault tree(s) can now be edited. The fault tree logic can be modified or the recovery rules for this specific analysis. Again, the advantage of this analysis process is the logic will only be affected for this specific workspace – the logic in the original model is left untouched.

After making the modifications, continue on to the next screen. The last option is the **Select Solve Options**. The solving methods available are:

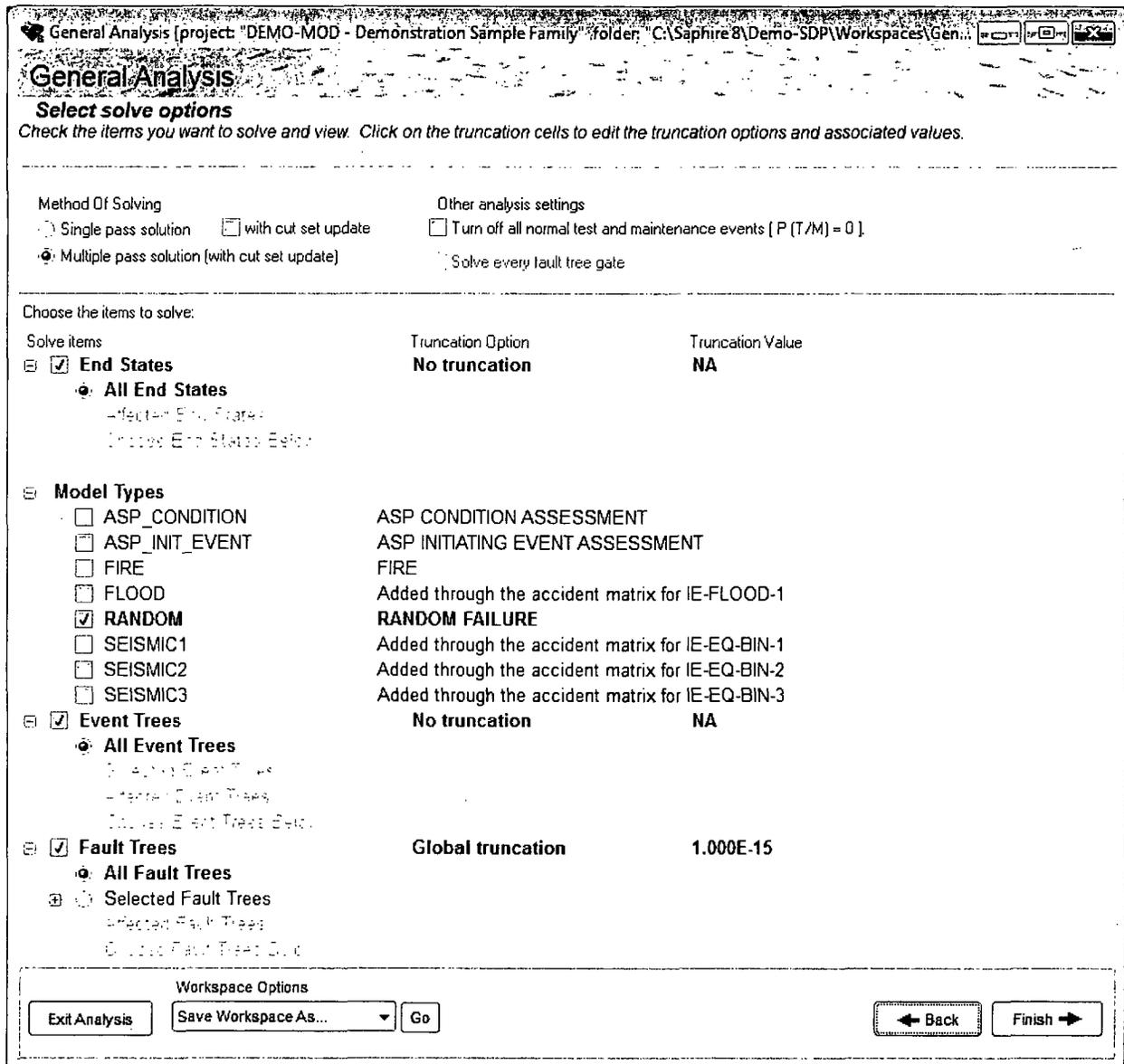- Singe pass solution
- Multiple pass solution

Figure 25. General Analysis Solve options screen

This option allows the user the flexibility of what event trees, fault trees, end states, and model types to be analyzed. The individual event trees or fault trees can be selected or all event trees and fault trees can be selected. The option to turn off test and maintenance basic events is also provided. Once the selections are made, click the **Finish** button.

SAPHIRE will show a prompt expressing that the following analysis could take some time to complete, and allows the analyst to decide to perform the analysis (which is a complete re-solve of all logic models). Clicking Cancel will just show existing results (if available). Once the analysis is complete, a View Results screen is displayed. This screen is used to provide the final output result for the event trees, fault trees, and end states.
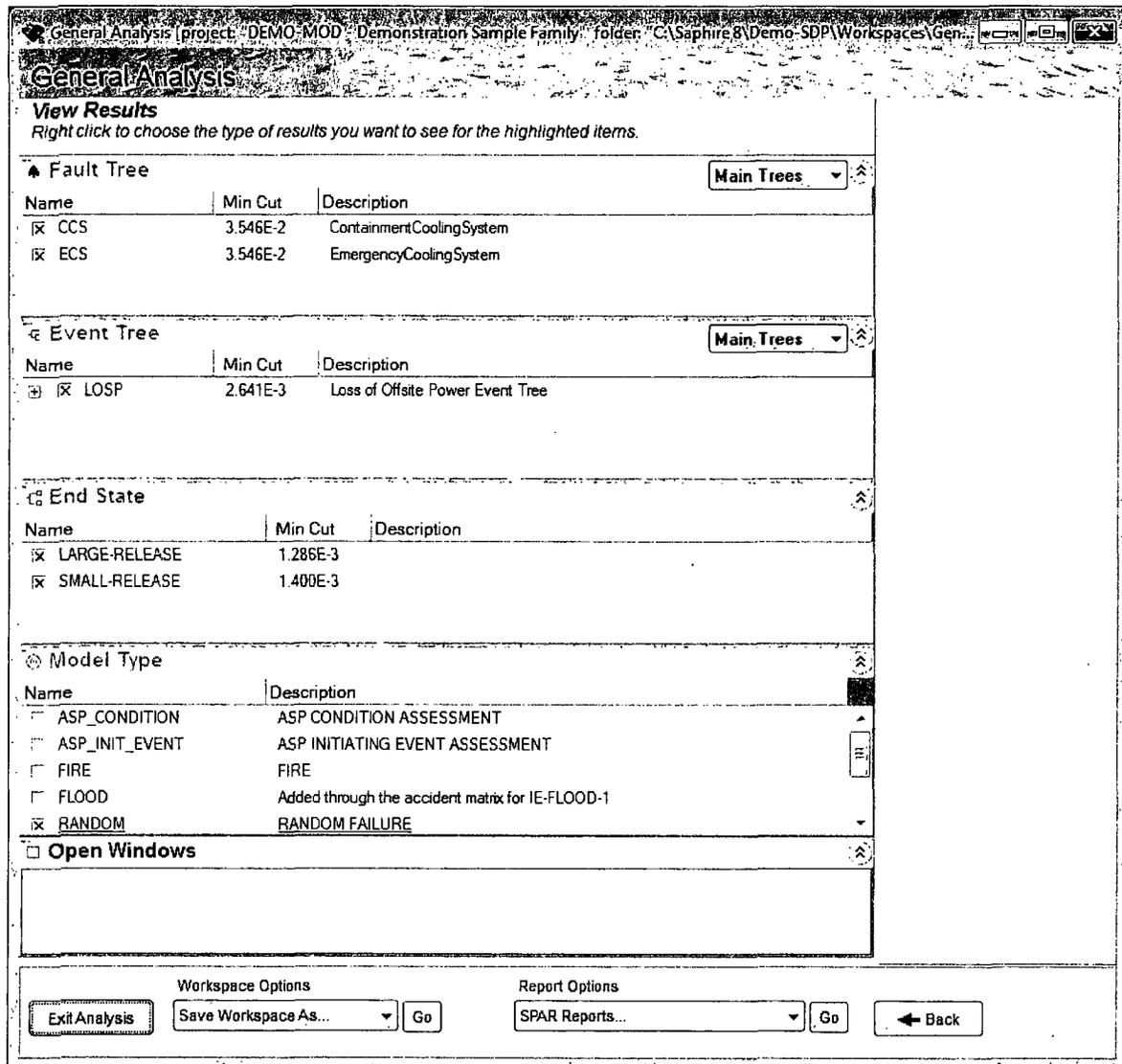
Figure 26. General Analysis results screen

The overall results for the fault trees and the event tree analysis are shown in the column labeled "Min Cut". However, each object can be further queried for additional information. For example, with the LOSP event tree highlighted, click the right mouse button to bring up the menu options show at right.

When clicking the **View Summary Results**, the overall summary for the LOSP event tree will appear in the right field of the window.

57
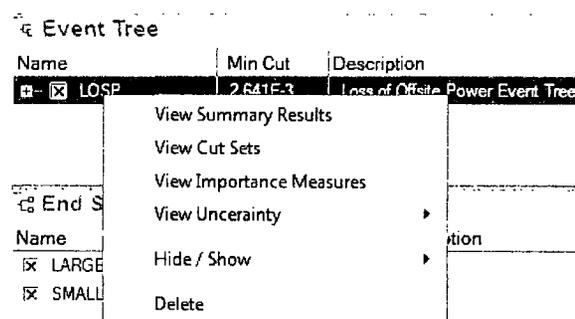
The GA figures of merit differ from the SDP and the ECA figures of merit in that no "delta" between the original and the new cases are calculated. This is because: 1) in the GA workspace changes to the model logic are permitted, thus, a delta could represent differences other than basic event unreliability modeling changes, and 2) the originally loaded model database in a workspace is not saved after modifications are made to it in the workspace, so a delta calculation involving logic changes cannot be performed without adding this capability to SAPHIRE.

4.2   General Analysis Workspace Reports

A large variety of reports are available in the GA Workspace, including:

SPAR Reports

> Event Tree Dominant Results
>
> Dominant Sequence Results
>
> Event Tree CDF by Category
>
> Nominal Results by Initiator
>
> Dominant EE Sequence Results
>
> Component Importance
>
> Operator Action Importance
>
> Common Cause Failure Importance
>
> Nominal Results by Initiator

General Insights Reports

> Event Tree Dominant Results
>
> Dominant Sequence Results
>
> Component Importance
>
> Common Cause Failure Importance
>
> Nominal Results by Initiator

Project Reports

> Statistics

Attributes

End State Partition Rules

Fault Tree Recovery Rules

Event Tree Recovery Rules

Uncertainty

Change Sets

Flag Sets

Custom Reports

Fault Tree Reports

Fault Tree Listing (with and without flag sets)

Fault Tree Logic (normal, expanded, and modified)

Cut Sets

Detailed Cut Sets

Post-processing Rules

Uncertainty

Importance Measures

Component Importance

Operator Action Importance

Fault Tree Graphics

Custom Reports

Event Tree Reports

Event Tree Listing

Cut Sets (by Event Tree)

Cut Sets (by Sequence)

Detailed Cut Sets (by Event Tree)

Detailed Cut Sets (by Sequence)

Event Tree Sequence Logic

Linkage Rules

Partition Rules

Post-Processing Rules

Event Tree Dominant Results

Dominant Sequence Results

Event Tree CDF by Category

Nominal Results by Initiator

Dominant EE Sequence Results

Uncertainty

Importance Measures

Component Importance

Operator Action Importance

Event Tree Graphics

Custom Reports

End State Reports

End State Listing

Cut Sets

Detailed Cut Sets

Event Tree Dominant Results

Dominant Sequence Results

Uncertainty

Importance Measures

Component Importance

Operator Action Importance

Custom Reports

5. REFERENCES

Atwood, C., et al, 1998, *Evaluation of Loss of Offsite Power Events at Nuclear Power Plants: 1980-1996*, NUREG/CR-5496.

Rasmuson, D. M. and D. L. Kelly, 2008, "Common-cause failure analysis in event assessment," *Proceedings of the Institution of Mechanical Engineers*, Vol. 222, Part O: Journal of Risk and Reliability, DOI: 10.1243/1748006XJRR121.

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

NRC FORM 335 (12-2010) NRCMD 3.7	U.S. NUCLEAR REGULATORY COMMISSION	1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
	BIBLIOGRAPHIC DATA SHEET *(See instructions on the reverse)*	NUREG/CR-7039, Vol. 5 INL/EXT-09-17013

2. TITLE AND SUBTITLE	3. DATE REPORT PUBLISHED	
Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8	MONTH	YEAR
	June	2011
Volume 5: Workspaces	4. FIN OR GRANT NUMBER	
	N6423	

5. AUTHOR(S)	6. TYPE OF REPORT
C. L. Smith, J. K. Knudsen, D. O'Neal	Technical
	7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Idaho National Laboratory
Battelle Energy Alliance
P.O. Box 1625
Idaho Falls, ID 83415-3850

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

10. SUPPLEMENTARY NOTES

D. O'Neal, NRC Project Manager

11. ABSTRACT *(200 words or less)*

The SAPHIRE Version 8 is a software application developed for performing a complete probabilistic risk assessment using a personal computer running the Microsoft Windows ™ operating system. In older versions of SAPHIRE, the model creation and analysis functions were intermingled. However, in SAPHIRE 8, the act of creating a model has been separated from the analysis of that model in order to improve the quality of both the model (e.g., by avoiding inadvertent changes) and the analysis. Consequently, in SAPHIRE 8, the analysis of models is performed by using what are called Workspaces. Currently, there are Workspaces for three types of analyses: (1) the NRC's Accident Sequence Precursor program, where the workspace is called "Events and Condition Assessment (ECA);" (2) the NRC's Significance Determination Process (SDP); and (3) the General Analysis (GA) workspace.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*	13. AVAILABILITY STATEMENT
SAPHIRE 8, software, reliability, risk, safety, PRA, workspaces, event assessment	unlimited
	14. SECURITY CLASSIFICATION
	(This Page) unclassified
	(This Report) unclassified
	15. NUMBER OF PAGES
	16. PRICE

NRC FORM 335 (12-2010)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS