United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-6952
Vol. 5
INL/EXT-05-00682

Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 5 GEM Manual

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:
Address: U.S. Nuclear Regulatory Commission
Office of Administration
Mail, Distribution and Messenger Team
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—
The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—
American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-6952
Vol. 5
INL/EXT-05-00682

Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 5 GEM Manual

Manuscript Completed: October 2007
Date Published: September 2008

Prepared by
C.L. Smith, J. Schroeder, S.T. Beck

Idaho National Laboratory
Battelle Energy Alliance
Idaho Falls, ID 83415

D. O'Neal, NRC Project Manager

NRC Job Code N6203

Office of Nuclear Regulatory Research

PREVIOUS REPORTS

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) is a software application developed for performing a complete probabilistic risk assessment (PRA) using a personal computer running the Microsoft Windows™ operating system. SAPHIRE is primarily funded by the U.S. Nuclear Regulatory Commission (NRC) and developed by the Idaho National Laboratory (INL). The INL's primary role in this project is that of software developer and tester. Using the SAPHIRE analysis engine and relational database is a complementary program called GEM. GEM has been designed to simplify using existing PRA analysis for activities such as the NRC's Accident Sequence Precursor program. In this report, the theoretical framework behind GEM-type calculations are discussed in addition to providing guidance and examples for performing evaluations when using the GEM software. As part of this analysis framework, the two types of GEM analysis are outlined, specifically initiating event (where an initiator occurs) and condition (where a component is failed for some length of time) assessments.

FOREWORD

The U.S. Nuclear Regulatory Commission has developed the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software 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.

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 can also 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 it includes 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 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. The versions currently in use (6 and 7) run in the Microsoft Windows® environment. A user-friendly interface, Graphical Evaluation Module (GEM), streamlines and automates selected SAPHIRE inputs and processes for performing event assessments.

SAPHIRE has also evolved with users' needs, and Versions 6 and 7 include new features and capabilities for developing and using larger, more complex models. For example, Version 7 can solve up to 2 million sequences and includes enhancements for cut set slicing, event tree rule linkage, and reporting options.

This NUREG-series report comprises seven volumes, which address SAPHIRE/GEM Versions 6 and 7. Volume 1, "Overview/Summary," gives an overview of the functions available in SAPHIRE and presents general instructions for using the software. Volume 2, "Technical Reference," discusses the theoretical background behind the SAPHIRE functions. Volume 3, "SAPHIRE Users' Manual," provides installation instructions and a step-by-step approach to using the program's features. Volume 4, "SAPHIRE Tutorial Manual," provides an example of the overall process of constructing a PRA database. Volume 5, "GEM/GEMDATA Reference Manual," discusses the use of GEM. Volume 6, "SAPHIRE Quality Assurance (QA) Manual," discusses QA methods and tests. Lastly, Volume 7, "SAPHIRE Data Loading Manual," assists the user in entering PRA data into SAPHIRE using the built-in MAR-D ASCII-text file data transfer process.

Christiana H. Lui, Director
Division of Risk Analysis
Office of Nuclear Regulatory Research

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Incidents at facilities such as nuclear power plants occur at many different times and under a variety of conditions. To evaluate these situations, analysts perform what is known as an "event evaluation." To perform event evaluations, GEM was developed for the Nuclear Regulatory Commission (NRC) by the Idaho National Laboratory (INL). 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.

An event evaluation represents the use of a probabilistic risk assessment (PRA) model to obtain a risk measure that is conditional on the situation that existed during an incident. GEM allows analysts to perform these types of assessments for both initiating event and condition cases.

This report addressed how the technique of event assessment is performed using the GEM risk analysis tool. Specifically, four areas of interest were discussed:

- Background material related to event evaluations.
- A theoretical framework behind event evaluation calculations.
- Pragmatic considerations when performing event evaluations using GEM.
- Guidance for performing event evaluations when using the GEM software.

As part of this analysis framework, the two types of GEM analysis, specifically initiating event (where an initiator occurs) and condition (where a component is failed for some length of time) assessments are described. The calculation of an operational risk measure creates a risk profile, over time, conditional upon the component outages and plant initiating events that actually occurred during the period of interest. However, what is *not* being calculated for the nuclear power plant risk profile is the probability that severe core damage *did* happen. Instead, the risk profile evaluation 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?"

The conditionality that was estimated on measures such as conditional core damage probability (CCDP) in GEM reflects impacts on the measure of interest (i.e., core damage). Such impacts include scenarios such as condition and initiating event assessments (e.g., a component outage or the occurrence of an initiating event). Additional complications such as the potential for common-cause failures, the recovery of failed components, and the restoration from initiating events are considered as part of these impacts.

A method of calculating risk levels for plant operational events was illustrated using GEM. Two cases were considered, first a case where a plant experienced an initiating event (initiating event assessment) and second a case where a component was inoperable for a length of time (condition assessment).

For initiating event assessments, the initiating events in a model must be modified to reflect the event in question. For those initiators that *did not* occur, they are turned off while 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. For these types of events, GEM will determine the CCDP specific to the event.

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, GEM will account for the probability that an initiating event could have occurred. The initiator probabilities are necessary even if the event duration is very short. For condition assessments, GEM will determine an "event importance" by evaluating the difference in the CCDP and CDP, where the CDP is the nominal core damage probability.

The GEM software has been developed to aid in accident sequence precursor (ASP) event analysis. It is intended to simplify the use of SAPHIRE PRA databases when performing an event assessment. GEM is able to setup default analysis procedures (either initiating event assessments or condition assessment) for each of the initiating event types in the SPAR plant models and provides a powerful framework for performing event evaluations.

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
LOCA	loss-of-coolant accident
LOOP	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)

Vol. 5 GEM Manual

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).

Using SAPHIRE 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.
SARA provided the capability to access PRA data and results (descriptive facility information, failure data, event trees, fault trees, plant system model diagrams, and dominant accident sequences) stored in MAR-D. With SARA, a user could review and compare results of existing PRAs. It also provided the capability for performing limited sensitivity analyses. SARA was intended to provide easier access to PRA results to users that did not have the level of sophistication required to use IRRAS.

FEP provided common access to the suite of graphical editors. The fault tree and event tree editors were accessible through FEP as well as through IRRAS, whereas the piping and instrumentation diagram (P&ID) editor was only accessible through FEP. With these editors an analyst could construct from scratch as well as modify fault tree, event tree, and plant drawing graphical representations needed in a PRA.

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.

With the release of SAPHIRE versions 5 and 6, INL included a separate module called the Graphical Evaluation Module (GEM). GEM provides a highly specialized user interface with SAPHIRE, automating SAPHIRE process steps for evaluating operational events at commercial nuclear power plants. In particular, GEM implements many of the accident sequence precursor (ASP) program analysis methods. Using GEM, an analyst can estimate the risk associated with operational events very efficiently and expeditiously.

1.2 The Need for GEM

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, GEM was developed for the NRC by the INL. GEM contains a simplified user interface that relies on the SAPHIRE analysis engine in order to perform "what if" 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 GEM software 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 report discusses four areas of interest related to the use and understanding of the GEM software when performing event evaluations:

1. A theoretical framework behind event evaluation calculations.

2. Considerations when performing event evaluations using GEM.

3. Guidance and examples for performing event evaluations when using the GEM software.

4. Application and use of the GEMDATA module to edit GEM-specific analysis parameters such as initiating event and failed component recovery.

2. GENERAL EVENT EVALUATION FRAMEWORK

2.1 Introduction

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 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 1 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.

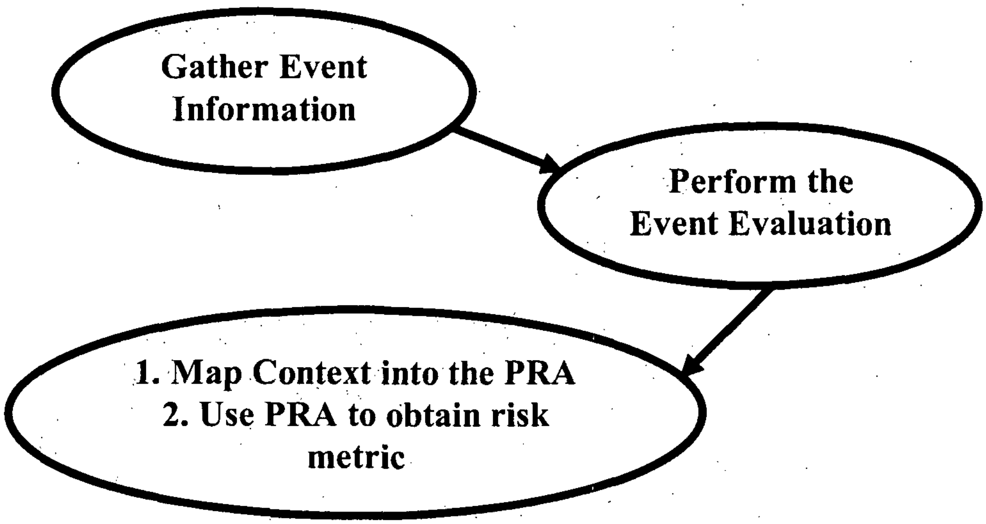

Figure 1. Event evaluation methodology.

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:

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.

2.2 Conditional Probability Calculations

Conditional probability calculations estimate the probability of a negative outcome (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:

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. 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.

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 case, the nominal (unconditional) equation for Example #1 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 Example #1 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:

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

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.

2.3 Event Importance Calculations

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

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

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.

3. THE TWO TYPES OF GEM EVENT EVALUATIONS

3.1 Initiating Event Assessments

Components or systems that are inoperable at the time the initiator occurs increase the overall risk of the event. A CDP can be calculated that is conditional upon the initiator occurring and the initial conditions of the event. Typical initiating events (in nuclear power plants) that are available for modeling purposes include:

- Trip (including loss of condenser, loss of main feedwater, and anticipated transients without scram).
- Loss of offsite power.
- Steam generator tube rupture.
- Small, medium, or large break loss-of-coolant accident (LOCA).
- Inadvertent/stuck open relief valve.
- Loss of a DC bus.
- Loss of service water.
- Loss of component cooling water.
- Interfacing-systems LOCA.
- Excessive LOCA.

For an initiating event analysis, GEM will allow the analyst to model the scenario where one of these initiating events has occurred. The CCDP that is quantified by GEM 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 $\lambda(t) \cdot \Phi(t)$ 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.

3.1.1 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 (LOOP), *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 short-term nonrecovery probability.

For initiating event assessment, the initiating events should be modified according to the flow diagram below in Figure 2.

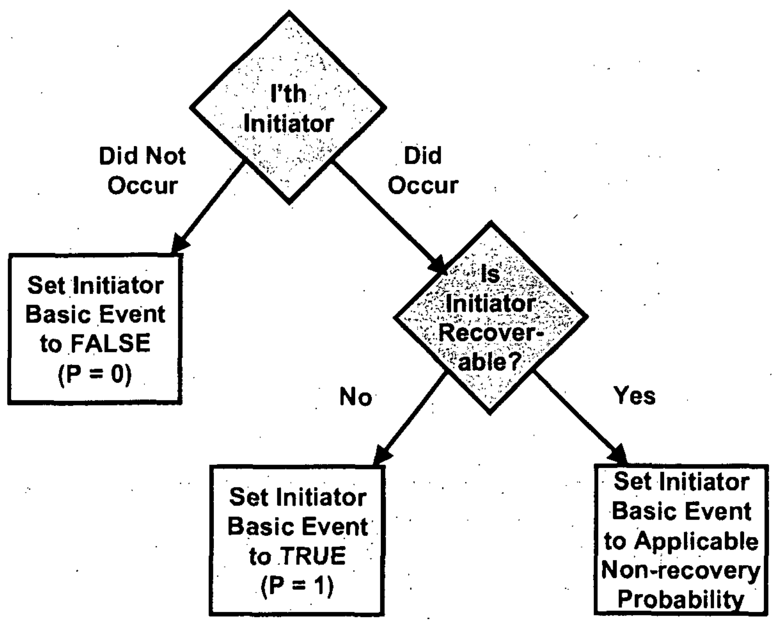

Figure 2. Modification of initiating events during an initiating event assessment.

3.1.2 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

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 Manual, Volume 2).

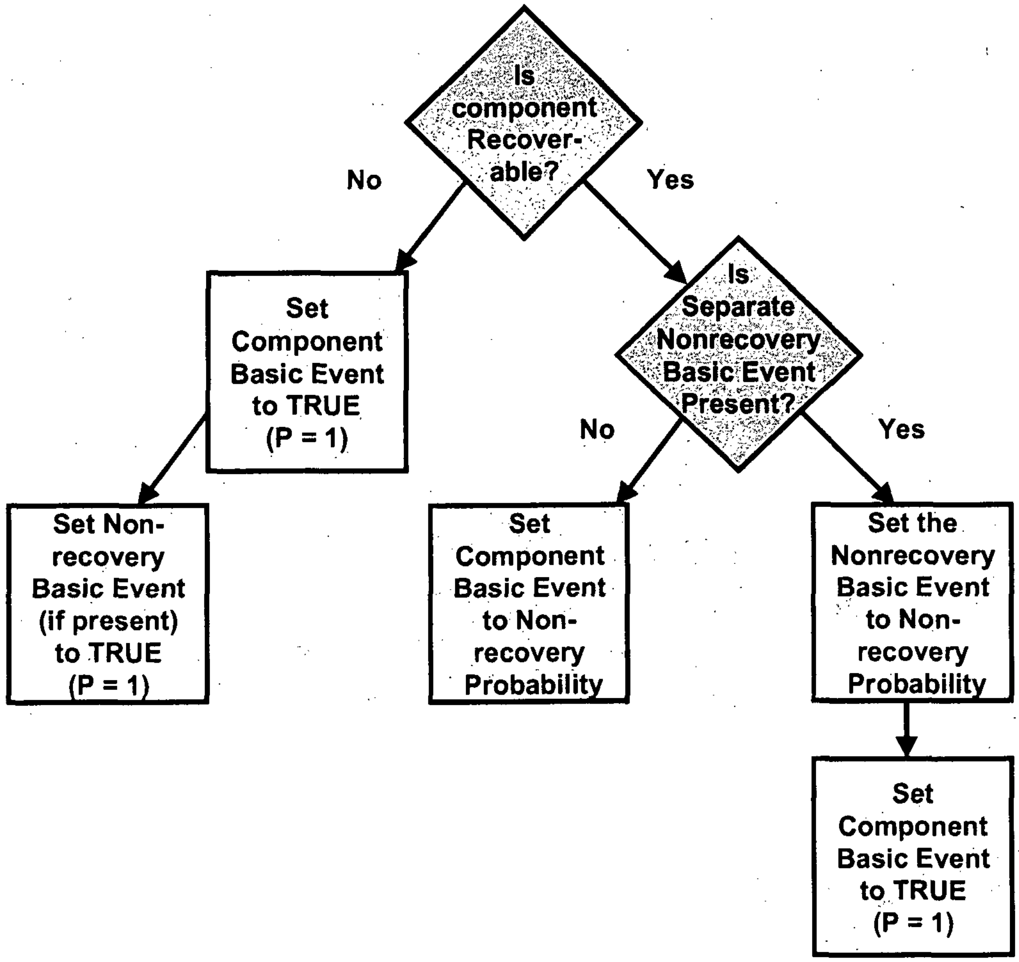

Figure 3. Modification of component nonrecovery events during an initiating event assessment.

3.1.3 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, GEM is going 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 (and is shown in Figure 4).

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

2. Calculate a new CCF probability based upon failure.

3. Modify the CCF probability in the PRA model. Note that the SPAR models in use will automatically modify the CCF since they use the SAPHIRE CCF module.

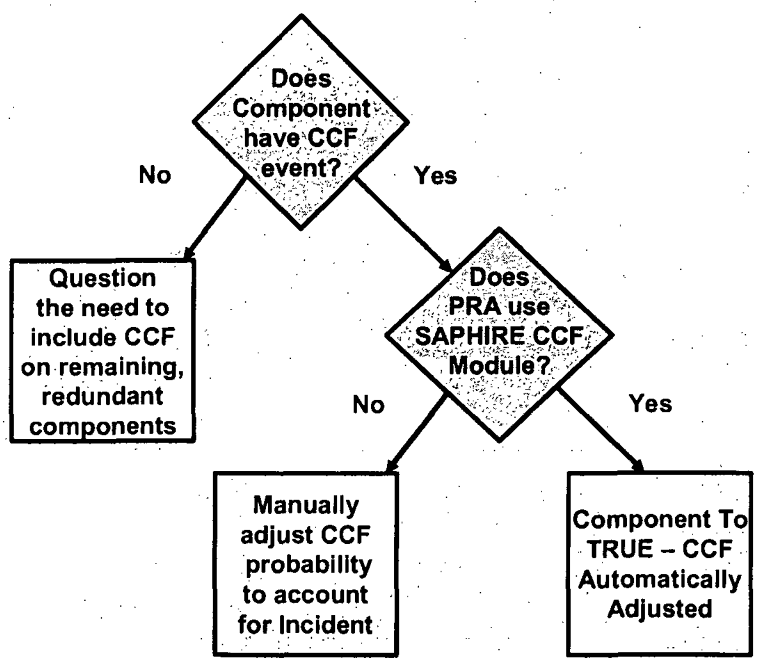

Figure 4. Modification of common cause events during an initiating event assessment.

3.1.4 Appropriate Risk Measure for Initiating Event Assessments

In GEM, 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?).

3.2 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.

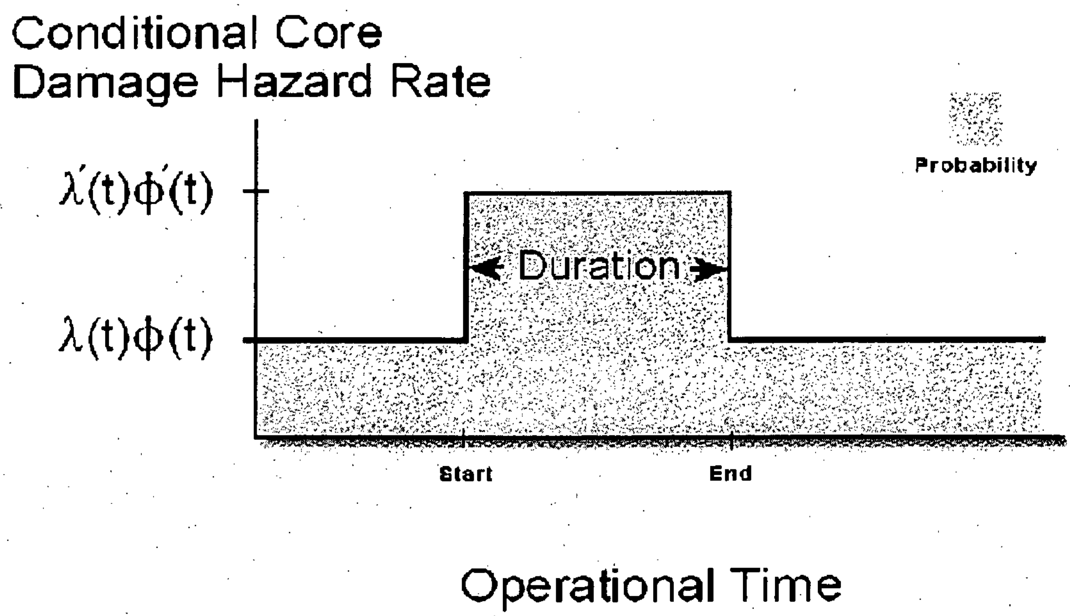

Figure 5. Example of the increase in risk during the duration of a component outage.

For component outages, GEM assumes that the risk is assumed constant over the duration of the event. This constant (the $\lambda' \Phi'$ 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.

3.2.1 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, GEM 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.

3.2.2 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 3.1.2). The treatment of common cause failures is the same as that in the initiating event assessment section (Section 3.1.3).

3.2.3 Appropriate Risk Measure for Condition Assessments

In GEM, 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, GEM 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.

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

	Assessment Type	
Item	**Initiating Event Assessment**	**Condition Assessment**
Unique Attributes	Initiating event happens (point in time)	One (or more) component is unavailable for some duration of time (t_1 -> t_2) 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,* λ_i = *i'th initiator frequency* Φ_i = *P(CD | 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	I_e = CCDP - CDP

4. OVERVIEW OF THE GEM SOFTWARE

4.1 Introduction

The GEM software has been developed to aid in accident sequence precursor (ASP) event analysis. It is intended to simplify the use of SAPHIRE PRA databases when performing an event assessment. GEM automates the analysis procedure and provides result reports in the format used in the ASP program. GEM is able to setup default analysis procedures (either initiating event assessments or condition assessment) for each of the initiating event types in the SPAR plant models. For these analyses, the primary purpose of GEM is to interface with the SAPHIRE analysis module.

GEM uses the SAPHIRE cut set generation and quantification routines to solve sequences in the SAPHIRE database. Further, GEM stores the results of sequence quantification in the project's SAPHIRE database. GEM stores the quantification result in one of the reserved analysis types in SAPHIRE:

- ASP_CONDITION for the condition assessments
- ASP_INIT_EVENT for the initiating event assessments

While the analysis results are viewable in GEM, these results can also be reviewed and manipulated from within SAPHIRE. In addition, GEM uses its own database to store information about each model – this database is known as GEMDATA. While the use of GEM DATA has been superseded by the circa 2005 SPAR models, information on GEMDATA for older models may be found in Appendix A.

4.2 Using GEM for Initiating Event Assessment

This section demonstrates how GEM was used to evaluate events that involve initiators. As an example of initiating event assessment, the evaluation of a loss of offsite power (LOOP) event at a nuclear power plant follows, as well as:

- The event to be modeled,
- The preliminary steps to an analysis of the event,
- A walk through of the use of GEM to evaluate the event

GEM was used to determine the probability of a core damage event as a result of a LOOP event. GEM's built-in analysis procedure handled most of the details for the analysis. To model the scenario, the basic events in the model were modified to map the event into the model. Then the appropriate changes were entered through the GEM Initiating Event Analysis interface.

The hypothetical event is as follows. A brush 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 busses were supplied by the diesels for 24 hours. Two days after the LOOP, the low-pressure injection (LPI) 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. This event was considered to be a **grid-related** loss-of-offsite power initiating event.

The failed LPI pump was accounted for separately. For this example, the obstruction was the assumed reason the pump failed to start. If a pump could not start, it also could not run (assuming no recovery from the initial failure). After reviewing the PRA model, the recirculation line failure was modeled by setting basic events

LPI-MDP-FR-P015 to TRUE
LPI-MDP-FS-P015 to TRUE

The GEM software was started and the data was entered using the following procedures.

GEM was started by clicking on the GEM icon in the "SAPHIRE for Windows" program group under the "Windows Start" button (see Figure 6). In addition to using the "Windows Start" menu, the GEM or SAPHIRE icons may be put directly on the desktop as a shortcut.

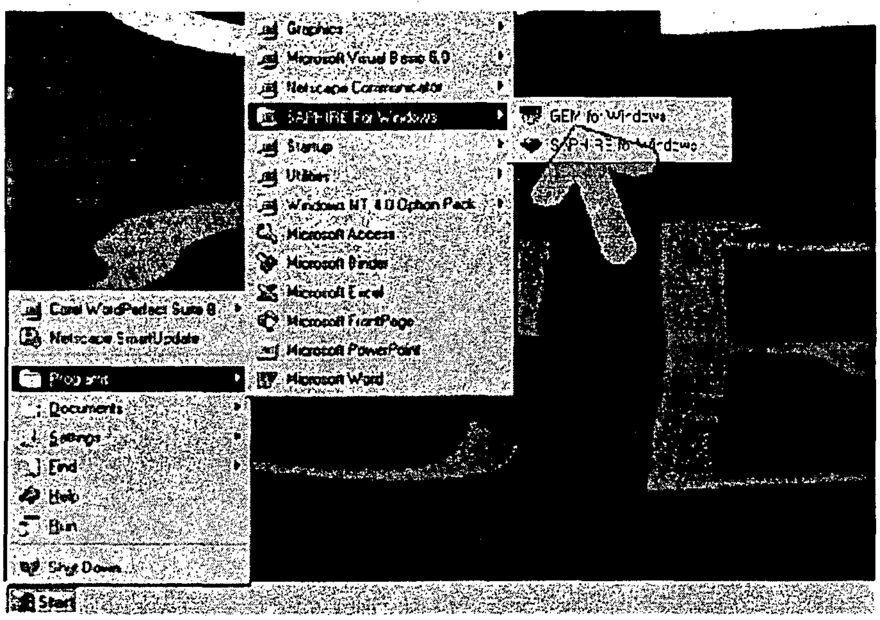

Figure 6. Starting GEM in Windows.

Next, the "Initiating Event Assessment" option was selected from the main Gem Menu. A new assessment was made by clicking the right mouse button and selecting the "New" option. The assessment was given a name (up to 24 characters) and a description in order to make a record in the SAPHIRE database that will hold the assessment. Finally, <Enter> was pressed or the Save button was clicked in order to continue.

After GEM displayed the Initiating Events screen (see Figure 7), the assessment that most closely matched was chosen by double clicking on it.

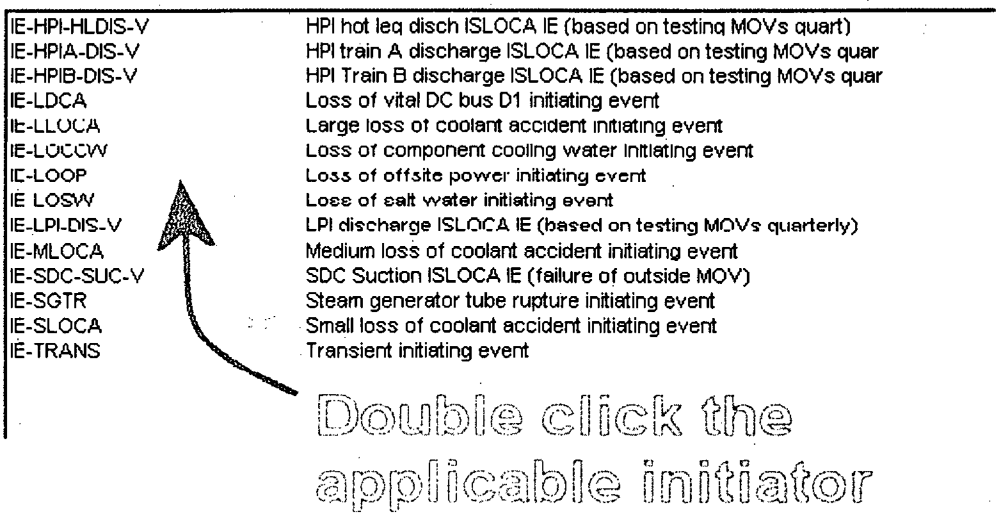

Figure 7. The GEM initiating event list dialog.

For example, if the LOOP initiator was chosen, the cursor would be moved to the IE-LOOP line and the left mouse button would be double clicked. For LOOP-related initiating event assessments, GEM has been designed to further query the user to select the type of initiating events (additional information on LOOP treatment is provided in Appendix B). The list of sub-type LOOPs varies, but a typical list will be (Atwood, 1998):

- Grid related
- Plant centered
- Switchyard
- Weather related

The LOOP in the example was "grid related," so "GRID RELATED" was selected and <Enter> was pressed. For initiating event assessments, only one initiator was selected. Continuing with the assessment, either the assessment record was double clicked or the record was highlighted and the "Select" button was clicked. On the "IE Assessment Events" screen (Figure 8) basic event probabilities were added or modified (if necessary) before being saved with the analysis record.

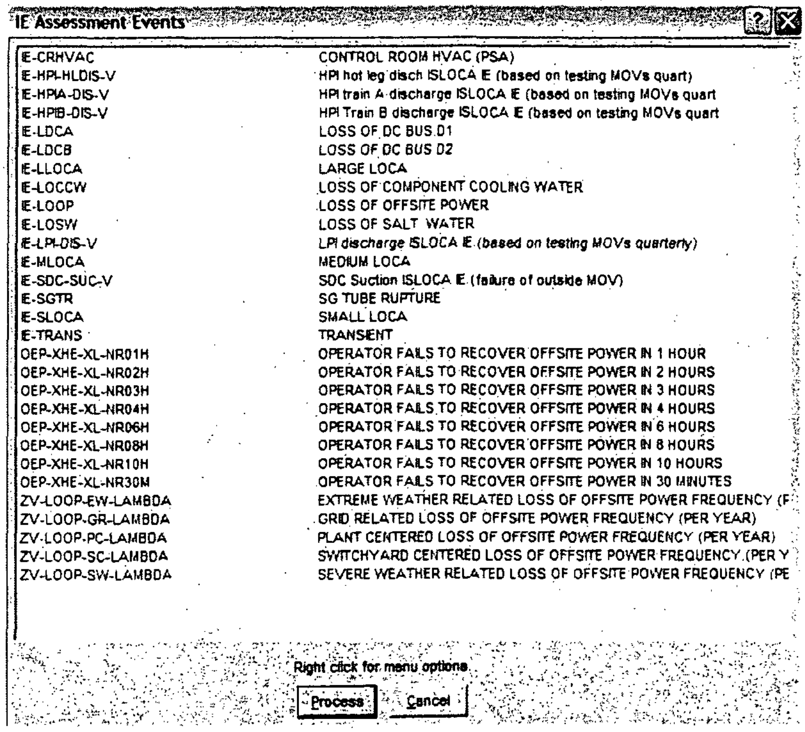

Figure 8. GEM initiating event assessment event screen.

Initially, GEM added a few events to the list (20 basic events as shown in Figure 8) indicating that these events were modified from their nominal values. For example, the non-LOOP initiators were all set to FALSE (a probability of zero) since these initiators did not occur. At this point, other events were added to the list, specifically the events related to the LPI pump failure, by clicking the right mouse button and then, selecting the "Add" option.

The event LPI-MDP-FR-P015 was selected by scrolling the list or by simply typing in the first few characters of the event name (i.e., L, P, I, -, M, etc.). Once the event was found, it was highlighted and chosen by double clicking the event (or right click and select Add), which began the probability change process. On the next dialog, the basic event LPI-MDP-FR-P015 was set to TRUE, indicating failure, and the OK button was clicked.

Once the OK button was clicked, GEM added the LPI event to the change list. The previous steps were repeated to set LPI-MDP-FS-P015 to TRUE also. At this point, the steps to setting up the analysis were finished and the Process button was clicked.

GEM processed the analysis and, when finished, displayed the "Event Assessment" screen (see Figure 9). The total CCDP for the event was displayed at the bottom of the screen (8.8E-5). The accident sequences contributing to the CCDP was displayed and sorted from highest (4.5E-5) to lowest CCDP (1.5E-12).

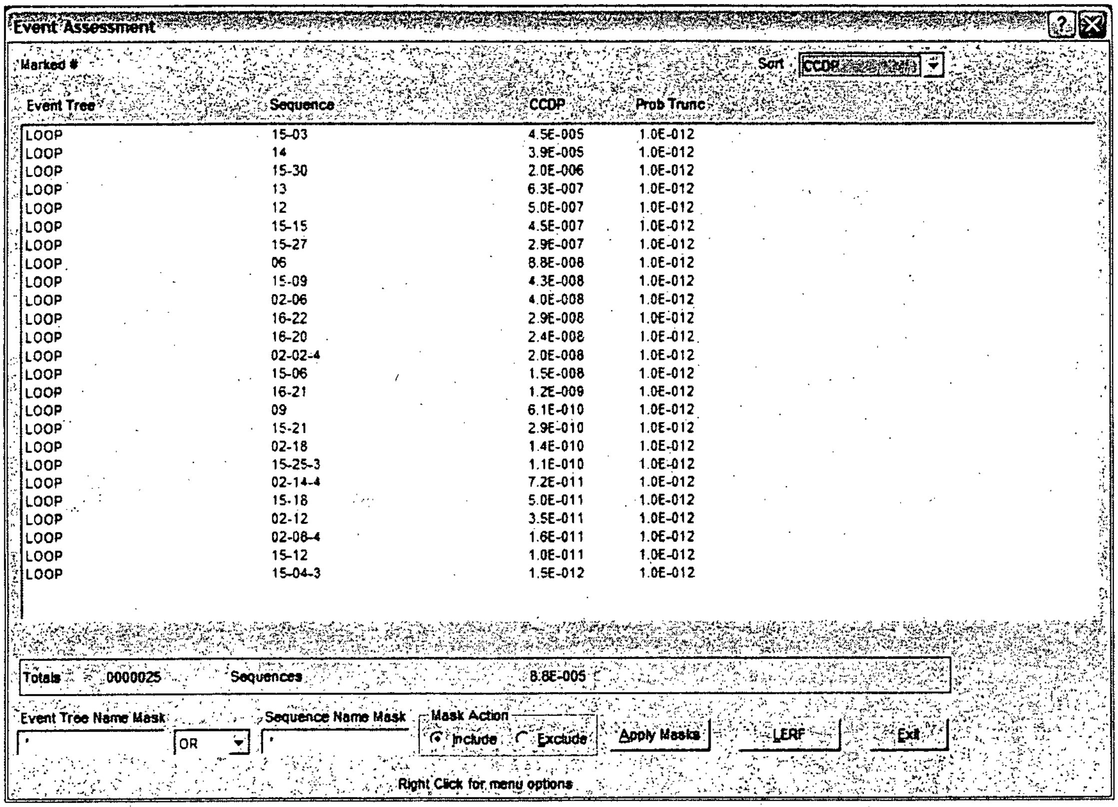

Figure 9. The GEM event assessment screen display for initiating event assessments.

At this point, by clicking the right mouse button 🖰 over the dialog window, other options were available. For example, by highlighting all the sequences, right clicking, and then selecting one of the Importance options the conditional importance measures (e.g., Fussell-Vesely, risk increase ratio) appeared. The "Event Assessment" screen also allowed a review of the results and printed pre-formatted reports. By clicking the right mouse button 🖰 over the dialog box then selecting the "Report" option, GEM displayed the Report Options screen.

Several report options were available (see Figure 10). The report was viewed on screen through the default option and by pressing the Ok button. To print to the default printer, the option was changed to "Print (Default Printer)," which can change the "report truncation" values from 100.0 (%) to 90 or 95 in order to minimize the volume of paper needed for the report.

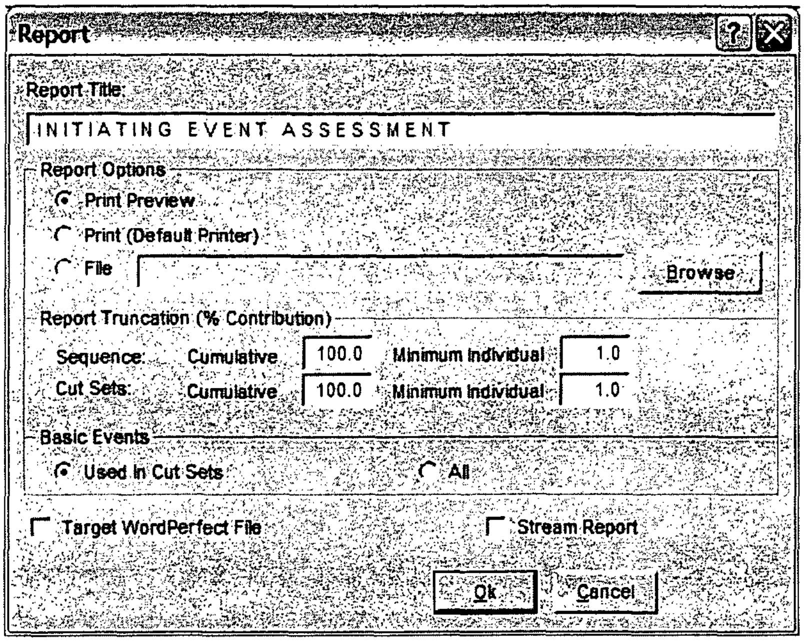

Figure 10. Report options available in GEM.

A plain text file can be made by changing the option to File and entering a valid file path and name. To make a WordPerfect file, the option was changed to File and the file name was filled in. Then, the Target WordPerfect File option was checked.

The Stream Report option, when checked, output the report as a single, continuous results list. Otherwise, the report contained breaks for page information.

4.3 Using GEM for Condition Assessments

To use GEM to evaluate events that involve component degraded conditions – these are defined as operational occurrences (both real and hypothetical) that can not be modeled as initiating events. Instead, a condition exists that degrades the ability of the plant to respond to upsets over a period of time.

As an example of a condition assessment, the evaluation of a diesel generator unavailability event at a nuclear power plant follows. Topics to be covered will include:

- A discussion of the preliminary steps to analyze an event.
- A demonstration of GEM 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. Then this CCDP will be compared with the CDP for the same period had the diesel not been known to have been failed (i.e., in its nominal state). The difference in these two probabilities is a quantity known as the event importance.

In the hypothetical example, a diesel generator failed a periodic functional test. When repair crews investigated, they found that the diesel generator in division 2B of ac power (the number 3 diesel) had a plugged fuel filter. It may have been non-functional since the last operational check. Some other relevant facts are:

- Investigation showed that the machine had only been non-functional for 100 hours.
- The other diesel (number 2 in division 2A of ac power) was also checked, but the plugging was found only in Diesel Generator 3.
- 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.

First, the specific model modifications were determined. The event description stated that Diesel Generator 3 was failed for 100 hours, and that the failure appeared to be a potential "common cause." After reviewing the PRA, this event was mapped into the model by setting the basic event EPS-DGN-FS-DG3 to TRUE. In addition, EPS-DGN-FR-DG3 was set to TRUE (since the diesel can not run if it does not start).

Second, to enter the data, GEM was started by clicking on the GEM icon in the SAPHIRE for Windows program group.

From the GEM main menu, the "Condition Assessment" option was selected. A new assessment was made by clicking the right mouse button 🖱 and selecting the "New" option. The analysis was provided with a name (up to 24 characters) and description, then <Enter> was pressed or the Save button was clicked.

GEM displayed the Condition Assessments screen as shown in Figure 11 (this dialog listed all of the condition assessments as they were made).

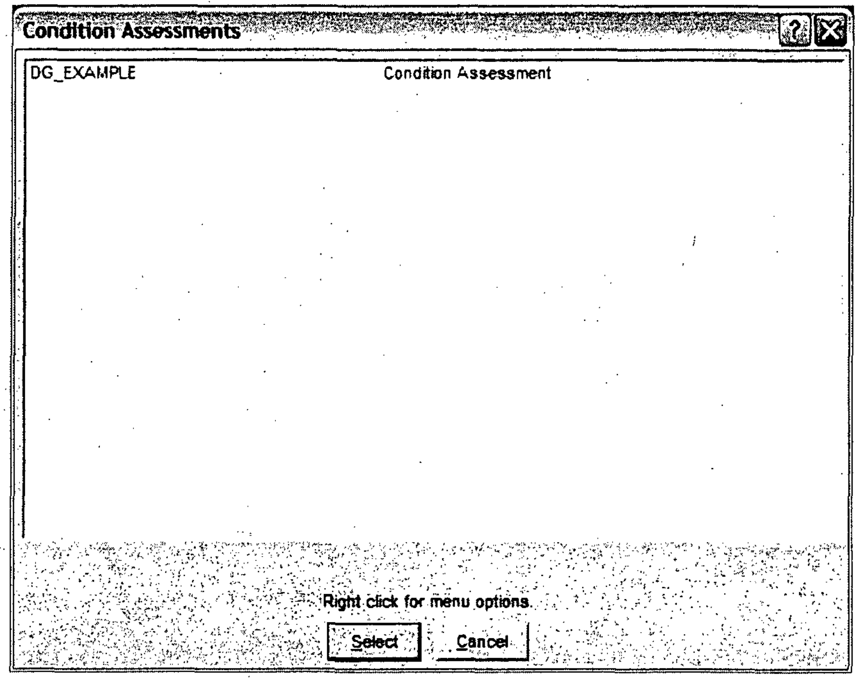

Figure 11. The GEM condition assessment initial dialog.

At this point, the assessment to be evaluated was selected by either double-clicking the left mouse button on the assessment or by highlighting the assessment and clicking the "Select" button. Selecting the assessment brought up an empty dialog box labeled "Condition Assessment Event." This dialog specified the components that were out for the duration of interest. To model the specific event from the example, failure of the diesel generator 3 was added to the list of relevant events by clicking the right mouse button on the dialog box, and selecting the Add option.

Next, a search for the event EPS-DGN-FS-DG3 was performed by scrolling the list or by simply typing in the first few characters of the event name (i.e., E, P, S, -, D, etc.).

Once the event was found and highlighted, double clicking the event to began the probability change process. The screen shown in Figure 12 appeared, allowing changes to be made to the diesel generator event. The basic event EPS-DGN-FS-DG3 was set to TRUE and the OK button was clicked. The steps were repeated for EPS-DGN-FR-DG3.

The analysis began once "Process" was selected.

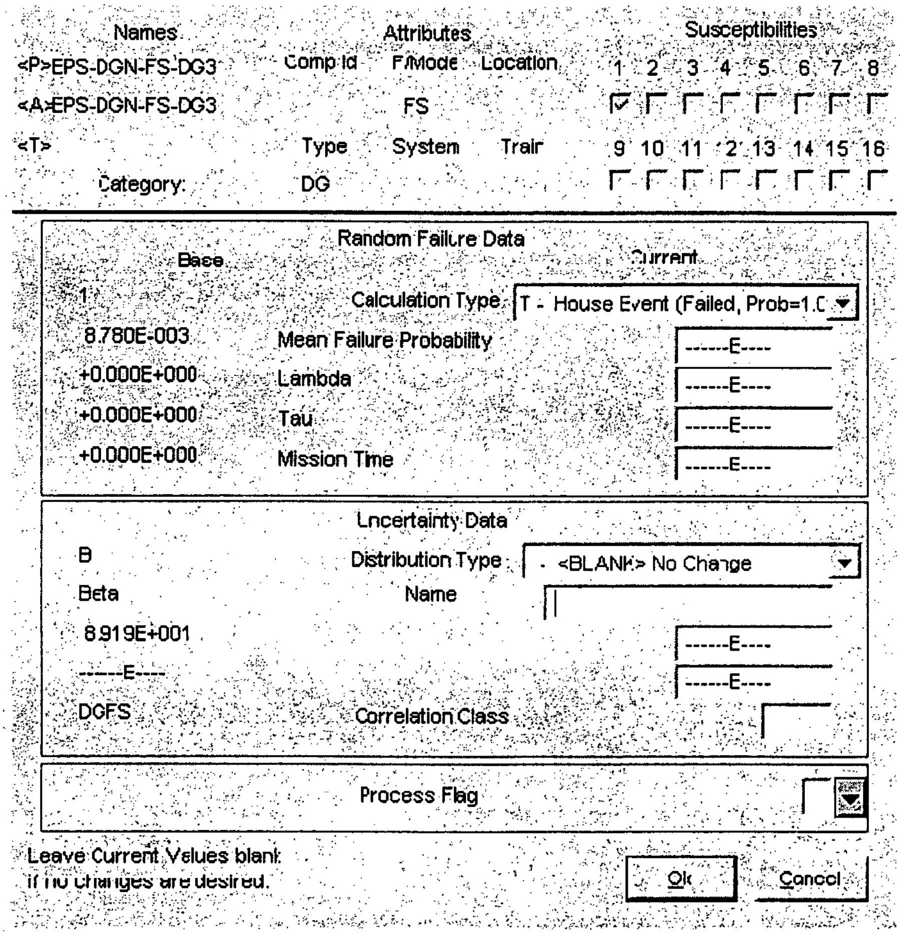

Figure 12. Modify basic event data screen in GEM.

After GEM completed the cut set evaluation (using the probability modification to the diesel generator basic events), it asked for the duration of this configuration. In this example, 100 hours was entered and the Ok button was clicked (see Figure 13).

GEM processed the analysis and then showed the "Condition Assessment" screen (see Figure 14). The CCDP, CDP, and $Importance_{event}$ for the analysis were displayed. Again, the accident sequences that contributed to the risk were displayed and sorted from highest to lowest $Importance_{event}$. The analysis report options were the same as those discussed in Section 4.2.

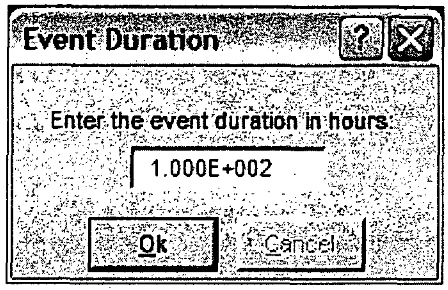

Figure 13. GEM screen to enter the condition assessment duration.

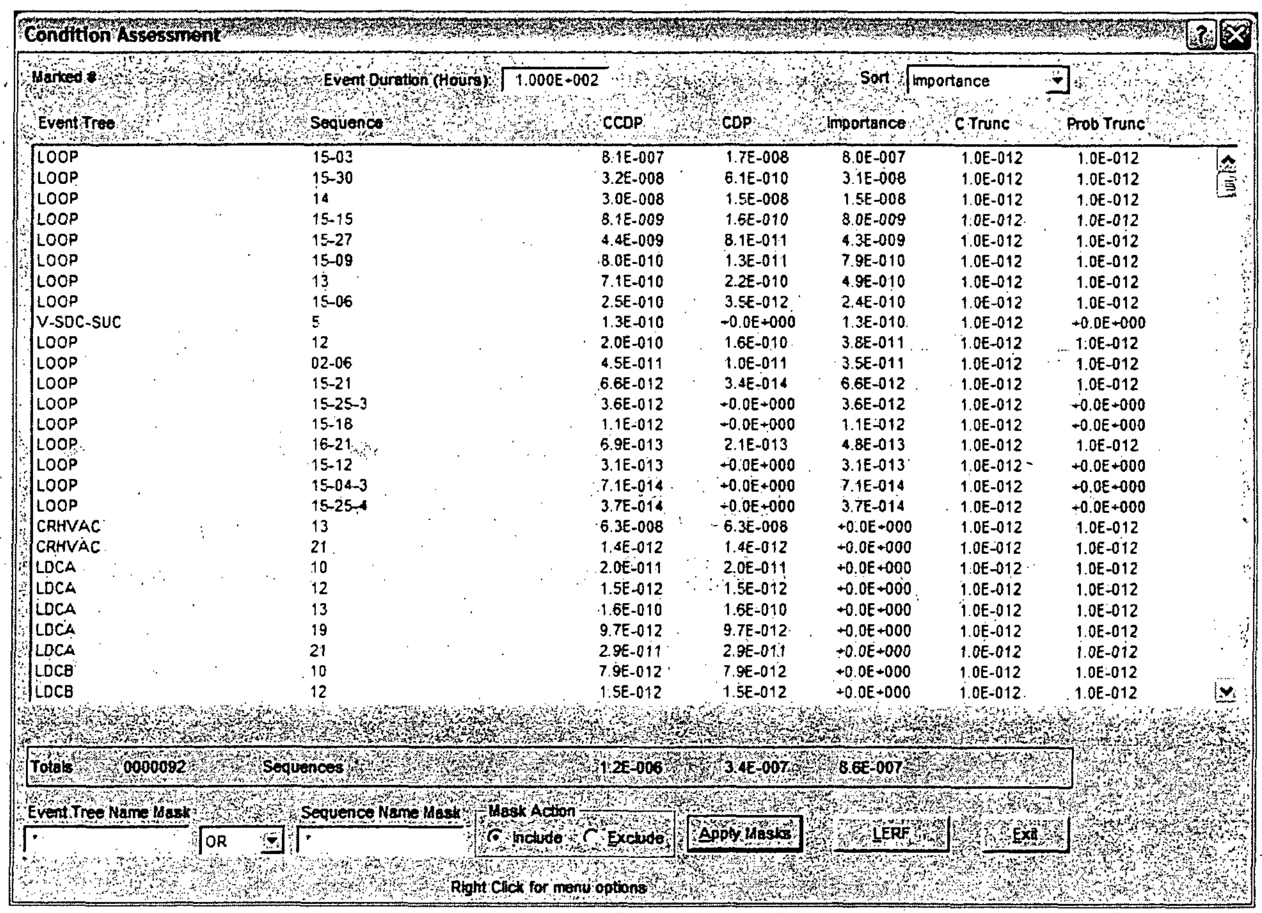

Figure 14. The GEM condition assessment screen.

4.4 Using GEM for LERF Assessments

The "LERF" option in GEM (Figure 15) allows a user to select an existing initiating event assessment or condition assessment; a change set; or create a new assessment, but evaluate the assessment using a large early release frequency (LERF) end state gather instead of the core damage sequences. GEM has been designed to look specifically for sequences labeled "PDS-" (either on the event tree graphic or created via event tree partition rules). As such, the plant model must be designed such that only LERF sequences are assigned to end states beginning with "PDS-" for the correct LERF results to be generated. In addition to the correct end state assignments, the model must be specified as "LERF-enabled" (see Vol. 3, section 9.2.9).

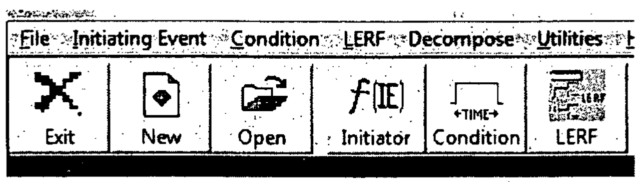

Figure 15. The GEM analysis options, including LERF.

5. CONCLUSIONS

Incidents at facilities such as nuclear power plants occur at many different times and under a variety of conditions. To evaluate these situations, the GEM software has been developed to perform what is known as an "event evaluation." An "event evaluation" represents the use of a PRA model to obtain a risk measure that is conditional on the situation which existed during an incident. GEM allows analysts to perform these types of assessments for both initiating event and condition cases.

This report addressed how the technique of event assessment is performed using the GEM risk analysis tool. Specifically, four areas of interest were discussed:

- Background material related to event evaluations.
- A theoretical framework behind event evaluation calculations.
- Pragmatic considerations when performing event evaluations using GEM.
- Guidance for performing event evaluations when using the GEM software.

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. However, what is *not* being calculated for the nuclear power plant risk profile is the probability that severe core damage *did* happen. 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?"

The conditionality that was estimated on measures such as CCDP in GEM reflects impacts on the measure of interest (i.e., core damage). Such impacts included the scenarios that have been discussed including condition and initiating event assessments (e.g., a component outage or the occurrence of an initiating event).

Lastly, a method of calculating risk levels for plant operational events was illustrated using GEM. This risk calculation, a CCDP or $\text{Importance}_{\text{event}}$, relied on the availability of a PRA model. Consequently, deficiencies in the PRA model itself, including errors, limitations, scoping issues, and questions of completeness, all could cause the resulting GEM calculations to be suspect. Investing the resources to build a risk model and then subsequently using that model as part of nuclear power plant operation obligates the users to ensure the quality of the PRA model. It is only after model quality issues have been resolved can analysts focus on the quality of operational risk calculations.

6. REFERENCES

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

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

APPENDIX A – GEMDATA

APPENDIX A – GEMDATA

Early versions of GEM have its own "stand alone" database called GEMDATA. The GEMDATA database has been prepared by the analyst who developed the SPAR models. The GEMDATA database contains the information needed to set up the ASP default analyses.

The GEM database contains or calculates the following information for each plant:

- The initiating events in the model
- The short-term nonrecovery probability for each initiating event, including offsite power nonrecovery probabilities for
    - Plant-centered
    - Grid-related
    - Severe-weather-related
    - Extreme-weather-related LOOP events
- For these short-term nonrecovery probabilities, several parameters are stored
    - Default recovery classes
    - EP fail time (i.e., time at which LOOP occurred)
    - DG median repair time
    - Core uncovery time and short-term recovery time
    - Plant recovery time and battery depletion time
    - RCP Seal design.

Note that SPAR models constructed after 2005 do not use the GEMDATA information. However, for earlier databases, the information contained in this section is applicable.

The link between GEM data and SAPHIRE data is established through the project name, so by changing a model's project name it will no longer be linked to its GEM data.

GEMDATA is an independent database management and computation software system with the primary purpose of calculating various electric power non-recovery probabilities and the reactor coolant pump (RCP) seal loss of coolant accident (LOCA) probability. GEMDATA is not a part of GEM and is not generally included in the standard distribution of the SAPHIRE software package. However, it does have the same general user interface and operating style of GEM and SAPHIRE.

GEMDATA stores and processes the information necessary to determine the proper short-term and long-term offsite non-recovery values and the probability of an RCP seal LOCA given a LOOP.

GEMDATA has five options available from its Menu Bar:

- File

- List Init Events
- Modify
- Reports
- Utilities

Selecting the "File" option, allows the creation of a new GEMDATA database, opens an existing GEMDATA database, or exits out of the program. Selecting "List Init Events" shows the user the currently available initiating events in the database (Figure A-1). By highlighting and double-clicking on a specific initiating event, the user can modify the various recovery data for that specific initiator.

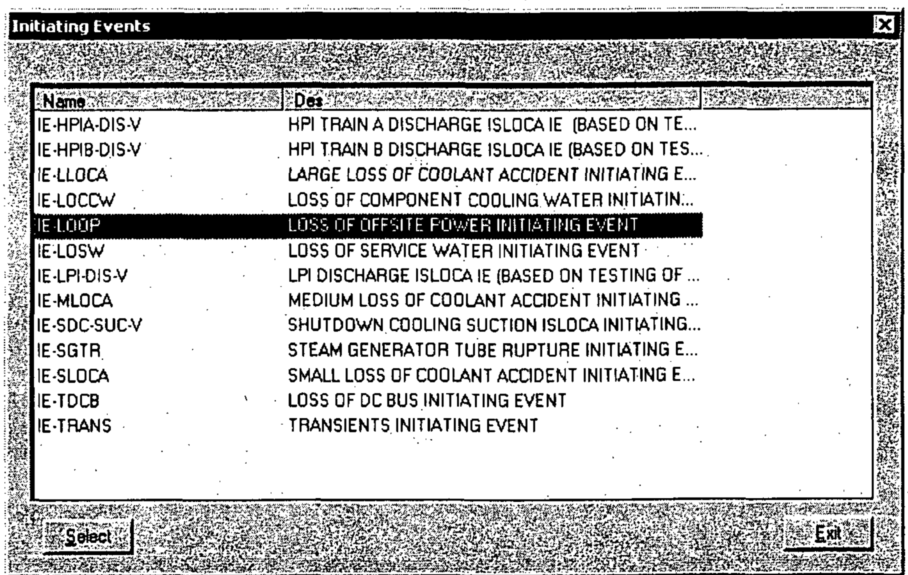

Figure A-1. Initiating events list in GEMDATA.

Selecting "Modify" allows for the analyst to modify the plant, class and recovery event data for each specific plant (Figure A-2). Modifying the various "Class" data allows for the adjustment calculation variables for the plant-centered, grid, severe weather and extremely severe weather non-recovery LOOP probabilities. Modifying the "Plant" data allows for the adjustment of assigned LOOP classes for each specific plant. This option also allows for the adjustment of the core uncovering time, battery depletion time, diesel repair time, short term recovery time and the reactor coolant pump seal design type. A brief description of the available Plant data is provided below:

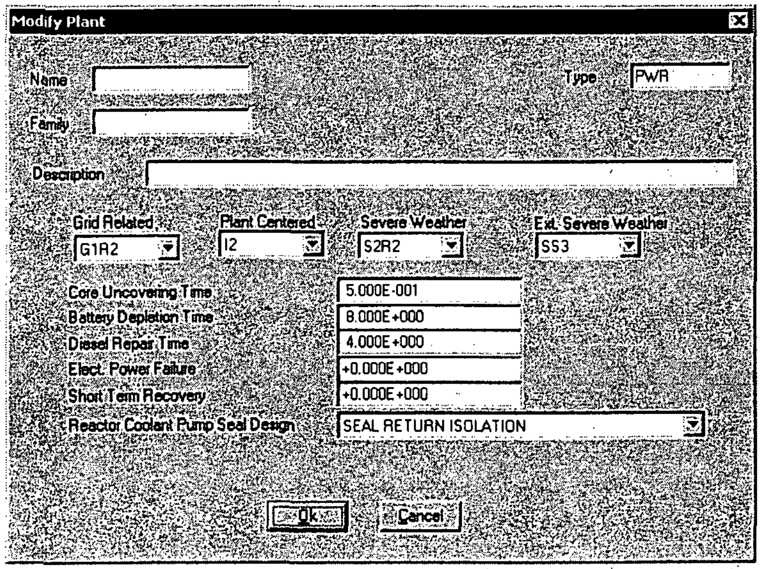

Figure A-2. Modify plant information screen in GEMDATA.

Plant_centered LOOP classs- Each plant has been assigned to one of three plant-centered LOOP classes based on the expected frequency of experiencing a plant-centered LOOP. Class I1 has the lowest frequency for a plant-centered LOOP of a given duration. Class I3 has the highest frequency and Class I2 is roughly half way in between the other two. These classes are defined and further explained in NUREG-1032[a].

Grid LOOP class - Each plant has been assigned to one of four grid classes based on the reliability of the offsite power grid. Class G1 has the lowest frequency of grid loss (less than 1 per 60 site years) and Class G4 has the highest frequency of grid loss (greater than 1 per 6 site years). Classes G2 and G3 have grid loss frequencies between the other two. See NUREG-1032 for more details.

Grid recovery class - Each plant is assigned to one of two grid recovery types. Type R1 is assigned to plants that have the capability and procedures to recover offsite (nonemergency) AC power to the site within 0.5 hour following a grid blackout. Type R2 is assigned to all other plants.

Severe weather LOOP class - Each plant is assigned to one of five severe weather classes based on the frequency of experiencing a loss of offsite power due to severe weather conditions. Severe weather conditions include lightning, rain, hail, sleet, snow, moderately high winds, and other weather related causes that do not greatly affect the time to restore power. Class S1 has the lowest frequency of offsite power loss (less than 1 per 333 site years) and Class S5 has the highest frequency (greater than 1 per 10 site years).

---

[a] U.S. NRC, NUREG-1032, *Evaluation of Station Blackout Accidents at Nuclear Power Plants*, June 1988.

Severe weather recovery class - Each plant is assigned to one of two severe weather recovery types. Type R1 is assigned to plants that have the capability and procedures to recover offsite (nonemergency) AC power to the site within 2 hours following a severe-weather-induced loss of offsite power. Type R2 is assigned to all other plants.

Extremely severe weather LOOP class - Each plant is assigned to one of five extremely severe weather classes based on the frequency of experiencing a loss of offsite power due to extremely severe weather conditions. Extremely severe weather conditions include tornadoes, hurricanes, very high winds, large accumulations of snow and ice, and other weather related causes that create conditions so that power cannot be restored for a long period of time. Class SS1 has the lowest frequency of loss of offsite power (less than 1 per 3,333 site years) and SS5 has the highest frequency (greater than 1 per 100 site years).

RCP seal design - Each PWR plant is assigned to one of seven RCP seal design categories based on the plant configuration for resisting and mitigating a seal LOCA given a loss of offsite power. BWR plants do not have entries in this field in the database. The seal LOCA probability models are based on the NUREG 11502 work and include models for the following designs: Westinghouse old O-ring, Westinghouse new O-ring, and seal return isolation. Additionally, models have been developed to simulate a select set of unique modeling conditions. These include: seals never fail, seals fail in 0.5 hours, seals fail in 1 hour, and seals fail in 2 hours.

Core uncovery time - This is the time it takes to uncover the top of active fuel from a complete loss of core cooling and injection based on the maximum decay heat rate. This value is nominally set to 0.5 hours.

Battery depletion time - This is the time it takes to suffer a complete loss of DC power following a station blackout. This time is based on the battery capacity, the expected DC power requirements, and the plant procedures for load shedding. This information has been gathered from the station blackout rule responses and other plant information such as the plant specific PRA.

Diesel repair time - This is the median time for restoration of one diesel generator when more than one is unavailable due to independent faults. A median time of 4 hours is nominally used based on information in NUREG-1032.

Short-term nonrecovery time, t-short - For initiating events that are recoverable (currently only small LOCAs and LOOPs are considered recoverable), recovery within this time would terminate the specific initiating event response. The general transient response would then be appropriate. A rigorous treatment of these recovered initiating events would transfer to the transient event tree; however, the sequence frequencies would be much smaller than the existing transient sequence frequencies and are ignored. The short-term nonrecovery time is generally 0.5 hours.

Non-LOOP initiating event non-recovery values - Transients and steam generator tube ruptures are considered nonrecoverable and are assigned a nonrecovery value of 1.0. Small LOCAs are recoverable within time t-short. The probability of not recovering within t-short for BWRs is 0.5 and 0.43 for PWRs based on information provided in NUREG/CR 46743. Modifying the "Recovery Event" data allows for the adjustment of nonrecovery probability parameters such as the equation type GEMDATA uses to calculate the recovery probabilities (Figure A-3).

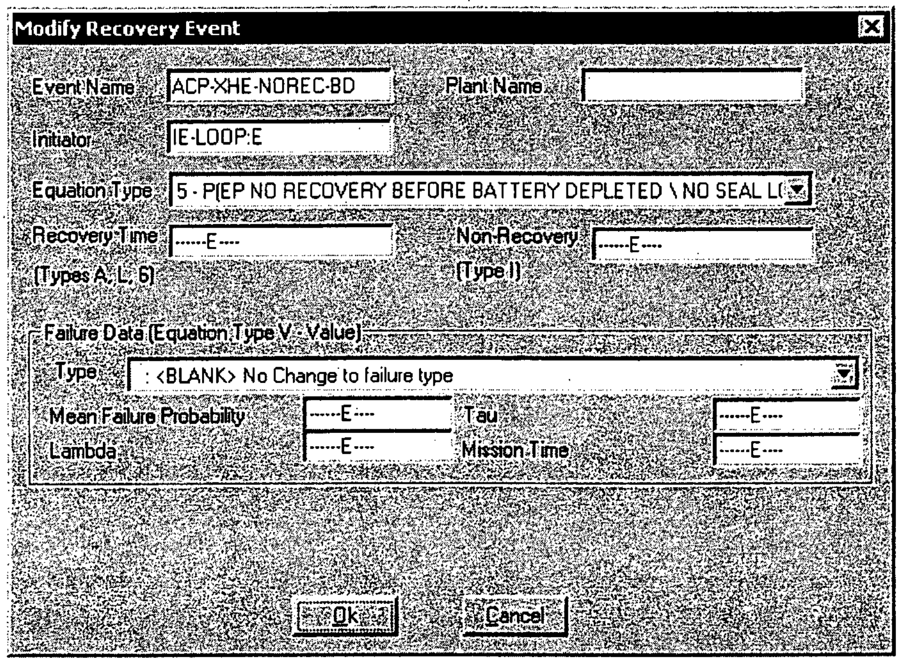

Figure A-3. LOOP nonrecovery screen in GEMDATA.

Selecting the "Reports" menu option allows the user to produce reports for Plant, Class and Recovery data. Reports can be produced on the screen, sent to a printer, or stored in text file format.

The "Utility" menu option is used to load or save GEMDATA information in a text file format. It also allows the user to "fix" a corrupted or damaged database using the "Rebuild" function.

APPENDIX B – LOOP-RELATED RECOVERIES

APPENDIX B – LOOP-RELATED RECOVERIES

The SPAR model loss of offsite power and station blackout event trees are constructed using typical fault tree linked to event tree models. This section provides additional detail on the calculation of loss of offsite power initiating event frequency, offsite power recovery failure probability, and diesel generator recovery failure probability. This information is applicable for SPAR models developed prior to 2005 (where they used five categories of LOOP):

- Plant-centered. A LOOP event in which the design and operational characteristics of the nuclear power plant itself play the major role in the cause and duration of the loss of offsite power. The line of demarcation between plant-centered and switchyard-centered LOOP events is the nuclear power plant main and station transformers high-voltage terminals. Both transformers are considered to be part of the switchyard.
- Switchyard-centered. A LOOP event in which the equipment, whether human-induced or actual equipment failure, in the switchyard play the major role in the loss of offsite power.
- Grid-related. A LOOP event in which the initial failure occurs in the interconnected transmission grid that is outside the direct control of plant personnel.
- Severe-weather-related. A LOOP event caused by severe weather, in which the weather is widespread, not just centered at the site, and capable of major disruption. Severe weather is defined to be weather with forceful and non-localized effects.
- Extreme-weather-related. A LOOP event caused by extreme weather, in which restoration of offsite power requires more than 24 hours. Example, extreme hurricane that results in significant damage.

The LOOP frequency and nonrecovery probability calculations that follow must be performed for each of the above LOOP subcategories separately, and must be performed for a composite representing all categories together.

LOOP Frequencies

In the SPAR models the LOOP initiating event frequency (λ_T) is the sum from all the individual LOOP frequency subclasses combined, or

$$\lambda_T = \sum_{i=1}^{5} \lambda_i \quad . \tag{1}$$

LOOP Nonrecovery Probabilities

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

$$P_{OPRF}(\ t_{long}\,|\,t_{short}\ ) = P(\ L > t_{long}\ |\ L > t_{short}\ ) \qquad (2)$$

where L is the duration of a LOOP, and t_{long} is a sequence-dependent time requirement that is greater than t_{short}. The interpretation of t_{long} and t_{short} are model and sequence specific. The most common application is to station blackout sequences where t_{long} corresponds to either battery depletion time or core uncovery time and t_{short} corresponds to a short-term recovery interval based on the time to uncover the reactor core if no safety systems function. In the current generation of SPAR models t_{short} is most often zero unless there are multiple failures to recover offsite power 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.

The probability that offsite power will not be recovered at time t is the fraction of all LOOP events with duration L greater than t, or

$$P(\ L > t\ ) = \int_{t}^{\infty} f_L(\ l\ )\,dl = 1 - F_L(\ t\ ) \qquad (2)$$

where f_L is the density function for the distribution of observed LOOP durations, and F_L is the cumulative distribution form of f_L . Combining Equations 2 and 3 gives the general expression for offsite power recovery failure probabilities in the SPAR models

$$P_{OPRF}(\ t_{long}\,|\,t_{short}\ ) = \frac{\int_{t_{long}}^{\infty} f_L(\ l\ )\,dl}{\int_{t_{short}}^{\infty} f_L(\ l\ )\,dl} = \frac{1 - F_L(\ t_{long}\ )}{1 - F_L(\ t_{short}\ )} \qquad (3)$$

Equation 3 can be modified so that recovery failure probabilities can be calculated when LOOP frequency and LOOP recovery information is divided into plant, switchyard, grid, and weather subclasses by frequency-weighting the class probabilities as follows:

$$P_{OPRF}(\ t_{long}\,|\,t_{short}\ ) = \frac{1}{\lambda_T} \sum_{i=1}^{n} \lambda_i \frac{\left(1 - F_{Li}\left(t_{long}\right)\right)}{\left(1 - F_{Li}\left(t_{short}\right)\right)} \qquad (4)$$

Equation 4 is the most general form for calculating LOOP nonrecovery probabilities that is consistent with past and anticipated future LOOP modeling methods used in the SPAR models.

Once the general form is known for the LOOP nonrecovery probability (Equation 4) and the frequency of each LOOP category is known, GEM still requires the functional form of the durations of LOOP for each category. The SPAR models have used two different forms, Weibull and lognormal.

The Weibull-based form of f_L is

$$f_L(t) = \frac{\alpha}{t}\left(\frac{t}{\beta}\right)^{\alpha} e^{-(t/\beta)^{\alpha}} \tag{5}$$

where

α = the distribution shape parameter, and

β = the distribution scale parameter.

The lognormal-based form of f_L is

$$f(t) = \frac{1}{t\sqrt{2\pi\sigma}} e^{-\frac{1}{2}\left[\frac{\ln(t)-\mu}{\sigma}\right]} \tag{6}$$

where t = offsite power recovery time

μ = mean of natural logarithms of data

σ = standard deviation of natural logarithms of data

Φ = error function.

If the lognormal form of the LOOP duration is used, it is typical to rely on numerical methods to evaluate Equation 4. However, if the Weibull form is used, Equation 4 may be solved analytically. Using Equation 4 and Equation 5 gives the following general expression for failure to recover offsite power at time t_{long} for LOOP class i, conditional on failure to recover offsite power at time t_{short}

$$P_{OPRF_i}(t_{long}|t_{short}) = \frac{\int_{t_{long}}^{\infty} f_{L_i}(l)\,dl}{\int_{t_{short}}^{\infty} f_{L_i}(l)\,dl} = \frac{e^{-(t_{long}/\beta_i)^{\alpha i}}}{e^{-(t_{short}/\beta_i)^{\alpha i}}} \quad (7)$$

Equation 7 is presently applied when evaluating a specific class of LOOP, as in initiating event assessments where the class of initiating event is known. For the base case SPAR model a frequency-weighted average recovery failure probability is required and Equation 7 becomes

$$P_{OPRF}(t_{long}|t_{short}) = \frac{1}{\lambda_T}\sum_{i=1}^{5}\lambda_i \frac{e^{-(t_{long}/\beta_i)^{\alpha i}}}{e^{-(t_{short}/\beta_i)^{\alpha i}}} \quad (8)$$

Diesel Nonrecovery Probabilities.

The SPAR model event trees include various emergency power nonrecovery top events in the LOOP/SBO sequences. The emergency power nonrecovery values associated with these top events include recovery of an emergency diesel generator. A median time for restoration of one diesel generator when more than one is unavailable due to independent faults is approximately four hours. In the SPAR models using the assumption of an exponential distribution of diesel recovery times, a median diesel generator repair time of four hours is used. This information can be used to construct a diesel generator recovery distribution density function

$$f_D(t) = \lambda_D e^{-\lambda_D t_{DGR}} \quad (9)$$

where t_{DGR} is the diesel generator repair time. Thus, the cumulative diesel generator recovery distribution is

$$F_D(t) = 1 - e^{-\lambda_D t_{DGR}} \quad (10)$$

Solving for λ_D associated with the median (50th percentile) gives

$$\lambda_D = \frac{-\ln(0.5)}{t_{DGR_{50}}} = \frac{0.693}{t_{DGR_{50}}} \quad (11)$$

where $t_{DGR_{50}}$ is the median diesel generator repair time.

The probability that at least one diesel generator is not recovered for some duration G is

$$P(G>t) = \int_{t}^{\infty} f_D(g)\,dg = 1 - F_D(t) = e^{-\lambda_D t} = e^{-0.693t/t_{DGR_{50}}} \quad (12)$$

The sequence-dependent repair failure probabilities used in the SPAR models are calculated from Equation 12. Some SPAR models may assume that the DG restoration times are distributed via a Weibull distribution. In these cases, the form of Equation 9 is modified to the Weibull distribution and evaluated via an equation similar to Equation 12.

Current (2005 and newer) revisions of the SPAR models used a modified LOOP recovery approach. For these SPAR models, GEM assumes the LOOP initiating event frequency (λ_T) is the sum from all the individual LOOP frequency subclasses combined, or

$$\lambda_T = \sum_{i=1}^{4} \lambda_i \tag{13}$$

The **four** classes of LOOP initiating event identified are:

- Plant-centered. A LOOP event in which the design and operational characteristics of the nuclear power plant itself play the major role in the cause and duration of the loss of offsite power. The line of demarcation between plant-centered and switchyard-centered LOOP events is the nuclear power plant main and station transformers high-voltage terminals. Both transformers are considered to be part of the switchyard.

- Switchyard-centered. A LOOP event in which the equipment, whether human-induced or actual equipment failure, in the switchyard play the major role in the loss of offsite power.

- Grid-related. A LOOP event in which the initial failure occurs in the interconnected transmission grid that is outside the direct control of plant personnel.

- Weather-related. A LOOP event caused by weather, in which the weather is widespread, not just centered at the site, and capable of major disruption. Weather is defined to be weather with forceful and non-localized effects.

The LOOP frequency and nonrecovery probability calculations must be performed for each of the above LOOP subcategories separately, and must be performed for a composite representing all categories together. The LOOP plug-in in SAPHIRE must perform the calculation described by the equation above using specified parameters in such a way that both the correct point estimate and correct uncertainty distribution of λ_T is obtained from the uncertainty distributions of the λ_i. Given the use of SAPHIRE basic events to represent the λ_i, the uncertainty is obtained from the standard SAPHIRE sampling procedures.

The current revisions of the SPAR model (2005 and newer) model the LOOP duration data using the assumption of lognormal applicable models (not Weibull). Specifically, the formulation used is for the duration distribution is given by:

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

for the probability density function or:

$$F_i(t) = \Phi\left[\frac{\ln(t) - \mu_i}{\sigma_i}\right] = \Phi(z)$$

for the cumulative distribution function,

where	t	=	offsite power recovery time
	μ_i	=	mean of natural logarithms of data for i'th LOOP category
	σ_i	=	standard deviation for i'th LOOP category
	Φ	=	standard normal distribution function.

Like for the LOOP nonrecovery calculation, SAPHIRE and GEM can also be used to determine diesel generator nonrecoveries. In older versions of the SPAR models, the DG recovery was based upon the DG failure duration time being exponentially distributed. The current SPAR models, and corresponding SAPHIRE calculation, assumes that the recovery time is Weibull distributed. The Weibull-based form of f_{DG} (the DG failure duration) is:

$$f_{DG}(t) = \frac{\alpha}{t}\left(\frac{t}{\beta}\right)^{\alpha} e^{-(t/\beta)^{\alpha}}$$

where

α	=	the distribution shape parameter, and
β	=	the distribution scale parameter.

Note that if the α parameter is assigned a value of one, then the distribution reverts to the exponential distribution used by earlier SPAR models.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202	U.S. NUCLEAR REGULATORY COMMISSION **BIBLIOGRAPHIC DATA SHEET** (See Instructions on the reverse)	1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.) NUREG/CR-6952 INL/EXT-05-00682
2. TITLE AND SUBTITLE Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 5 Gem Manual		3. DATE REPORT PUBLISHED MONTH: September YEAR: 2008 4. FIN OR GRANT NUMBER N6203
5. AUTHOR(S) C. L. Smith, J. Schroeder, S. T. Beck		6. TYPE OF REPORT 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 Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) is a software application developed for performing a complete probabilistic risk assessment (PRA) using a personal computer running the Microsoft Windows operating system. SAPHIRE is primarily funded by the U.S. Nuclear Regulatory Commission (NRC) and developed by the Idaho National Laboratory (INL). The INL's primary role in this project is that of software developer and tester. Using the SAPHIRE analysis engine and relational database is a complementary program called GEM. GEM has been designed to simplify using existing PRA analysis for activities such as the NRC's Accident Sequence Precursor program. In this report, the theoretical framework behind GEM-type calculations are provided in addition to guidance and examples for performing evaluations when using the GEM software. As part of this analysis framework, the two types of GEM analysis are discussed, specifically initiating event (where an initiator occurs) and condition (where a component is failed for some length of time) assessments.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)	13. AVAILABILITY STATEMENT
SAPHIRE, software, reliability, risk, safety, PRA, GEM, CCDP, core damage probability, ASP	Unlimited
	14. SECURITY CLASSIFICATION (This page) Unclassified (This report) Unclassified
	15. NUMBER OF PAGES
	16. PRICE

NRC FORM 335 (2-89)

Printed on recycled paper

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS