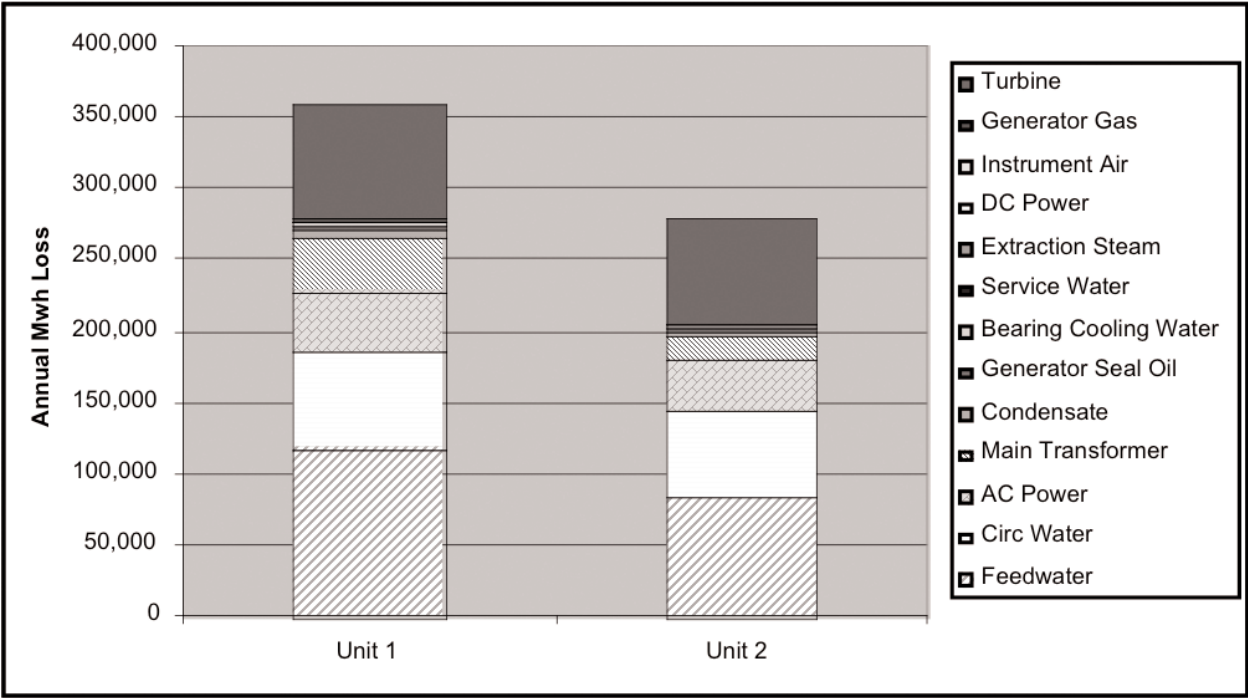


Generation Risk Assessment (GRA) Plant Implementation Guide

Technical Report



Generation Risk Assessment (GRA) Plant Implementation Guide

1008121

Final Report, December 2004

EPRI Project Manager
G. Sliter

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Applied Reliability Engineering, Inc.

ORDERING INFORMATION

Requests for copies of this report should be directed to EPRI Orders and Conferences, 1355 Willow Way, Suite 278, Concord, CA 94520, (800) 313-3774, press 2 or internally x5379, (925) 609-9169, (925) 609-1310 (fax).

Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc.

Copyright © 2004 Electric Power Research Institute, Inc. All rights reserved.

CITATIONS

This report was prepared by

Applied Reliability Engineering, Inc.
1478 27th Avenue
San Francisco, CA 94122

Principal Investigators

D. Blanchard

W. Brinsfield

P. Szetu

This report describes research sponsored by EPRI.

The report is a corporate document that should be cited in the literature in the following manner:

Generation Risk Assessment (GRA) Plant Implementation Guide, EPRI, Palo Alto, CA: 2004.
1008121.

REPORT SUMMARY

The ability to predict potential generation loss from plant trips or derates due to equipment failures is crucial for risk-informing plant operation and long-term equipment reliability planning. This guide describes how plants can implement various forms of component and system models for assessing generation risk.

Background

Just as probabilistic risk assessment (PRA) is a key activity in assuring the safety of nuclear power plants, generation risk assessment (GRA) is a key activity in assuring productivity and profitability as plants worldwide become more competitive. GRA is the process of predicting the risk of generation loss during future operation by estimating the probability frequency and duration of plant trip or derate due to equipment degradation or failure. A GRA model, whether rudimentary or detailed, is an important element of nuclear asset management risk-informed tools for analyzing effects of equipment reliability and availability on plant value and resource allocation decision-making.

Objectives

To provide plants with a guide for simplified, cost-effective modeling of systems and components for the purposes of prioritizing them in terms of risk of trip or derates due to failure and of optimizing their long-term performance in the face of constraints on capital and O&M budgets.

Approach

The researchers used their expertise in PRA and economic risk modeling for nuclear and fossil power plants, along with results from other EPRI and industry work, to provide guidance for developing plant-specific GRA models. The GRA process involves identifying equipment functions related to production, performing failure modes and effects analyses, constructing a trip/derate model, calculating future year-by-year availability, efficiency, and capacity factor for input to economic models. The guide also identifies types and sources of data required by the GRA process.

Results

A survey of plants revealed that GRA is in its infancy—three of the twenty-nine plants surveyed have detailed GRA models and only six others have made any progress toward constructing GRA models. Because lack of resources is a major barrier to progress in implementing GRA, this guide is developed in a way that should be useful to utilities with varying degrees of budget and staff availability. The guide tells how to use equipment functions and failure analysis to select the most important systems and components for modeling. It also discusses types of data

required, data uncertainties, how to calculate propagation of uncertainties in the model, and how to display and interpret GRA model results.

EPRI Perspective

The cost of implementing and applying GRA over a plant's remaining life is estimated to be less than a million dollars in present value. This would be paid back if a GRA model prevents losing revenues from just a few days of full-power operation. EPRI expects the field of generation risk assessment, in support of plant decision-making, to grow as benefits of asset management in a competitive industry become more widely recognized, as pressures of competition increase, and as plants age, pointing out the wisdom of applying risk-informed asset management for equipment long-term life-cycle planning. A trial implementation of GRA modeling is under way at the Cooper Nuclear Station of Nebraska Public Power District.

Keywords

Probabilistic risk assessment

Generation risk assessment

Life-cycle management

Nuclear asset management

Risk-informed asset management

ACKNOWLEDGMENTS

EPRI and the authors acknowledge the support and technical guidance provided by the following cofunders:

Generation Risk Assessment User Group

EDF Electricité de France	Hervé Chardonnel
Nebraska Public Power District	Kent Sutton
Omaha Public Power District	Alan Hackerott
South Texas Project NOC	Ernie Kee, Alice Sun
Tennessee Valley Authority	Walter Justice, William Mims

Nuclear Asset Management User Group

British Energy	John Smart
Candu Owner Group	Vince Gonsalves
Constellation Energy	David Snyder
Detroit Energy	Wayne Colonnello
DukeEnergy	Mitch Baughman
Electricite de France	Serge Hugonnard-Bruyerè, François-Noël Rémy,
Iberdrola/Iberinco	Jose Gomez, Luis Gerez
Nebraska Public Power District	Joseph Edom
Omaha Public Power District	Mike Gayoso, Joseph Gasper
South Texas Project NOC	Drew Richards
Texas Utilities	Mark Mangum

We also gratefully acknowledge technical support from:

Russ Green, Texas Utilities

James Liming, ABS Consulting

William Parkinson and Ken Canavan, EPRI

Rambir Parmar, Nuclear Safety Solutions

Jacques Plourde, Candu Owners Group

Elmira Popova and David Morton, University of Texas at Austin

Shuwen Wang, Texas A&M

CONTENTS

1 INTRODUCTION	1-1
1.1 Background	1-1
1.2 Objective	1-2
1.3 Approach	1-3
1.4 Industry Status of GRA Implementation	1-5
1.5 Organization of the Guide	1-5
2 POWER REDUCTIONS FROM POSTULATED FAILURES.....	2-1
3 SYSTEM MODELING AND ANALYSIS	3-1
3.1 Selection of Systems for GRA.....	3-1
3.2 Logic Model Development.....	3-4
3.2.1 Supercomponent Approach.....	3-5
3.2.2 Detailed Logic Model Approaches.....	3-10
3.2.2.1 Generating New Fault Trees.....	3-12
3.2.2.2 Conversion of Existing PRA Fault Trees.....	3-20
3.3 Sources of Information for Selecting Systems for Detailed Modeling and Analysis	3-22
4 INPUTS AND DATA SOURCES	4-1
4.1 Types and Accuracy of Data Required for a GRA.....	4-1
4.2 Sources of Data.....	4-3
5 QUANTIFYING GRA RESULTS	5-1
5.1 Quantification of the GRA Models in Terms of Event Frequency.....	5-1
5.1.1 Supercomponent Model	5-1
5.1.2 Fault Tree Logic Models	5-2
5.1.2.1 Elimination of Duplicate Failure Combinations	5-3
5.1.2.2 Treating Differences between the Trip and Derate Frequencies of the Models and Operating Experience.....	5-3

5.2 Quantification of Lost Generation Consequences.....	5-4
5.3 Propagation of Uncertainties	5-5
6 RESULTS AND APPLICATIONS.....	6-1
6.1 Primary Results	6-2
6.2 Breaking Down the Results	6-2
6.2.1 Breaking Down the Results by System and Derate Level	6-3
6.2.2 Breaking Down the Results at the Component Level	6-3
6.2.3 Distribution of the Plant Capability to Produce Power	6-15
6.3 Applications	6-17
6.3.1 GRA Applications	6-17
6.3.1.1 Converting Reliability Results to Economic Value	6-19
6.3.2 Trip Model Applications	6-19
6.3.3 FMEA Applications	6-21
7 RESOURCE REQUIREMENTS.....	7-1
7.1 Resource Allocation	7-1
7.1.1 Initial Resources for Implementation	7-2
7.1.2 Resource Estimates for Applications	7-5
7.1.3 Recurring Costs.....	7-9
7.2 Cost-Benefit Assessment.....	7-12
7.3 Coordination with Other Projects.....	7-14
8 FUTURE DEVELOPMENTS.....	8-1
9 REFERENCES	9-1
A GRA MODEL DATA SOURCES.....	A-1
B QUANTIFYING GRA RESULTS – SUPPORTING INFORMATION.....	B-1
B.1 Eliminate Duplicate Failure Combinations (Section 5.1.2.1).....	B-1
B.2 Treating Differences between the Trip and Derate Frequencies of the Models and Operating Experience (Section 5.1.2.2)	B-2
B.2.1 Models with Operating Components having Failures Expressed in Units of Annual Frequencies.....	B-2
B.2.2 Models with Operating Components having Only 24 Hour Mission Times	B-3
B.2.3 Models Containing Both Frequency and Mean Time to Repair Events	B-4

B.2.4 Models Containing Surrogate Events.....	B-5
C CONFIGURATION/CHANGE CONTROL.....	C-1

LIST OF FIGURES

Figure 1-1 GRA Model Role in an Economic Model	1-2
Figure 1-2 Overview of the Development of Trip and GRA Models	1-4
Figure 1-3 Major Steps of a GRA Implementation	1-6
Figure 2-1 Failure Modes and Effects Analysis (FMEA) – Example	2-5
Figure 2-2 Top Logic Model for Delineating Derate Levels – Example	2-6
Figure 3-1 A Typical Single Failure Vulnerability Supercomponent Model	3-7
Figure 3-2 Typical Supercomponent Train Level Model	3-9
Figure 3-3 Example of Fault Tree Linking	3-11
Figure 5-1 Generation Loss (Right Scale Probability Density – Left Scale Cumulative Distribution)	5-7
Figure 6-1 Overview of the Development of Trip and GRA Models (From Figure 1-2)	6-1
Figure 6-2 Example GRA Results Display: Cumulative Annual Lost Generation per Unit, Two Unit Site	6-4
Figure 6-3 Example GRA Results Display: Two Unit Site – Annual Lost Generation as a Function of Derate Amount	6-5
Figure 6-4 Example GRA Results Display: Single Unit (Unit 1), System Contribution to Annual Lost Generation as a Function of Derate Amount	6-6
Figure 6-5 Example GRA Results Display – Matrix of Results	6-7
Figure 6-6 Example GRA Results Display – Two Importance Measures	6-10
Figure 6-7 Example GRA Results Display – 4 Quadrant Plot Overview	6-11
Figure 6-8 Example 4 Quadrant Plot for Selected System	6-14
Figure 6-9 Incorporating Uncertainty into Results to Support Decision Making	6-16
Figure 6-10 Displaying Economic Indicators: Example	6-20
Figure 6-11 Example Trip Monitor Interface Screen	6-22
Figure 7-1 Simplified Cost Benefit Analysis Using GRA Results	7-7

LIST OF TABLES

Table 1-1 Sample Applications Supported by GRA	1-7
Table 2-1 Functions Important to Generation	2-3
Table 3-1 BWR Top 25 Contributors to Lost Generation (Unit-Years = 474.58).....	3-3
Table 3-2 PWR Top 25 Contributors to Lost Generation (Unit-Years = 1009.25).....	3-4
Table 3-3 Contribution of I&C Failures to Trip and Derate Frequencies for PWRs and BWRs	3-16
Table 3-4 Balance-of-Plant Systems that may be Modeled in PRAs	3-21
Table 4-1 Data Effort for Sample GRA Applications	4-2
Table 6-1 Examples of Applications of GRA and Intermediate Results	6-17
Table 7-1 Resource Estimates for Initial Steps of a GRA	7-3
Table 7-2 Resource Estimates for Detailed Fault Tree Approach, First Set of Systems	7-3
Table 7-3 Level of Effort for Applications	7-10
Table 7-4 Resource Estimates for Recurring Efforts	7-10
Table 7-5 Total Resource Requirements, Including Applications	7-11

1

INTRODUCTION

Generation Risk Assessment (GRA) is the process of predicting the risk of generation loss during future operation by estimating the probability and duration of plant trip or derate due to degradation or failure of equipment (systems, structures, and components – SSCs).

The primary reason for implementing GRA is to support the performance of applications that impact plant operations and economic performance by improving reliability, reducing maintenance costs, or reducing future lost generation. Table 1-1 at the end of this section is list of applications that can be supported by GRA.

1.1 Background

Risk is defined as the product of the **frequency** of degradation or failure of SSCs and the **consequences** of those failures.

In general, the **consequences** of failures relate to safety, generation, or economic loss. Safety consequences, although an obviously important potential result of equipment failure and unavailability, are treated by PRA and not addressed in this guide. The consequence of main interest to GRA is the impact of generation loss on economic loss. (Note that risk informed asset management (RIAM) evaluations *do* consider safety and other considerations not explicitly addressed by this GRA guide.)

The path from generation loss to economic loss is indicated in Figure 1-1. The shaded rectangle represents some of the key parts of a GRA model. Equipment failures reduce revenues by an amount equal to generation loss times the price of electricity and increase production cost by the cost to repair the failures and return the plant to full power. The focus of this guide is generation loss. Economic consequences are addressed by economic evaluation tools such as LcmVALUE for long-term equipment reliability planning [1] and RIAM, under development by EPRI [2] for examining the effects of risk and uncertainty on life cycle decision making.

The **frequency** factor in the risk equation can be derived using plant-specific or generic information on equipment failure rates and plant response models to translate failures into lost generation. The plant's responses to failures are characterized by *trip and derate logic models*. Logic models have a variety of forms. The simplest is a list of components for which failure directly trips the plant. If component failure does not always trip the plant, experience data can be used to estimate the trip percentage, and this percentage can be used to predict future plant response. This simple model is used by the EPRI life cycle planning (LCM) process [3] for guiding decisions on preventive maintenance and capital improvement projects over the remaining plant operating term. The LCM process assesses industry and plant-specific

experience data on the extent to which failures of a given SSC have led to lost megawatt-hours. These data combined with engineering judgment are used to estimate future failure rates and their impact on generation.

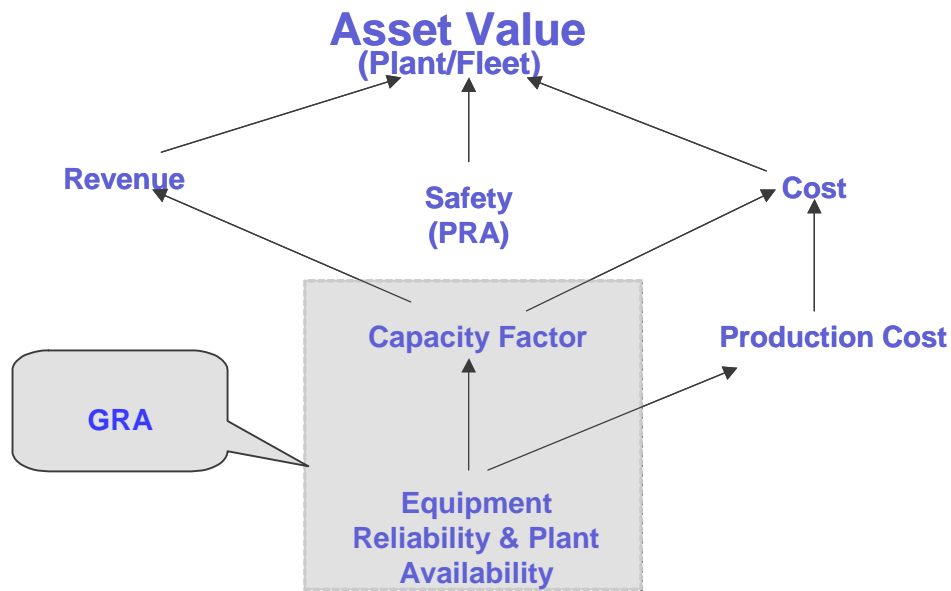


Figure 1-1
GRA Model Role in an Economic Model

The logic model could also be as simple as a list of systems with corresponding estimates of trip and derate frequencies or, going one step further, expanding the list of components discussed in the preceding paragraph to also include single point vulnerabilities contributing to system degradations or failures resulting in derates of less than 100%.

The most detailed plant response model is a fault tree trip and derate model. Although this guide attempts to cover all forms of plant response models that may be appropriate for use in GRA models in various situations, it focuses on pointing out the benefits of a fault tree trip and derate model of plant equipment important to generation, and how plants can implement such a model most cost-effectively.

1.2 Objective

The objective of this guide is to provide EPRI member utilities with the know-how to implement a GRA process at their nuclear power plants. The guide emphasizes the development of appropriately simple logic models; the treatment of uncertainty in models, assumptions, and data; and how to interpret results of a GRA model. These capabilities can improve equipment long-term planning, which is an important part of the equipment reliability process in INPO Report AP-913 [4]. A GRA model can be used to prioritize the importance of components to reliability and productivity. This prioritization can be a basis for refining the degree of “criticality” of components assigned by less rigorous methods in current implementations of AP-913. (Note that there can be a “feedback loop” between GRA and AP-913 - data and information already

compiled in response to AP-913 may be valuable as initial input to the GRA effort, such as work done in the scoping and identification of critical components step; the GRA results can be used as stated to refine the AP-913 criticality findings.)

The guide is developed in a way that should be useful to utilities with varying degrees of resource availability (both budget and personnel). Users will be guided in determining the approach to predicting lost power generation that is most cost-effective for achieving the benefits of risk-informed asset management and other applications of trip and derate modeling for their plants.

1.3 Approach

This guide takes full advantage of previous work completed by EPRI and utilities that have performed GRA-type analyses. Specifically, EPRI report 1007386 (Introduction to Simplified Generation Risk Assessment Modeling) [5] provided a foundation for trip and derate modeling from which this guide was developed. Note that another useful companion document for information on risk-based methods applicable to generation risk assessment is “Risk-Based Methods for Equipment Life Management: An Application Handbook” [6]. In addition, documents available from various utility organizations, and interviews with personnel involved with GRA implementation at those utilities, were used to obtain information on balance-of-plant (BOP) modeling as well as the GRA process in general.

A trip and derate model (sometimes referred to simply as a trip model) integrates the effects of all SSCs involved in a trip or derate.¹ A trip model is sometimes called a “balance-of-plant” (BOP) model, although it also includes all nuclear steam supply components important to production. A trip model is a model comprised of a collection of top logic that represents combinations of key plant systems whose failure can result in a plant trip or derate, detailed models of key systems, and the probability of failure and unavailability of plant components in key systems.

GRA modeling also identifies combinations of basic events (i.e., equipment failures) that lead to trip or derate and combines these events with repair and recovery times to predict the resulting lost power generation over a future period. The fundamental difference between the trip models and GRA models is the explicit treatment within the GRA process of the consequences of the trip/derate, namely, future megawatt-hours lost. The primary use of trip/derate models to date has been to provide the relevant input data for trip monitors, which are displays that provide valuable tools for keeping track of (1) the generation related response of the plant to system, structure, and component (SSC) failures; and (2) online trip/derate risk as a function of which components are in and out of service during operation.

¹ Derates are defined as any drop in power from the 100% level. A plant “trip” is a 100% derate. Some models include only those events that result in a 100% trip, and therefore are truly “trip models.” Other models include events whose unavailability results in power derates of less than 100%, including events associated with 100% derate (i.e., plant trip) situations. This latter version of the trip/derate model is the version of interest in this guide.

Figure 1-2 is an overview of how a trip/derate model supports GRA, ultimately leading to an economic model for Risk-Informed Asset Management (RIAM). The activities on the left, leading to the box labeled “availability model”, are described in Section 2 and discussed in more detail in Sections 3, 4, and 5. These activities result in the combination of trip/derate frequencies with plant recovery times to produce the main part of a GRA model, namely, the prediction of lost generation (Mwh). The other part of a GRA model is a thermal efficiency model (heat-rate model) such as PEPSE [7]. Efficiency modeling is beyond the scope of this report. Note that a GRA model (a GRA “calculator”) consists of an availability model and an efficiency model, but in this report we refer to the availability model by itself as the GRA model.

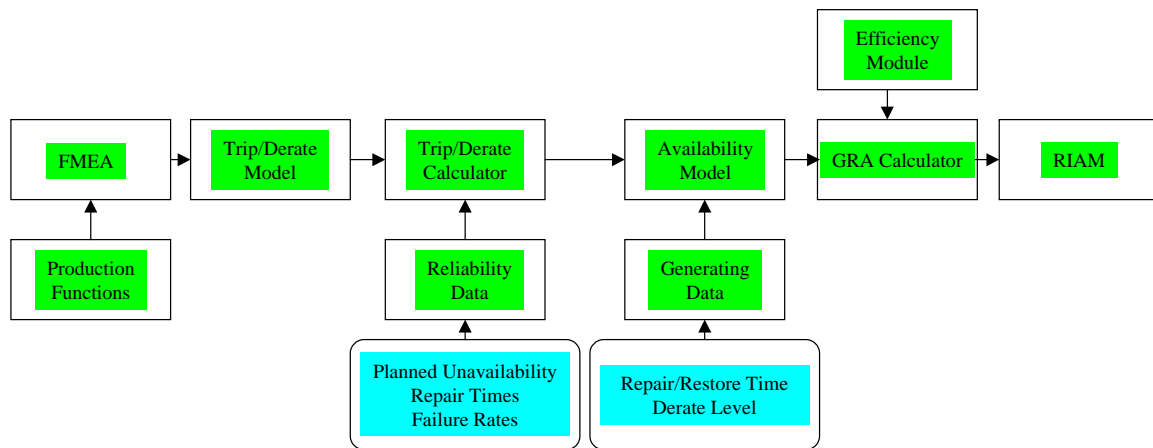


Figure 1-2
Overview of the Development of Trip and GRA Models

The GRA process is an extension of the risk or trip monitor tool set developed by EPRI [8], i.e., the trip monitor can be viewed as a subset of (or module of) a GRA model. Whereas the trip monitor is focused on changes to the risk profile at a plant over a relatively short time frame (e.g., the next day or week), the objective of the GRA process is to allow a utility to estimate risk (as measured in megawatt-hours (Mwh) lost) over the future of the plant. The output of a trip model is a listing of the equipment failures that result in a plant trip or derate and their associated frequencies of occurrence. The GRA model calculates the risk of generation loss as a result of the equipment failures. The output of the GRA process serves as input to the RIAM model and software. In addition to Mwh lost there may be many other outputs that can be derived using GRA models and results, including performance measures such as capacity factor, equivalent forced outage rate (EFOR), availability, etc. (see, for example, Appendix F of Reference [9]). However, this guide limits its discussion to Mwh lost. Note also, that the Mwh lost is only one type of input required for RIAM. Others (not indicated in Figure 1-2) are costs and safety parameters.

The generation loss calculated by the GRA model is a function of the resulting power reduction and the time to repair/restore the equipment to service and recover the plant power level. If desired, uncertainty distributions can be applied to key failure rate parameters and propagated through the analysis to provide indications of the degree of confidence in the results. In the case of a trip, the loss is 100% of the plant power level in megawatts, times the duration of repair including ramp-down and ramp-up. With this model, the analyst can consider the impact of

revisions to the equipment failure rate or the repair time as a result of alterations to the operation of the plant and/or SSCs in future years. The revisions to the equipment failure rates or recovery times of specific SSCs can be used to evaluate the merits of different, and sometimes competing, investments for avoiding the loss of megawatt hours during the remaining operating term. The revised or future failure rates can include the effects of aging that increase the failure rate as well as the effects of preventive maintenance activities that reduce the failure rate. Alternative aging management plans are conceived and evaluated as part of the LCM process [3]. A GRA model can be used in the economic evaluation of each alternative aging management plan. The evaluation is enhanced in RIAM by the explicit treatment of uncertainty in value drivers like power price, failure rates, and lost power generation forecasts.

Note that a GRA analysis is similar to a PRA analysis in that both have event frequencies as part of their results. A PRA analysis translates these frequencies into a total core damage frequency. A GRA analysis gives event frequencies but, in addition, considers both the duration and magnitude of resulting derates to produce a year-by-year projection of lost generation and capacity factor.

1.4 Industry Status of GRA Implementation

An early step in this project was to survey plants to determine the status of GRA implementation in the nuclear power industry. The survey covered 29 utilities in the U.S, France (Electricité de France – EDF), and Spain (Iberdrola).

Of course, all plants have some kind of model, however basic, regarding how components affect power generation. The survey inquired about the status of plants in constructing or using PRA-like logic models for their balance-of-plant equipment.

Only three of the utilities surveyed have a detailed balance-of-plant model in use (South Texas Project (STP), EDF, and Iberdrola). Two of the three (STP and Iberdrola) are using it for GRA. Six other utilities have made some progress toward building a model. Twenty (about 70 percent) have no logic models nor near term plans for constructing one. Of the twenty, fifteen view the models as desirable for supporting improved plant performance, but lack the resources to build them. Five are not convinced of the cost-effectiveness of building and using detailed models. They prefer using some kind of single point vulnerability models for estimating the effects of failures on generation loss.

1.5 Organization of the Guide

This guide is arranged in a manner consistent with the overview of GRA presented in Figure 1-3. Section 1 introduces the concepts of generation risk, frequency, and consequences. Sections 2 and 3 provide detail with respect to plant, system and component information needed to complete a GRA. Section 4 provides information about data sources and uncertainty. Section 5 follows with discussions of techniques available to integrate and generate numerical results. Section 6 describes ways of interpreting the results and presenting them in a manner that is meaningful not only to the analyst but in a form that is (a) useful to others in the utility's organizational structure, and (b) easily used as input to RIAM modules. Section 6 also contains a discussion of the uses and applications of GRA models and results.

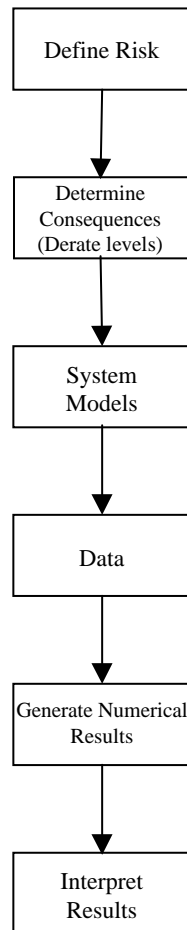


Figure 1-3
Major Steps of a GRA Implementation

Section 7 contains information pertaining to resource requirements and other GRA process topics of interest. Finally, Section 8 identifies potential future developments in the area of GRA.

Table 1-1
Sample Applications Supported by GRA

<p>Risk-Informed Asset Management (RIAM) Applications (See Reference [2])</p> <ul style="list-style-type: none"> • Refueling outage schedule and duration optimization • Generating unit power uprate or upgrade • Capital spares procurement analysis and optimization • Unit efficiency (i.e., heat rate) improvement • Plant license renewal • Treatment of risk from human errors • O&M procedure improvement • Operating/maintenance procedure training prioritization • Trade offs between online and offline maintenance • Quality assurance audit prioritization
<p>Equipment Reliability & Life Cycle Management (LCM) Applications (See Reference [2])</p> <ul style="list-style-type: none"> • Equipment criticality • Design modification optimization • Major equipment refurbishment/replacement/repair decisions & optimization • Station major maintenance activity prioritization • Component aging and aging management • Component obsolescence management • Equipment long-term planning (LCM)
<p>Other GRA Applications (See Reference [5])</p> <ul style="list-style-type: none"> • Input to RIAM • Test/maintenance frequency optimization • System health reporting • Project prioritization • Component prioritization • Online/shutdown trade offs given equipment degraded performance • Grid stability issues • Trip monitor
<p>Other Applications Supported by GRA (See Reference [28])</p> <ul style="list-style-type: none"> • Preventive/Predictive/Corrective Maintenance prioritization • Capital improvement assessment • Operating experience review • Bulk power trading • Insurance • Business plan optimization • Mergers and acquisitions

GRA applications are discussed further in subsequent sections (see, for example, Section 6).

2

POWER REDUCTIONS FROM POSTULATED FAILURES

A GRA depends upon the analysis of the impact of postulated equipment unavailability on the ability of a plant to produce power (as measured in megawatt-hours). The power level reduction associated with postulated failures is a key factor in determining the consequences of the failures, and thus in estimating the overall risk significance (risk = frequency x consequences) associated with the equipment (see Figure 1-3). Thus, regardless of the level of detail to which the GRA model will be developed, the plant response (i.e. level of derate) resulting from equipment unavailability must be identified.

The resulting reduction in power is determined by performing a “top down” assessment of the contributors to plant derates. At the top level, this approach begins with the identification of plant functions important to generation. Additional information is added by identifying systems that support the functions, trains that comprise the systems, and components that make up the trains. Tools such as reliability block diagrams (RBDs) and availability block diagrams (ABDs) can be used to outline the top level logic.

Working from the top level downward, techniques such as relatively simple failure modes and effects analyses (FMEAs) are useful for discovering and documenting information at the component level, whether developing a single point vulnerability component model or logic models for each system. In the first approach (single point vulnerability model), components in each system are classified as having the potential to contribute to one or more magnitudes of derate. The second approach, the system logic model approach, has the advantage that it can predict derate levels not only from each individual failure, but all combinations of failures as well. In either case, the primary purposes of the FMEAs are to identify major single failures and to assist with the definition of success criteria for the subset of systems selected for more detailed modeling.

Note that although FMEAs are explicitly identified in Figure 1-2 and in this section, any approaches and/or data sources that provide information relating component unavailability to plant derate levels are acceptable alternatives. For example, system training documents, design basis documents, Maintenance Rule scoping documents, and INPO AP-913 criticality analyses at the plant may contain “FMEA-like” material directly applicable to the task of determining plant response (derate) following component and system outages (for example, some plants may have completed single point vulnerability assessments as part of their implementation of AP-913). During this step, plants may also take advantage of detailed equipment and system relational databases and associated tools, if available, although those tools may have a level of sophistication not necessary for the FMEA. For illustration purposes, the remainder of this section focuses on the development of FMEAs.

As mentioned previously, the first step required for determining plant responses to equipment outages is to identify the functions important to generation at the plant. Although there may be an overlap between functions important to safety and those important to generation, for the most part those important to generation consist of “balance-of-plant” systems and components.

Table 2-1 contains a list of primary, supporting, auxiliary, and regulatory functions important to generation for boiling water reactors (BWRs) and pressurized water reactors (PWRs). The information contained in Table 2-1 is consistent with similar types of lists prepared for PRAs and is an inherent part of the approaches employed by the few utilities that have completed GRA applications. Although the labeling of the functions and their placement within the table may differ from plant to plant, the information in the table is generally representative of the functions that must be satisfied at any plant in order to maintain power generation. The GRA analyst must generate a function list that applies to a specific plant.

In Table 2-1, primary functions are those that directly support the power conversion system. In other words, these functions may be thought of as having a direct relationship to power production.

Supporting functions do not by themselves directly impact power production, but are required to maintain the systems providing primary functions.

Auxiliary functions neither directly relate to power production nor support functions that do. However, failure to maintain these functions will result in degradation of other equipment that will eventually result in power derates (including full plant shutdown).

As the name implies, regulatory functions are functions that must, by regulation, be maintained for the plant to remain at power. These functions are typically associated with safety concerns, but may be connected to other topics such as environmental issues (e.g., high temperature discharge impacts on fish species, etc.). Failure to maintain the regulatory functions will result in power derate (including the possibility of plant shutdown) due to technical specifications and limiting conditions of operation.

Once all the functions in the table are identified, the systems that support the functions can be delineated. FMEAs then can be completed on each of these systems to assess derates associated with equipment and train unavailability. The results provide the basic level of input to logic models to begin associating equipment unavailabilities with consequences, namely, lost generation.

In some cases, the levels of derate resulting from equipment outages may appear to be easily determined as a direct function of the relative size of the equipment. For example, loss of a 33% pump (i.e., one of three pumps in a three pump system, all of which are required for full power operation) will lead to a 33% derate. However, secondary effects must be examined as well to ensure that the plant can and will continue to operate at this reduced power level given the loss of the equipment. In this example, without intervening operator action to implement the load reduction, loss of one of the three pumps may result in a complete shutdown due to conditions associated with load imbalance, even if the plant were capable of physically maintaining operation with only two pumps remaining operable. Thus, the loss of one of these three pumps in conjunction with failure of the operator to initiate a power reduction results in a 100% derate (i.e., a plant trip). In other situations, a component outage may result in loss of generation (perhaps as a result of technical specification requirements) that may require a manual shutdown even though it may not directly affect the ability to generate power.

Table 2-1
Functions Important to Generation

Function Category	BWR	PWR
Primary	<ul style="list-style-type: none"> • reactivity control <ul style="list-style-type: none"> – CRDMs – reactor recirculation (flow control) • flow of the steam to the turbine, • conversion of the energy to electrical power in the turbine/generator, • connection to the grid • condenser operation • maintenance of the inventory in the reactor 	<ul style="list-style-type: none"> • reactivity control <ul style="list-style-type: none"> – CRDs – boration • reactor recirculation (flow) • flow of the steam to the turbine, • conversion of the energy to electrical power in the generator, • connection to the grid • condenser operation • maintenance of the inventory in the steam generator
Supporting	<ul style="list-style-type: none"> • motive power • control power (incl. pneumatic) • equipment cooling • lubrication • HVAC 	<ul style="list-style-type: none"> • motive power • control power (incl. pneumatic) • equipment cooling • lubrication • HVAC
Auxiliary	<ul style="list-style-type: none"> • reactor coolant system integrity <ul style="list-style-type: none"> – seals – SRVs • reactor water chemistry 	<ul style="list-style-type: none"> • reactor coolant system integrity <ul style="list-style-type: none"> – seals – PORVs • reactor makeup & letdown • reactor & SG chemistry
Regulatory	<ul style="list-style-type: none"> • Technical Specification LCOs 	<ul style="list-style-type: none"> • Technical Specification LCOs

Derate levels can be grouped into categories, e.g., 100% for plant trips or shutdowns, 50% derate for multi-train BOP systems having half full capacity per train, 33% derate for multi-train systems having one third capacity per train, 10% for equipment failures that lead to only a minor load reduction, etc. The number and magnitude of the categories depend on the capability of the plant to continue generation on less than a full complement of trains for each system needed to support power operation. Each category can be assigned a power level or magnitude of load reduction based on the actual capability of the individual trains in each system (for example, a single train of feedwater in a two train feedwater system may actually be capable of providing flow to support 60% power, in which case a 40% derate category would be created). If a component failure results in a derate level for which a category does not exist, the analysts can either create a category specifically for the derate level, or make the assumption that the derate level is the same as a derate level for which a category does exist. For example., a component contributing to a 30% derate may be included within the 33% derate category to simplify subsequent modeling and evaluation efforts. It is important to recognize that there may be a trade-off between the accuracy of the results and the time spent generating those results if this type of assumption is employed.

Sources available to assist with the determination of derate levels and the categories into which they might be grouped include the following:

- System design documentation (in terms of capacity of individual trains)
- Plant power history data/records
- System descriptions
- System engineers and operators with their knowledge of system and plant operations
- Maintenance Rule [10] (information developed in support of the Maintenance Rule includes descriptions of functional failures that have occurred or could occur, and their impacts on the system and the plant)
- North American Energy Research Council (NERC) data [11] (the NERC database includes information on Mwh losses associated with equipment outages)
- Technical specifications (e.g., for limiting conditions of operation that may require a plant shutdown)
- Operating, training, and abnormal incident manuals

Figure 2-1 is an example of an FMEA performed for a system. Upon completion of the FMEAs, analysts will have a list of systems cross-referenced with levels of derate that will be included in the analysis. A simple top logic model (as simple as a table, or with more detail such as in “event tree” or “fault tree” format) can then be developed to illustrate what frontline systems are assumed to contribute to each level of derate. Figure 2-2 is an example of a simple top logic fault tree model developed to highlight the failures that contribute to various derate levels. The choice of logic model is representative of the various approaches available for implementing a GRA, ranging from single point vulnerabilities to detailed fault trees with uncertainty distributions.

Component	Failure Mode	Effect	Comments
FW Pump A	Fail to Run	Reduction in load to 60% power	Redundant to FW Pump B; failure of both results in plant trip. Loss of one pump requires operator action to reduce power or reactor trip on low level will occur.
FW Pump B discharge check valve	Fails to Close	No effect with FW train B in service If FW Pump B is tripped, 100% power reduction occurs	FW check is normally open during operation. If FW Pump B is tripped and discharge check valve fails to close, back flow from FW Pump train A will occur and low reactor water trip will result.
FW Train A Reg Valve	Fails to remain open	Reduction in load to as low as 60% power	Each FW train has a 60% capacity FW regulating valve that must be opened to sustain full power operation
FW Train A Reg Valve	Fails full open	Eventual reactor trip on high reactor level	A fully open FW regulating valve can result in high reactor level. Operator can avoid trip by reducing flow from FW Train B.

Figure 2-1
Failure Modes and Effects Analysis (FMEA) – Example

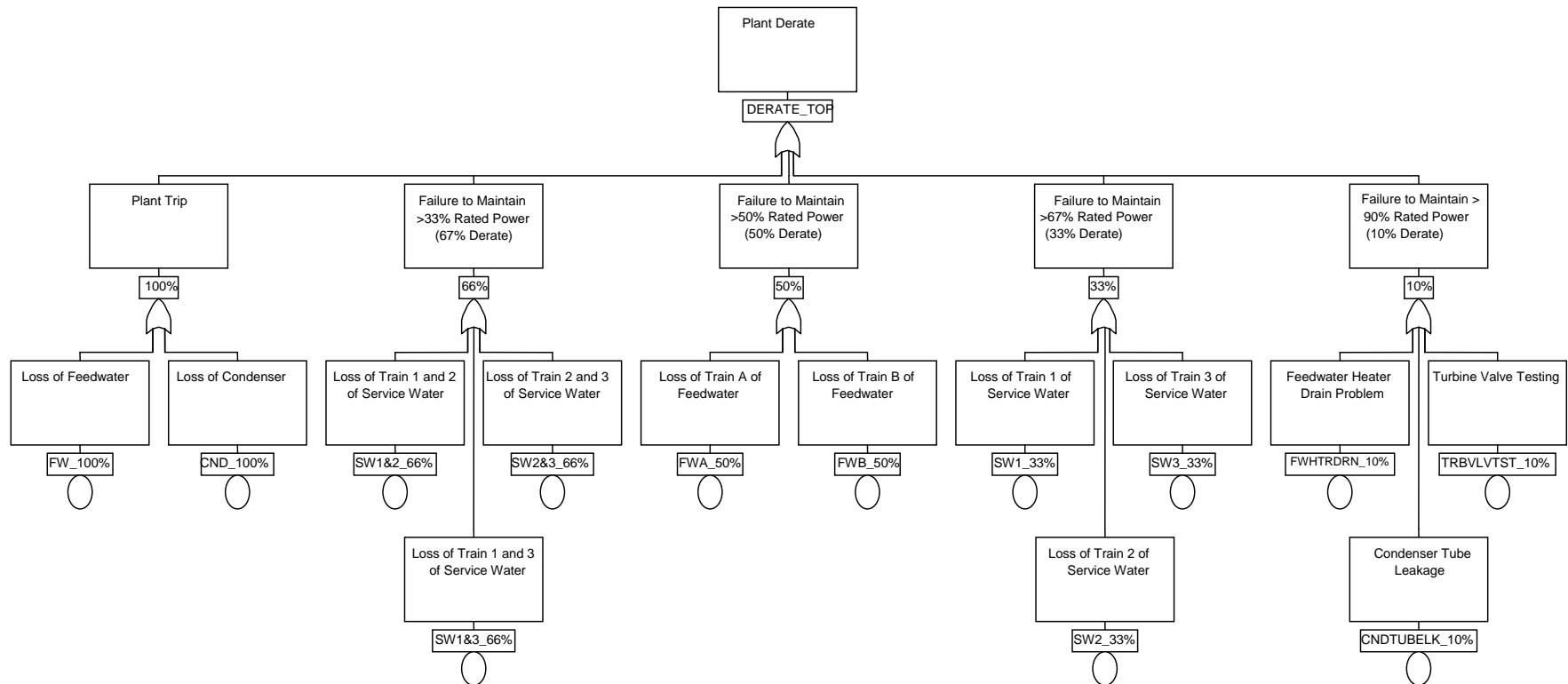


Figure 2-2
Top Logic Model for Delineating Derate Levels – Example

Note that “support systems” can be assigned directly to a given derate category or grouped with the “primary” systems that they support. When a system supports a frontline system for which the derate levels resulting from train failures have been determined, the parts of the support system associated with the frontline system train failures leading to derates can be categorized with the frontline system. This requires an FMEA be performed on the support system – explicitly accounting for the cascading effects of support system component/train failures on frontline system operation. Alternatively, support system logic can be directly linked into the logic of the frontline system if techniques such as fault tree modeling are used. These types of logic modeling techniques automatically result in the appropriate categorization of support system trains and components even if a formal FMEA has been performed only on frontline systems. Using the list of supporting and auxiliary functions in Table 2-1 and associating systems with these functions will assist the analyst making these determinations.

Section 4 of Reference [5] provides an example approach for identifying and prioritizing systems for which FMEAs may be necessary. That approach is generally consistent with the description for identifying systems presented in previous paragraphs, i.e., a series of questions are asked and answered that essentially determine the functions supported by the systems. Other questions address the impact of postulated failures upon the ability of the plant to continue to produce full power. The answers to the questions are used to direct the analysts’ attention to systems that may require additional examination. Section 6.3 of Reference [5] is one example of defining derate categories and assigning system/component failures to those categories.²

When the impacts on power level resulting from component and system unavailabilities are understood, the next step in the GRA process is to determine the frequency of occurrence of those different power levels. That step is accomplished through system models and system analysis (see Figure 1-3). Section 3 provides more discussion on this subject.

² Reference [5] uses a set of system codes within the tables and lists developed and presented in the reference (see for example Table 4-4 of Reference [5]). To avoid confusion, any system or component coding/labeling scheme chosen for use in FMEAs and other logic models must be consistent with the plant’s equipment database and/or the labeling schema employed by the PRA; the codes used in Reference [5] may not be the same as those used by other plants.

3

SYSTEM MODELING AND ANALYSIS

This section of the guide describes approaches to modeling and analysis of systems that have been selected as important for Generation Risk Assessment. The models, when combined with data (Section 4) and consequences (Sections 2 and 5), form the availability models indicated in Figure 1-2.

Models of varying levels of detail may be developed for systems supporting the functions discussed in Section 2 (see Table 2-1). In Section 2, FMEAs were recommended as one approach for determining the effect of system and component failure on important generating functions and to determine power level reductions associated with equipment outages. This information is now used to construct GRA models that are cost effective for plant implementation; i.e. they provide the detail needed to characterize future plant performance (reliability and availability) with reasonable accuracy. (This document recognizes that there is a wide variety of commercial software tools developed by EPRI and others for constructing safety models that can also be used to develop, quantify, and apply GRA. The guide is developed to highlight important considerations in the generation of the models that any of these currently available software packages should be capable of implementing.)

3.1 Selection of Systems for GRA

Although all systems that support the functions important to generation (Section 2) must be included to some degree, the extent to which those systems are examined in detail should consider other factors.

RIAM Related Issues

An obvious influence on the selection of systems to be included in the GRA is the set of issues at the plant for which risk-informed asset management decisions are being sought. These include:

- Selecting optimum proposed/potential plant modifications
- Optimizing preventive and corrective maintenance activities
- Reducing risk associated with human error
- Deciding whether to perform maintenance on-line or off-line
- Analyzing and prioritizing spares procurement

(Table 1-1 contains other examples of RIAM related issues.)

Historic Contributors to Lost Generation

The historical performance of the plant is a major source of information to identify systems that should be included in a GRA implementation. Of course, systems that have resulted in significant power derates as a result of poor performance, excessive maintenance demands, or other reasons, should be considered for inclusion. In this context, “significant power derates” include not only large derates taken as a single hit (e.g., a 33% to 100% derate given system failure), but may also include smaller derates that have occurred many times (e.g., a 10% derate several times within a year).

Some relatively quick and simple reviews can be performed to gain insights from historical operating experience. For example:

- A review of the North American Energy Research Council (NERC) database [11], focusing on data specific to the plant under review, may identify relatively frequent contributors to load reduction, and/or those components or systems that have contributed most significantly to generation loss
- Plant-specific functional failure data gathered in support of the Maintenance Rule can be reviewed to determine what balance-of-plant equipment has contributed to system outages and/or plant derates or shutdowns
- A plant’s operating experience database (e.g., event and trip reports) will highlight significant derate events and provide descriptions as to the causes of those events.

Without an inordinate amount of effort these types of reviews can point out components, systems, or functional areas that warrant more detailed investigations when developing the GRA. As an example, Tables 3-1 and 3-2 are summaries of NERC-GADS information on the top 25 contributors to lost generation for BWRs and PWRs (respectively) for the period 1987 through 2003. The tables highlight systems that on average dominated lost generation (total Mwh) for that period.³

³ To illustrate how helpful information can be generated relatively easily, these tables were produced by using one of the pre-programmed features within NERC-GADS software (Reference [11]). Thus, the tables include all items within the top 25, including normal refueling and other fuel related issues that may not be explicitly modeled within a GRA (these issues may still be important in RIAM applications). NERC and other databases like it provide tools for focusing on areas of interest with little additional effort, once those areas are identified by reviewing output such as in Tables 3-1 and 3-2.

Table 3-1
BWR Top 25 Contributors to Lost Generation⁴ (Unit-Years = 474.58)

Rank	Cause Code ⁵	Description	Averages		
			Occurrences per Unit-Year	Mwh per Occurrence	Mwh per Unit-Year
1	2070	Normal Refueling	0.9693	702,246.78	680,672.42
2	9510	Plant Modifications Strictly For Compliance W/ Reg. Req	0.0632	7,015,289.19	443,463.01
3	4400	Major Turbine Overhaul (720 Hours Or Longer)	0.2507	813,500.70	203,983.70
4	2999	Other Nuclear Reactor Problems	1.7384	51,024.64	88,700.17
5	2900	Reactor Overhaul	0.1222	463,649.14	56,664.10
6	9110	Core Coastdown (nuclear)	1.2769	43,585.92	55,655.67
7	2660	Safeguard Buses And Assoc. Equipment (transformer,, etc.)	0.0674	465,976.27	31,419.87
8	2200	Reactor Coolant/recirculating Pumps	1.1442	26,895.10	30,772.56
9	4099	Other High Pressure Turbine Problems	0.1875	156,862.44	29,417.08
10	2995	Reactor Performance Testing	3.5063	6,976.97	24,463.08
11	2650	Emergency Diesel Generators (inc. Actuating System)	0.0716	275,380.02	19,728.86
12	2510	Main Steam Isolation Valves (BWR and PWR)	0.453	38,641.59	17,505.88
13	9720	Other Safety Problems	0.0147	1,027,354.67	15,153.36
14	2031	Fuel Preconditioning	4.8443	3,073.56	14,889.20
15	9320	Other Miscellaneous External Problems	1.8206	7,812.03	14,222.26
16	3960	Thermal Derating	0.3034	46,846.07	14,214.32
17	2010	Fuel Failure Including High Activity In RCS Or...	2.8193	5,018.06	14,147.59
18	3620	Main Transformer	0.2781	47,142.35	13,112.20
19	3999	Other Miscellaneous Balance-of-plant Problems	0.472	23,700.66	11,186.62
20	3410	Feedwater Pump	0.5605	19,166.64	10,742.82
21	9500	Regulatory (nuclear) Proceedings/hearings	0.0063	1,576,073.79	9,962.96
22	9310	Operator Training	0.0169	580,630.16	9,787.69
23	4499	Other Miscellaneous Steam Turbine Problems	1.3654	7,053.39	9,630.83
24	9590	Miscellaneous Regulatory	0.0211	433,251.61	9,129.16
25	4261	Turbine Control Valves	1.0746	8,176.92	8,787.19

⁴ From NERC database – Reference [11].

⁵ The NERC database uses “cause codes” to categorize reported events as a function of system, component, or other identifier. For more information on the definition of the cause codes, see Reference [11].

Table 3-2
PWR Top 25 Contributors to Lost Generation (Unit-Years = 1009.25)

Rank	Cause Code	Description	Averages		
			Occurrence per Unit-Year	Mwh per Occurrence	Mwh per Unit-Year
1	2070	Normal Refueling	1.2385	666,135.78	825,038.12
2	3960	Thermal Derating	1.2504	49,854.41	62,339.62
3	4400	Major Turbine Overhaul (720 Hours Or Longer)	0.0822	628,643.35	51,699.18
4	9710	Investigation Of Possible Safety Problem	0.0377	1,361,058.79	51,246.21
5	9720	Other Safety Problems	0.0228	2,005,468.50	45,703.02
6	9110	Core Coastdown (nuclear)	1.0225	35,388.76	36,186.48
7	9510	Plant Modifications Strictly For Compliance W/ Regulatory Requirements.	0.0069	4,842,488.60	33,586.74
8	2200	Reactor Coolant/recirculating Pumps	0.319	101,365.63	32,340.58
9	2400	Steam Generator Tube Leaks	0.217	144,302.30	31,312.56
10	2650	Emergency Diesel Generators (inc. Actuating System	0.1011	254,520.47	25,723.15
11	2422	Other Steam Generator Internals Problems	0.1308	192,364.10	25,159.34
12	2370	Reactor Trip System Including Sensors, Logic And..	0.9195	26,190.12	24,081.67
13	2071	Refueling Equipment Problems	0.0218	811,499.86	17,689.37
14	9500	Regulatory (nuclear) Proceedings/hearings	0.0139	1,203,561.26	16,695.43
15	2411	Steam Generator Tube Inspections	0.0575	280,122.43	16,098.19
16	2900	Reactor Overhaul	0.0327	492,173.58	16,092.87
17	9590	Miscellaneous Regulatory	0.0535	286,550.46	15,331.90
18	3520	Extraction Steam Piping	0.0852	162,139.96	13,816.24
19	2599	Other Steam Generator Problems	1.8221	7,366.39	13,422.64
20	3499	Other Feedwater System Problems	0.2834	47,264.41	13,393.73
21	2265	Pressurizer	0.0416	316,946.25	13,189.74
22	9999	Total Unit Performance Testing	0.108	117,063.39	12,642.96
23	2849	Other Auxiliary Feedwater Problems	0.0327	353,372.38	11,554.41
24	2380	Reactor Control System/integrated Control System..	0.1397	82,181.11	11,481.33
25	3620	Main Transformer	0.1932	55,389.91	10,702.04

3.2 Logic Model Development

As indicated previously, there are a variety of approaches that can be used when developing a reliability model for plant systems. The approaches range from simple point value system modeling to more detailed fault tree logic model development. Two general modeling approaches are discussed in this guide:

1. several forms of the “supercomponent” method, where systems and trains are treated as if they are a single (“super”) component in the power plant, and
2. the fault tree approach, where individual system components and their potential failures are modeled using a Boolean logic model called a fault tree.

The principal difference between these two methods is that the supercomponent approaches require less effort to develop than detailed models. However, as will be discussed in Section 7, the supercomponent approach will be more difficult to apply and is likely to be useful in fewer applications than detailed fault tree models.

An important consideration in any approach chosen is the level of detail included in the model. Guidance on this and other issues is provided in sub-sections below for each of the approaches. These sub-sections are aimed at PRA specialists. Non-specialists may wish to only skim the contents of these sub-sections on the way to reading Section 3.3.

3.2.1 Supercomponent Approach

A simple approach to assessing the impact of systems on lost generation is to group components within a system and represent each group as a single entity, called a “supercomponent.” For example, the feedwater/condensate system, comprised of pumps, valves, piping systems, instrumentation and control, etc., could be treated as a single supercomponent (much like a “black box”). The supercomponent has a single failure probability associated with it, representing in aggregate all contributors to loss of the system. Treating systems in this manner is beneficial in situations where information about the impacts on lost generation at the system level is sufficient and resources for performing more detailed analyses may be limited. This approach is useful when decisions are made at the system level, such as allocation of resources to system health assessments, audits and inspections. Basic advantages of this approach are that it is simple to implement and the results are easy to understand. A major disadvantage is that because the analysis is performed at the system level, it lacks the detail necessary to support applications that require component-level generation risk information. Moreover, preventive maintenance and equipment long-term planning are almost always addressed at the component level. Therefore, the usefulness of the supercomponent approach in supporting typical resource allocation decisions faced by plant management is limited as compared to the detailed fault tree modeling approach. Nevertheless, this approach can provide valuable information on generation risk for some plant applications.

Supercomponents can be developed at different levels within a system. As discussed above for the feedwater system, the entire system can be grouped and identified as one supercomponent. Another approach is to group portions of the system together, e.g., all components comprising Train A could be grouped as one supercomponent, while all components of Train B are another supercomponent. Supercomponents can also represent single components with subcomponents and their various failure modes included in the quantification of the supercomponent. Several forms of the supercomponent approach ranging from the system level to the train level are discussed below.

The supercomponent approach shares many characteristics with FMEAs in that, like an FMEA, it examines the impact of postulated train or component failures on the system to which they belong. In fact, it is equivalent to an FMEA if the “failure modes” analyzed within the FMEA are associated with trains and components

Supercomponent Modeling – System Level

The system level supercomponent approach is a simple approach where each plant system determined to impact power generation is modeled as a single entity, whose failure leads to a predetermined derate level (see Section 2 for the discussion on determining derate levels). The failure rate, unavailability, and/or reliability values assigned to the supercomponent are taken from plant-specific information or industry sources such as discussed in Section 4. For this approach it is important that the supercomponent boundary (i.e., the envelope defining which components are inside and which are outside the supercomponent) be as consistent with the data as possible. If this is not done properly the impact of a particular system on lost generation potential may be over or underestimated. As an example, the Feedwater system may be supported by plant air, service water, and electrical systems. However, data on system performance may exclude the supporting systems and focus solely on those systems designated as “Feedwater System” components. Thus, the boundary of the supercomponent must be defined such that instrument air, service water and electrical system components are excluded. A separate supercomponent may be defined for each of those supporting systems. Existing documents or programs such as plant equipment system databases or the Maintenance Rule often provide good guidance for system boundary determination. Given that failure/unavailability of each supercomponent (system) in this model is associated with a derate level (as discussed in Section 2), the lost Mwh can easily be obtained by calculating the product of the supercomponent failure frequency, the change in Mw output as a result of the failure (i.e., the derate), and the duration of the derate.

Supercomponent Approach – Highlighting Single Point Vulnerabilities

The supercomponent method can be further expanded in detail by reducing the boundary of the supercomponents to highlight key components (such as components “critical” for production in the terminology of INPO AP-913). For example, by using the FMEAs developed to determine derate levels (Section 2), two sets of supercomponents can be developed: (1) a set of components, each of which represents a single piece of equipment that, if failed, leads to unavailability of the system to support a given power level (i.e., a “single point vulnerability”), and (2) a supercomponent representing all other components that must fail in combination to fail the system. The finer level of detail in item (1) allows analysts to quickly focus on the single point vulnerabilities of the system when addressing system reliability issues.

The first step in this approach is to identify all single failures in the system that could lead to the inability of the system to maintain a given power level. This should be done at the level of trains or major components, i.e., at the level of valves and pumps, as opposed to piece-parts associated with these components. FMEAs similar to that illustrated in Section 2 can be used to identify these failures. Once the single point vulnerabilities have been identified, individual events are included in the model to represent these particular trains or components. All remaining components or failures can be grouped together and represented by another, single, event. An example of this type of model for the plant is shown in Figure 3-1.

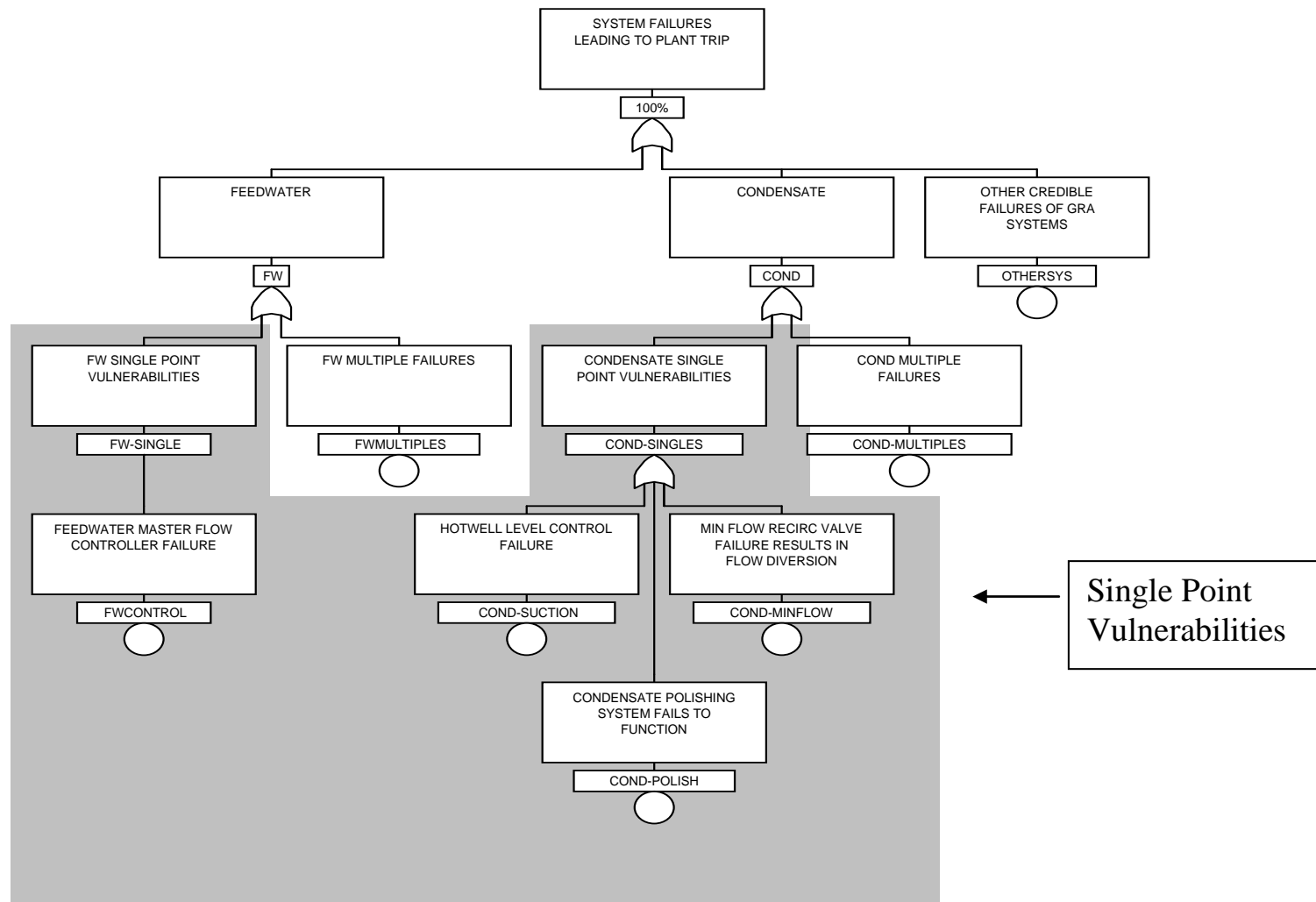


Figure 3-1
A Typical Single Failure Vulnerability Supercomponent Model

Supercomponent Approach – Train Level

The system level supercomponent model can be taken one level downward to the train level, including combinations of trains. This finer level of detail modeling is useful when information regarding the impacts on generation from the train level is desired. Also, because many balance-of-plant systems do not have fully redundant trains, failure of a system train can often lead to a plant derate. As a result, modeling to the train level would be useful in capturing the train's contributions to lost generation.

The FMEAs performed to identify levels of derate will first identify the trains which by themselves, if failed, can lead to a plant derate. These trains are similar to single point vulnerabilities of the system for the associated derate level but are included in the model as supercomponents. Systems trains that do not lead directly to derate or trip are those that require failure of other trains or components to impact plant generation. For these trains, the FMEA will have had to establish the success criteria for number of trains needed in each system to avoid a particular level of derate. For example, a condensate system may be designed with 3 – 50 percent capacity trains and failure of at least two trains must occur to impact generation. Therefore, the failure criteria would be loss of two of three trains for a derate level of 50% and loss of all three trains for a 100% derate. The trains would be included in the model with the failure criteria logic even though a single point vulnerability analysis would not indicate that a derate would necessarily occur. Figure 3-2 shows an example of the train level supercomponent model. The figure illustrates the modeling of a 2-50 percent Feedwater and 3-50 percent condensate train. As shown in the figure, the train failures contribute to two derate levels: 50% and 100%. The corresponding logic for the two top events is illustrated by appropriate combination gates.

As in the system level modeling approach, it is important to define the components in a system train to avoid double counting or excluding component defined in the train. A train typically consists of components in series where failure of any component defined in the train would result in failure of the train. A simple method of segregating components into trains is to use the system piping and instrumentation drawings (P&IDs) typically included in the PRA. The identification of the items that comprise a train should be compared to the components included in the reliability data chosen to represent the train's performance. Wherever possible, the components assigned to a train should match the components included in the development of the data. For example, train-level data from references such as those discussed in Section 2 may include reliability information for pumps and valves, as well as certain motive power (electric, air, etc.) components interacting with the pumps and valves. Thus, for the supercomponent approach, the train level supercomponents should also be defined to include these same motive power components.

Supercomponent Modeling Considerations

An important consideration in supercomponent modeling is to ensure consistency in modeling between the different top events associated with the plant derates. For example, when train level modeling is included as a supercomponent in a derate level top event, it should also be included as a supercomponent in the other derate levels to which the train contributes, even when the train by itself only leads directly to one derate level. This is also the case for component modeling. When a component is identified as a single point vulnerability for one level of derate and broken

out explicitly, then wherever that component is located in the models, it should also be broken out explicitly to ensure that the modeling is consistent across the different load reduction top events, and to properly account for the contribution of the event across all derate levels, including those levels where the event must fail in combination with other events to result in the derate.

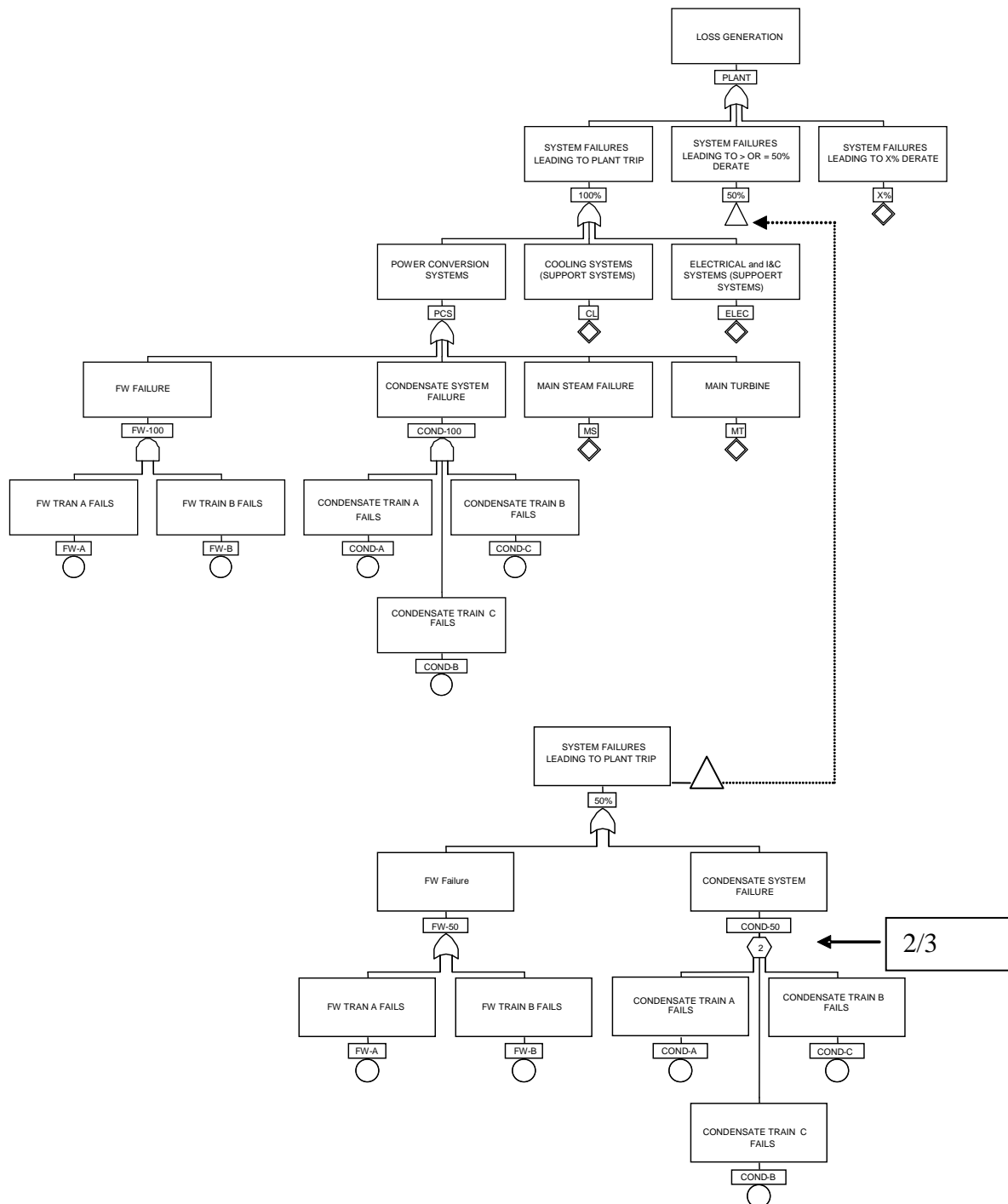


Figure 3-2
Typical Supercomponent Train Level Model

Although the train level supercomponent approach addresses some of the deficiencies in the single point vulnerability or system level supercomponent approaches, it still may lack enough detail for some applications where the focus of generation risk is on individual components. Therefore, detailed modeling of the system may be desired to maximize the benefits of GRA modeling. Detailed modeling is discussed in the next subsection.

3.2.2 Detailed Logic Model Approaches

An even more detailed approach to GRA modeling is to develop reliability logic models of the systems, i.e., fault trees. System fault trees are detailed Boolean models that represent combinations of system component failures that could lead to failure of the system. This approach yields results that provide the broadest applications for generation risk assessments. One of the modeling approaches used in plant probabilistic safety assessments (developed from a safety perspective) that can also be employed in generation risk assessments is the fault tree linking method. Information on and descriptions of the PRA terms and techniques used in this section can be found in such references as “PRA Procedures Guide” [12], “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Application” [13], “PSA Applications Guide” [14], and “Fault Tree Handbook” [15].

The fault tree linking method is widely used in PRAs., primarily due to the advances in solution software and computer hardware capabilities. All inter- and intra-system dependencies are modeled explicitly using this approach Figure 3-3 is an example of a linked fault tree. The downside of the approach is that each support or frontline system is often modeled in detail, and then linked together to create what can be very large and complex fault tree models. The approach can also lead to “circular logic” issues that must be eliminated before solutions can be generated (an example of circular logic is a service water pump that requires AC power to operate, while the AC power equipment requires service water cooling (i.e., pump operation) – failure of “A” leads to failure of “B”, which leads to failure of “A”, etc.).

There are several approaches that can be considered in the development of detailed GRA fault trees ranging from creating them from scratch to modifying existing fault trees from the PRA. For any of these approaches, one tool useful in the development of fault trees is the reliability block diagram (RBD). Reliability block diagrams are a method of portraying a system in terms of blocks of components (pipes, valves, pumps, etc.) that, when they are available, satisfy the function of the system (see the discussion of block diagrams in Reference [5], for example). System engineers are often familiar with RBDs, since RBDs are similar to (but in most cases, simpler than) P&IDs, following the same general flow paths and with the same interconnections. RBDs can be constructed to assist in the development of the detailed fault trees. An RBD breaks the system into parts and therefore allows the analyst to focus on each part of the system one part at a time. Each part of the system or block in the reliability block diagram is typically comprised of a component or a group of components of the same function. Support systems for the components in each block are also identified and included with their own blocks. Once the reliability block diagram is constructed, analysts can convert each of the blocks into a fault tree model by changing the perspective of the RBD from “success” into “failure”. The fault trees developed for each block of the RBD are then combined to form the fault tree for the train or the system. For example, consider an RBD showing that any one of three paths can satisfy the function (in other words, the success criterion is “one out of three”). In this example, all three

paths must fail for the function to not be satisfied. The RBD with success being defined as “one of three paths in operation” is converted to a fault tree with failure defined as “three of three paths unavailable.”

The following subsections present some of the different approaches to fault tree development.

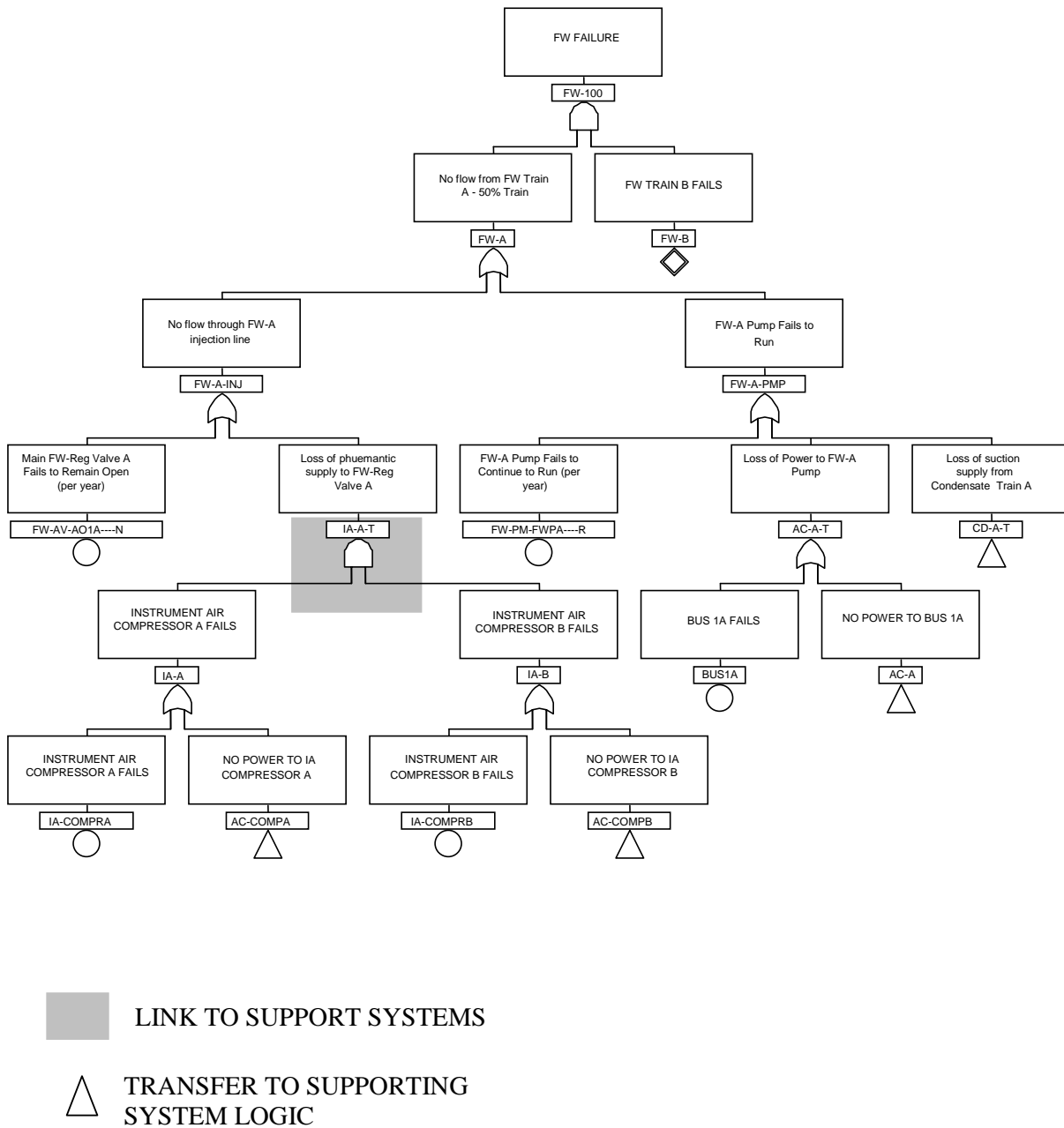


Figure 3-3
Example of Fault Tree Linking

3.2.2.1 Generating New Fault Trees

Whether developing new fault trees or modifying those that already exist, it is worthwhile to consider the following for each system:

- Success/failure criteria and corresponding definition for the fault tree top event
- Level of detail, including consideration of:
 - Instrumentation and control (I&C)
 - Flow diversion
 - Active and passive failures
 - Common cause failures
 - Human error
 - Test and maintenance unavailabilities

Failure criteria and top event definition

For GRA, the purpose of a system's operation is to perform its function to maintain plant electrical output at full power. In a nuclear power plant, a variety of normally operating systems function collectively to fulfill this purpose. Because each system is designed differently and performs specific functions for power production, each system's impact on plant output will be different. Therefore, the first step in fault tree modeling is to define system failure criteria for power generation. Unlike safety systems where there may be just one system failure criterion for accident mitigation, balance-of-plant systems in a GRA model generally have more than one failure criterion due to the partial system failure impacts on plant electrical generation. This is the case, for example, for multiple train systems wherein each train is designed to support less than 100% full power operation. Failure of a train would result in a plant derate that generally corresponds to the power level supported by the train (e.g., failure of a 50% feedwater system train generally results in a 50% derate). Therefore, it can be worthwhile to develop models with multiple top events representing the different failure criteria for the trains and components that make up the system. For the purpose of GRA system modeling, the failure criterion of a system is defined as a failure or a failure combination leading to *the inability to maintain a power level greater than or equal to x% (or a derate level of 1-x% or more)*. This definition is important given how these models are generated and quantified. More discussion on this definition as it pertains to getting results can be found in Section 5.

Frontline systems (systems supporting primary functions)

The FMEA method of Section 2 provides one means of identifying success/failure criteria for systems performing frontline or primary functions supporting power generation. Each train of a frontline system should be evaluated for its impact on system failure and on plant generation capacity. Continuing with the hypothetical two feedwater train system with each train supplying 50% of rated flow to the reactor (BWR) or to the steam generators (PWR), a failure of both trains would lead to a plant trip, while failure of either one of the two trains would lead to a 50% plant derate. Thus, this system would have two failure criteria: (1) plant trip requiring failure of both trains, and (2) 50% derate requiring failure of either train. A fault tree with two top events representing these failure criteria would be developed.

Support systems (systems supporting frontline or other support systems)

Failures of support systems may lead to plant trip or derate through failure of the frontline components which they support. There are two options available for modeling support systems:

- The first approach is to create a top event for each level of derate that can result from failure of a train or collection of components that make up the support system, much in a manner similar to the frontline systems. This requires performance of an FMEA for each train or component making up the support system, cascading the effects of the postulated failures into each of the frontline systems that they support to determine the final effects. A fault tree top event would then be developed for each of the levels of derate that would result from the failures of the supported frontline systems.
- The second approach requires linking the support system directly into the frontline system logic, much in the way that is performed for the safety models of the PRA. With this approach, the effects of support system train and component failures are cascaded through the frontline system models as a part of the model solution, directly capturing the effects of these failures through the frontline systems.

Creating a top event for each of the support systems has advantages in that model changes, debugging, and breaking of logical loops do not have to be performed as they would if the support systems were directly linked into the frontline fault trees. The fault trees are smaller and require less effort to assure consistency when integrating the results. A detailed FMEA is required for each train, however, and sometimes for individual components to assure that the effects of individual failures are taken into account appropriately. Where crossties exist that make operation of the frontline systems relatively independent of specific trains of a support system, it may be simplest to create appropriate top events for each support system in this manner. However, where there is not a structure to a support system that has a well defined effect on frontline system operation or where individual components can have a variety of impacts on multiple frontline systems (e.g., AC and DC electrical distribution), the effects of failures or combinations of failures can be inadvertently overlooked by attempting to develop top events for some support systems.

Linking a support system directly into the frontline systems that it supports avoids the need to develop explicit failure criteria with respect to generation for that system because the criteria are already defined by the logic of the frontline systems. For example, an AC bus may provide power to many components, some of which would result in various levels of derate if they were to be lost and others that may lead to plant trip without operator intervention. By linking the dependency on this AC bus directly into the frontline system components that it supports, the effects on load reductions and plant trips are taken into account directly in the frontline system models. There is no need to create individual models that contain this AC bus for each level of derate that it may cause or to perform detailed FMEAs for support systems. Further, combinations of failures between systems that may lead to plant trips or derates are appropriately captured if support systems are directly linked into their associated frontline systems.

Auxiliary systems

As described in Section 2, an auxiliary system supports a function that is neither directly related to power production nor supporting functions that do. However, failure to maintain these systems will result in other equipment degradation that eventually results in power derates (including trip).

Modeling these systems can be performed using the approaches described for support systems. However, auxiliary systems typically interact directly with the reactor or (for PWRs) the steam generator, and therefore there may be no linkage to frontline systems. Impacts on plant trip or derates are also usually slowly evolving (e.g., such as due to poor water chemistry). Addressing these systems through the use of FMEAs and the supercomponent approach may be the most effective use of time and resources, at least for initial GRA implementations. If early GRA results indicate that auxiliary systems may play an important role in lost Mwh, more detailed modeling can be completed on the systems.

Regulatory systems

A system that supports a regulatory function (see Section 2) and that is not already treated as a frontline, support, or auxiliary system can be assessed using any of the aforementioned approaches. A primary distinction between these and systems that fall into the frontline and support system categories is that there is no uncertainty about the window of opportunity available to repair/restore the system to full operation, i.e., the amount of time available is explicitly defined by the limiting conditions of operation (LCO) delineated in the technical specifications for the equipment and system. For systems in the other categories, the amount of time available to restore the equipment is dictated by the mean time to repair and return to service the component that has failed.

Failure to restore the regulatory system to operation before the end of the time allowed by the LCO typically leads to a manually initiated plant shutdown or derate (as specified by the directives of the technical specification/LCO).

Because many systems that fill regulatory functions are not required to support power generation, the amount of effort allocated to constructing detailed system models for regulatory systems can be driven by the historical contribution of these systems to LCO-dictated derates attributed to system outages. In other words, if plant records reveal that a regulatory system has, as a result of its unavailability, resulted in numerous plant shutdowns or derates, this system may warrant detailed logic modeling such as appropriate for a frontline system. However, if the impact has been minimal, the supercomponent or point value approach may be a reasonable starting point.

Level of Modeling Detail

As mentioned at the outset of Section 3.2, an important consideration in GRA modeling is to decide to what level of detail one needs to model. In theory, detailed models produce results that can be used in more ways (i.e., in more applications) than simple models. However, generating very detailed models can be resource-intensive and may not yield corresponding benefits. Therefore, even when considering the development of detailed system models it is important to select the level of detail for modeling required to support the projected use of the models within the constraints of the resources available.

The level of detail for modeling should be based largely on the proposed application of the results. As an example, for resource allocation planning it may be necessary to model only to the system or train level. For preventive maintenance activity planning, modeling to the major component level may be of value, since preventive maintenance is typically performed at this level. For GRA purposes, it is recommended that detailed models go no lower in detail than the major components. Since a major goal of GRA is improving equipment reliability, thus minimizing plant trips and derates, obtaining results at the major component level will often provide sufficient discrimination for this purpose.

A second consideration in determining an appropriate level of model detail is the availability of data for the systems and components, and the relative significance of the components/systems to plant generation risk. For example, it is not necessary to model a pump down to the bearings and control circuit contacts if the only data available has been collected at the gross “pump fails to start” level. In this case, failures of the subcomponents of the pump (bearings, control circuitry, etc.) are considered to be encompassed by the “fail to start” value. The data that are generally used in safety assessments include that for major pieces of mechanical and electrical equipment such as pumps, valves, compressors, motors, buses, batteries, battery chargers and motor control centers. The data sources in Section 4 should be consulted when deciding the level of detail to include in the model. Often, iteration between the model and the data is necessary before reaching a final solution.

Data can also be helpful in determining what to model based on relative importance or significance. For example, passive components are generally much more reliable than active components. Passive components such as pipes, non-pressurized tanks and manual valves may be eliminated from further consideration unless credible evidence has shown that they are bad actors. Programs such as the Maintenance Rule and INPO AP-913 can be used to screen passive component failures.

The level of detail to be included influences the amount of effort spent modeling various aspects of component and system operation, and vice versa. The following general guidance is provided for particular types of components:

Instrumentation and Control Failures

Because most normally running systems are controlled by automatic control systems consisting of instrumentation and control (I&C) components, and experience in PRA has shown that I&C can be a significant contributor to initiating event frequency, it may be worthwhile to consider important I&C in GRA modeling decisions. However, experience has also shown that modeling of instrumentation and control equipment can be difficult and labor intensive and the benefit is not always directly proportional to the resources spent. Therefore, the following items should be given consideration:

- Give priority to I&C failures that have historically impacted plant generation (Table 3-3 provides a listing of initiating events for the period 1987 to 2003 including estimates of that fraction that can be attributed to I&C; this table was developed using information available in NERC that associates derates with I&C cause codes).
- Within a priority system, consider modeling only I&C that affects multiple redundant trains.

- When a priority I&C system that affects multiple redundant trains is identified, FMEAs or importance measures for components affected by I&C can further help to manage the effort required for modeling.

Even when incorporating I&C into detailed models, using supercomponents to represent I&C elements should be considered to limit the effort needed to develop the models.

Table 3-3
Contribution of I&C Failures to Trip and Derate Frequencies for PWRs and BWRs⁶

Initiating Event – PWRs	Freq ((unit-yr) ⁻¹)	% I&C Initiated	Initiating Events – BWRs	Freq ((unit-yr) ⁻¹)	% I&C Initiated
Transients			Transients		
Transient with PCS	1.6	27%	Turbine/Reactor Trip	1.6	19%
Transient with loss of PCS	0.11	5%	Loss of Main Condenser	0.12	12%
Loss of Feedwater	0.31	12%	MSIV Closure	7E-2	10%
			Loss of Feedwater	0.18	16%
Support System Failure			Support System Failure		
Loss of Offsite Power	0.11	22%	Loss of Offsite Power	0.15	9%
Loss of Instrument Air	7.9E-3	negligible	Loss of Instrument Air	2.5E-2	negligible
Loss of Service Water	4E-3	negligible	Loss of Service Water	1.3E-2	negligible
Loss of Component Cooling	1.3E-2	negligible	Loss of Component Cooling	2.1E-2	negligible
Loss of an AC Bus	9.6E-2	24%	Loss of an AC Bus	8.6E-2	41%
Loss of a DC Bus	1.3E-2	8%	Loss of a DC Bus	4.2E-3	negligible

Flow Diversion

The potential for flow being diverted from the system main flow path is another possible consideration in GRA system modeling. A significant flow diversion could reduce the performance of the system and impact the generation capability. However, flow diversions may be low probability events. Therefore, it is important to consider the following:

- The diameter of the flow diversion line compared to the diameter of the main flow line. If the flow diversion is greater than $x\%$ of the main path, then it should be included a credible flow diversion path (“ x ” can be chosen by the analysts; it is typically on the order of 10-15%). Note that some balance-of-plant systems may be designed with greater than $x\%$ flow diversion margin.

⁶ Developed using data from Reference [11] (NERC) for the period 1987 to 2003.

- The number of valves in the flow diversion path. The probability of experiencing an inadvertent flow diversion in a line containing more than one normally closed valve is considered to be insignificant and therefore should not be given high priority unless there is a high potential for a common signal resulting in their repositioning.
- Backflow through idle trains has been known to lead to inadvertent trips. Consideration should be given to modeling these flow diversion paths if it is routine practice to rely on a single valve (such as a check valve) to isolate a train when it is removed from service during operation.

Active and Passive Failures

Past risk assessments generally have shown that a majority of passive failures do not contribute very much to risk relative to active failures and therefore can be left out in detailed modeling. However, there may be exceptions (such as certain passive components that have a history of significant leakage, like heater drains or condenser tubes). Where historical evidence of lost generation due to passive failures exists, it may be worthwhile to include these failures into detailed models.

Components that provide an active function in supporting power operation are candidates for inclusion into the GRA model (e.g., a valve must change position or a pump must run). Where an active component only supports another single active component, the supporting component may be considered to be a part of the component it supports (e.g., a breaker that provides power to a pump motor). Active components that only need to remain in position to support operation may not be necessary to model unless they have a default or fail safe position that would result in a load reduction or trip were failure to occur (e.g., a normally closed air operated valve that fails open on loss of air and would cause significant flow diversion).

Common Cause Failures

Multiple failures of like components due to common failure mechanisms are also potentially important considerations for GRA modeling. Past nuclear operating experience has shown that these failures could be significant contributors to system failures. The aim of common cause modeling is to capture multiple failure dependencies that are not explicitly modeled (such as occurs when modeling support system dependencies). Some of the more important common cause failure mechanisms that lead to multiple component failures are design flaws, manufacture and construction inadequacies, procedural inadequacies, maintenance, test and operational human errors, and common environmental stress. Multiple components that are subjected to any of these mechanisms may be candidates for modeling.

Because nuclear power plant systems are designed with redundancy in mind and contain similar components, it may be difficult to include all potential common cause events. Therefore, the following guidance is recommended for GRA common cause modeling:

- Include only major active components in the common cause modeling. Examples are pumps, compressors, motor or air operated valves.
- Include common cause events within a given system. Although the common component types are used throughout the plant, they are often subject to different operating conditions,

maintenance and environment. While similar in design, these components may not be subject to common cause failure mechanism unless there is credible evidence from operating experience that they could be subject to common failure mechanisms such as similar operating conditions, maintenance and environment. Absent this evidence, common cause modeling across systems need not be included.

- Include only one basic event to represent common cause failure of any size common cause component group. Common cause modeling can become labor intensive when the component group size is large (4 components and above) because all combinations of failures up to n components must be included (where n represents the number of like components). A simplified approach is to include only one basic event in the logic model to represent common cause failure of the entire component group. This is similar to what is known as the “beta factor” estimate in common cause failure modeling terminology. A beta factor is estimated to represent the conditional probability of all components in the component group failing given one component has failed. Sources for estimating beta factors are discussed in more detail in Section 4 and Appendix A.

Human Errors

Two types of human errors are credible in GRA: (1) errors that cause a system failure or system degradation and (2) errors in responding to a failure, where such errors themselves result in system failure or system degradation. The former involves an inadvertent action performed by plant personnel that causes a system failure or degradation in performance and will most likely be a result of errors that occur during routine maintenance or operating activities around the plant. The latter human error type is an operator failure to properly respond to system component failure in a timely manner to avoid system failure and would likely be an omission of actions found in plant operating procedures or covered in training. Data sources for estimating human error probabilities are discussed in Section 4.

Mission Time Considerations

In the development of detailed fault tree models for GRA purposes, it should be recognized that a variety of mission times may be considered for components that support operation of the plant. The appropriate mission time depends on the role that the component plays in achieving a particular derate or plant trip.

- Single point vulnerabilities

Components that, by themselves, lead directly to derate or plant trip will need only a single mission time for the top event associated with that level of derate (e.g., a mission time of a year).

- Standby components

Components that are not normally running, but are in standby during normal operation would appear only in combination with other failures that must occur before the component in question would be required to support operation. The mission time for a standby component would best be the mean time to repair of the component that must fail before the component in question is needed (e.g., 19 hours for a pump or 6 hours for an electrical component).

- Normally operating, redundant components

Components that are normally operating but would not, by themselves, lead to a plant trip or particular derate may need to be assigned one of several mission times. An annual mission time would be required if the component were assumed to be the first failure among several that are needed to lead to a plant trip or particular derate. If a redundant component is assumed to trigger the multiple failures needed to lead to a plant trip or derate, then the component in question would ideally be assigned a mission time associated with the mean time to repair of the triggering failure.

Theoretically it is possible to rigorously incorporate the above mission time assignments into the fault tree models. However, experience gained from working with PRA models has shown that such modeling changes is likely to be impractical, as the effort can be resource-intensive, complex, and can result in models that are difficult for fault tree solution codes to handle. Thus, to facilitate fault tree model construction and solution, simplifying assumptions are often made to approximate the appropriate mission times for the events that make up a GRA model. Post-processing of the cut set results is then used to address any issues arising as a result of the approximations (see Section 5.1.2).

Examples of these mission time approximations follow.

- Assign all mission time events an annual frequency

The advantage of this approximation is that it can be implemented easily simply by assigning an annual mission time in the data base for the fault tree software being used to solve the problem. It needs to be recognized that this approach can over-estimate or under-estimate the frequency of a given top event. The over-estimation occurs because for cut sets having two or more events with this mission time, it is essentially being assumed that continued plant operation would be attempted with no repair or recovery performed if one of the components failed (e.g., each component is assumed to have to run for a year to avoid a trip or a derate, rather than running for the time required to repair the first component that failed (i.e., the mean time to repair that component). It can under-estimate the frequency in that there are actually multiple combinations of the failures that make up these cut sets that can lead to the top event, not just one as would be produced by the fault tree. Whether this approximation introduces significant error into the analysis depends on whether there are single event failures that drive the frequency of the top event and the magnitude of λ (the hourly failure rate) for the components in question.

- Assign all mission time events a 24 hour mission time and adjust the top event frequency with a correction factor

Existing PRA models generally use a 24 hour mission time.⁷ If these models or their cut sets are used as a basis for GRA modeling, a much longer mission time must be used (e.g., a year). Transformation of the PRA mission time can be accomplished by taking the product of

⁷ For safety models, the effects of all failures that could occur within the first day following a plant trip are considered. The activities and events of these 24 hours generally identify the need for all systems and functions that must be successful in order to reach a safe stable state.

a 24 hour mission time model with a correction factor representing a year (365). It can also be applied to a 24 hour mission time model simply by taking the value for the top event and multiplying it by a factor such as 365. The advantage of this approach is, again, that it is simple to implement. Further, it avoids the potential for multiple annual frequency events appearing in a cut set. It has, however, the disadvantage of underestimating the frequency of the top event where multiple combinations of mission time events appear in cut sets. Further, the assumption effectively is being made that all events have a mean time to repair of 24 hours, where the actual mean time to repair may be greater or less than this. Again, the significance of this approximation depends on whether the top event in question is dominated by single failures that would not be affected by these approximations.

- Incorporate both annual and mean time to repair mission time events directly into the model for each component.

The advantage of this approach is that it directly addresses the issue of assuring all combinations of annual and mean time to repair mission time failures will be produced by the fault tree model. Further, any cut sets having multiple annual mission time events can be considered to be illogical and deleted from the cut sets. The disadvantage of the approach is that systems with significant redundancy can produce a large number of illogical cut sets, which can take time to generate as well as delete with a cut set post processor.

- Create a surrogate event for each component representing either an annual or a mean time to repair mission time to be assigned during post processing of the cut sets.

The advantage of this approach is that the fault trees are smaller, simple to solve and generate no illogical cut sets. The approach directly precludes multiple annual mission time events from appearing in the results. The principal disadvantage is that a cut set post processor is required to expand the cut sets and produce the appropriate combinations of annual and mean time to repairs events needed to estimate the frequency of the top event.

The method of assigning mission time that is most appropriate for use in producing GRA models depends on the degree of accuracy considered to be needed for the applications to be performed using the models.

3.2.2.2 Conversion of Existing PRA Fault Trees

When a PRA includes balance-of-plant models, such models are developed to evaluate accident mitigation. The systems are typically modeled by assigning a 24-hour mission time, as the consequences of all equipment failures occurring within the first day of a plant trip are generally considered when evaluating the potential for core damage or containment failure. It is not unusual for PRAs to include models for the balance-of-plant systems listed in Table 3-4. Note that there are balance-of-plant systems associated with power production (and thus important to GRA) that are not included in Table 3-4 because they do not have any impact on accident mitigation (e.g., turbine/generator).

Table 3-4
Balance-of-Plant Systems that may be Modeled in PRAs

Feedwater/Condensate
Main Steam (MSIVs)
Main Condenser and Condenser Vacuum
Circulating Water
Service Water or Cooling Water
Closed Cooling Water
Instrument Air
Switchyard
Electrical – non-safety AC distribution
Electrical – non-safety DC

The appropriate level of effort required to convert the models associated with the systems in Table 3-4 will of course depend on the success criteria employed for and the level of detail included in the PRA version of the models.

Many PRAs use point estimates to represent system failures that cause a plant trip (these are known as initiating events). Their values are based on a combination of plant-specific and generic data. The Feedwater System is an example of a system modeled both as initiating event and as a mitigation system in a typical PRA. Initiating event models developed for PRA only address plant trip; therefore, such an approach if utilized in GRA modeling must be expanded to include derates of less than 100% power generation. The following changes must be made to convert PRA mitigating system models to GRA models (the factors listed for consideration when developing new fault trees should also be reviewed if converting existing trees to ensure that no issue has been overlooked during the conversion):

- Failure criteria: Convert top logic to reflect the failure criteria defined for GRA (e.g., where only a single train is necessary for accident mitigation, multiple trains may be needed to keep the plant in operation).
- System status: Some balance-of-plant systems may be assumed to be in configurations for accident sequence evaluation that are not representative of the normal operating state (e.g., injection through low flow bypass lines as opposed to full flow lines with regulating valves as for Feedwater). Therefore, the models must be reviewed to remove failures that may not have an impact when the system is in its “normal” at-power state and to add those failures that were not considered in the development of the accident mitigation model.
- House events: House events are basic events used to turn logic on and off during fault tree quantification. Many of the house events represent the effects of initiating events. Some PRA fault tree models for balance-of-plant systems contain house events that must be removed for GRA modeling purposes.

- **Common cause:** Most PRA models include common cause events in their models. The level of detail depends on the common cause method used. As discussed earlier, a simplified common cause model is recommended for GRA modeling (beta factor model). Where a finer level of common cause modeling is included in the mitigating system models, they may be removed to simplify the GRA model.
- **Instrumentation:** Some balance-of-plant equipment receives actuation signals from safety systems on specific accident conditions (often to isolate or place the system being modeled into a state that would not support full power operation). PRA models may contain operator actions to override these signals and place the system back into service. Where this modeling exists, it can be removed leaving only the logic that supports the system remaining in service.
- **Human actions:** human actions modeled in the PRA for balance-of-plant systems must be reviewed to determine if the action is appropriate for GRA purposes. Quite often, actions included in the PRA will be for accident mitigation purposes and can be eliminated from the model (realignment of a system isolated following a trip). Conversely, many actions that would prevent a system from contributing to an initiating event may not be included in the PRA models and would have to be added (reduction in reactor recirculation flow in a BWR to prevent a reactor trip on loss of a train of feedwater).

Other PRAs have expanded the single event initiator model into initiating event frequency models (e.g., fault trees) that can be modified for GRA use. Where this modeling exists, many of the changes listed above may have already been completed. As these models are directed at estimating the frequency of plant trips, all that may be missing for GRA purposes is additional top logic to reflect partial load reductions.

3.3 Sources of Information for Selecting Systems for Detailed Modeling and Analysis

Sources of information that may be helpful in determining which systems are candidates for more detailed modeling and analysis include many of those used in the initial determination of categories of derates (see Section 2). Others supplement those sources. Among those that should be utilized are:

- **System engineers**
 - The system engineers should have perhaps the best “as operated” information about the systems of concern. If the engineers have not already been approached (for example, during the development of FMEAs), they should be engaged at this stage of model development. Engineers will provide information useful in addressing issues such as the following:
 - a. How systems are designed and operated, including limitations, operating ranges.
 - b. How systems are impacted by different failures (i.e., for development of FMEAs)
 - c. How systems are maintained.
 - d. Estimates of mean time to repair (MTTR), and estimates of the time required to restore the plant to full power once repairs are completed.

- Operators
 - The extensive expertise and information that operators have about plant behavior and response will be extremely useful. Operators can help address issues like:
 - a. Their response to a failure that leads to plant derate, including the impacts of training and procedures on the ability to recover (this is useful for the human reliability analysis).
 - b. Validation of the derate levels derived from the FMEAs.
 - c. Validation of component operations, such as how components are operated, rotations between trains, etc.
 - d. Operating experience of BOP systems.
 - e. Potential system vulnerabilities observed, and opinions about system and component problem areas.
- NERC database (e.g., detailed information on specific systems, components, cause codes)
 - By using search and sorting criteria within the NERC database analysts can “drill down” to extract information for specific components and failure modes. Information at higher (summary) levels can also easily be derived. Comparisons with other plants within the industry are also possible.
- Plant-specific PRA
 - As noted above, PRAs contain balance-of-plant (BOP) systems that impact accident mitigation. In some cases, the behavior exhibited by components in the BOP systems following an accident may have an impact on power operation during non-accident situations. Thus, the PRA models may be directly applicable to the GRA since they may already include important failures, or, with proper modification (e.g., to include success criteria and failure mechanisms appropriate for power reduction), can be transformed into GRA models. The PRA and its accompanying documentation will contain significant amounts of information about plant behavior and operating characteristics of direct relevance to the GRA.
- System notebooks
 - Often prepared by, or with input from, system engineers and/or PRA analysts, these notebooks may contain substantial detailed information about specific systems.
- Operating and Vendor Manuals
 - These will provide information about the system(s) that may not be found in other sources, including information concerning maintenance intervals, etc. For example, vendor manuals may provide more detailed information design and operating limits that prove useful in a GRA.
- Piping and Instrumentation Drawings (P&IDs)
 - For information about system configuration and system dependencies/interactions

Once models are developed to the level required to support the GRA applications, failure rates and unavailability information must be incorporated in order to generate numerical results. The next section discusses sources of data useful in supporting a GRA.

4

INPUTS AND DATA SOURCES

To produce numerical results using the models developed in earlier stages of the evaluation requires the assignment of reliability and unavailability data to the model events. This section discusses the types of data needed, various sources for obtaining data, and, in cases for which results are greatly influenced by data, how data uncertainties can be characterized.

4.1 Types and Accuracy of Data Required for a GRA

In general, a GRA model may need the following types of raw data to predict lost generation:

- Random failure events
- Common cause failure events
- Test and maintenance unavailability (i.e., routine/scheduled system and component tag-out)
- Repair time
- Recovery time (to restore plant to power following load reduction)
- Human reliability
- Magnitude of derate (load reduction)

Sources of information for each of these types of data (plant-specific as well as generic) are discussed in this section. Development of this information for both the supercomponent and detailed modeling approaches is outlined. Because some sources provide just raw data (such as number of failures and number of demands), while others provide calculated failure rates, each source type is addressed.

Assembly of data for the purpose of quantification of risk models can be resource intensive. It has sometimes been perceived as being one of the more critical tasks in completing a risk assessment. In addressing this perception, it is important to recognize that the failure probability is not an inherent property of a component that can be plugged into the model and be expected to closely represent its actual performance in the plant. Even for data that is fairly well characterized, it is not unusual to have situations for which the uncertainty in the failure rate of a component may be as much as a factor of 3 to 10.

Therefore, in planning the resources for the data collection task, a decision must be made as to how much precision is needed in the failure rates assigned to components, human actions, and repair and recovery activities, and, in addition, how the uncertainties should be addressed. For a GRA model, this decision depends strongly on what application it is being used for.

Table 4-1 lists a spectrum of potential GRA applications (adapted from Section 1) with comments regarding data needs for each. For the majority of applications, whether extensive plant-specific data is available or generic order-of-magnitude figures are used would likely have little effect on the decisions made. There are, however, a handful of applications for which data that closely represent the actual performance of the components in question may have great effects on predicted generation loss. Even then, not every component represented in the plant model will require precise data to reach an appropriate decision. It is likely that the components whose behavior drives the decision, and hence for which the best available data is needed, will be those which by themselves also drive the predictions of lost generation (e.g., components that make up single trains of equipment which can lead to trips or derates if unavailable).

Table 4-1
Data Effort for Sample GRA Applications

Application Type	Data Requirements
Prioritization activities	
Capital spares procurement analysis and optimization Quality assurance audit prioritization Operating/maintenance procedure training prioritization Station major maintenance activity prioritization Project prioritization Component prioritization Preventive/Predictive/Corrective Maintenance prioritization Operating experience review	Order-of-magnitude estimates
Determination of risk tradeoff	
Trade offs between online and offline maintenance Major equipment refurbishment/replacement/repair decisions & optimization Refueling outage schedule and duration optimization Online/shutdown tradeoffs given equipment degraded performance	Order-of-magnitude estimates Relatively rigorous data
Knowledge of absolute risk	
Trip monitor Bulk power trading	Order-of-magnitude estimates Relatively rigorous data
Demonstrate cost-benefit	
Equipment design modification optimization Capital improvement assessment	Moderately accurate data if results are near cost-benefit threshold
Procedures/training activities	
Treatment of risk from human errors O&M procedure improvement	Order-of-magnitude estimates
Life cycle management	
LCM planning at the plant level Component aging and aging management Component obsolescence management	Order-of-magnitude estimates
Corporate decision making	
Insurance Business plan optimization Mergers and acquisitions	Order-of-magnitude estimates

Regardless of the effort that will ultimately go into the data collection task, model making can begin with whatever sources of data are readily available. Development of the models to accurately reflect the design of the plant and its response to equipment failure or degradation will in general have a more significant influence on the results of the applications listed in Table 4-1 than will the failure rates used to quantify the models. For many components, the failure rates applied in the models will have only a secondary effect, and the effort needed to add additional accuracy to (or gain additional confidence in) the data and the derived failure rates can await the determination of which components drive the results of the models. There is not an exact science to determining when or if such effort is required. However, sensitivity evaluations can be performed by varying the failure rates of the components in question (upward and downward by one or more orders of magnitude) and determining the impact on the overall results; if a large swing in results that changes the decision under consideration is observed, additional effort toward confirming data may be required. Conversely, if little change is noted even with a large variation in failure probability, additional effort is probably not warranted. Importance measures (discussed in Section 6) are very useful in focusing in on components that drive risk. These importance measures also help identify the sensitivity of the risk results to variations in component unavailabilities and failure rates.

4.2 Sources of Data

The models developed to support the GRA may include a variety of component types as well as failure modes. In addition, the level of detail of the models may warrant the development of failure data for groups of components representing trains or entire systems. Appendix A provides an in-depth discussion of the following data topics and gives references to facilitate data searches:

- Random failure events
 - Plant-specific and generic failure rates
 - Plant-specific and generic raw failure data
 - a. Including derivation of failure rates from raw data
- Common cause failure events
 - Plant-specific and generic failure rates
 - Generic raw failure data
- Maintenance/test unavailabilities
 - Plant-specific probabilities
 - Plant-specific raw data
- Repair
 - Plant-specific and generic repair rates
 - Plant-specific and generic raw data for repair times

- Human reliability analyses (HRAs)
 - Plant-specific sources
 - Choosing screening values for human error probabilities (HEPs)
 - Generic HRA methodologies
- Recovery times
 - Recovery times: plant-specific and generic sources
 - Raw data: plant-specific sources

EPRI is developing the Nuclear Asset Management Database using LAMDA software [26] to make GRA data readily accessible to plant staffs.

5

QUANTIFYING GRA RESULTS

The GRA modeling described in Section 3 provides both quantitative inputs and qualitative insights to decision making. Among the useful outputs from quantification of GRA models are estimates of the *likelihood of load reduction or plant trip*, the corresponding consequences in terms of future *lost generation*, and a measure of the *relative importance* of each system, train and component's contribution to lost generation.

The generation risk measures for components, trains, systems, units and the plant as a whole are obtained by quantifying the GRA models described in Section 3 using reliability and generation data from sources such as those discussed in Section 4. This section describes the quantification methods associated with the two general modeling and analysis approaches. Quantification techniques for producing a *frequency* for each level of derate or plant trip is first presented. This is followed by methods for assignment of consequences to the frequency results to produce an estimate of the potential for *lost generation*.

5.1 Quantification of the GRA Models in Terms of Event Frequency

The quantification method used in GRA varies with the type of models developed. Understandably, simpler models like those described for the supercomponent modeling methods are easier to quantify than more detailed models such as those developed at the component level (i.e., fault trees). The following subsections discuss the methods used to quantify the *supercomponent* and *fault tree* models.

5.1.1 Supercomponent Model

There are two levels of detail that can be taken here: *system level* supercomponents and *train level* supercomponents.

Quantification of the *system level* supercomponent model is relatively straightforward. The system failure frequencies are obtained directly from plant-specific or related generic data as described in Section 4 and summed to obtain the total frequency for each load reduction. The calculation can be performed in table format with a calculator or in a spreadsheet. The frequency of failure is generally measured in occurrences per unit time (such as a week, a month or a year). Hence, if there are three systems that can lead to a given load reduction level, then the frequency of that load reduction level is simply the sum of the system failure frequencies contributing to that reduction level. At the system level, there is little or no discrimination regarding what parts of the system contribute to each level of derate unless it can be extracted from the data itself. If there is interest in a given train of equipment or a particular component, the data must be mined for this information at each level of derate as opposed to generating this information with the models (e.g., the data used to generate the system failure frequency must be examined to

determine what fraction of the frequency is due to failures of particular trains of equipment or components). Alternatively the system level supercomponents can be expanded to the train or component level for this information as described for the train level/supercomponent and fault tree approaches. After summing the failure frequencies for each contributor to a given load reduction level to obtain the total frequency at that level, the consequences associated with the load reduction level are applied to obtain the risk of the load reduction. This calculation of consequences is discussed in a later subsection.

Quantification of the *train level* supercomponent model is similar to that of the system level supercomponent model except that the supercomponents now represent the collection of components that make up each train. The train level supercomponent model can also include individual component level events where they may be single failures that could lead to loss of the system (these single failures are often referred to as single point vulnerabilities). With this technique, the combinations of trains and individual components that lead to a trip or to one or more levels of derate are listed, failure probabilities assigned from information derived in Section 4, and frequencies generated for each contributor to the trip and derate levels. The output of the quantification is a frequency of occurrence for each load reduction level. (Note that for the train/single point vulnerability models, quantification may benefit from fault tree quantification software as system failures leading to a load reduction may be defined by combinations of trains and components, and the number and size of the combinations may be difficult to assess and track manually or in a spreadsheet.)

5.1.2 Fault Tree Logic Models

Quantification of detailed fault tree models is typically performed using software designed to apply to the models the rules of Boolean algebra necessary to convert the logic into the combinations of component failures that would lead to each level of derate or plant trip. These combinations of component failures are known as minimal cut sets.⁸ By assigning a failure probability to each component represented in each cut set as described in Section 4, the product of the failure probabilities for the components in each cut set is taken to produce a frequency for that cut set. The sum of all cut set frequencies for a given top event determines the frequency of the level of derate or trip represented by that top event. The process of producing cut sets for the top event of a system is conceptually similar to that described for the supercomponent train level approach except that the cut sets are generally in terms of components and their failure modes as opposed to trains of equipment. In general, fault tree software not only applies the laws of Boolean algebra to produce the cut sets but performs the sum of products function for the failure probabilities of the components to produce a top event frequency (for a given level of derate or a plant trip) and a ranked list of cut sets that can cause the top event.

Depending on the techniques described in Section 3 that were selected for detailed modeling of the systems to be analyzed, it may be worthwhile to consider adjusting the cut sets for each level of derate or plant trip. These adjustments would be implemented to account for potential over- or under-estimation of the frequency of each level of derate resulting from simplifications made in development of the models.

⁸ A minimal cut set is defined as the smallest combination of component failures that, if they all occur, will cause the top event to occur. The combination is a “smallest” combination in that all the failures are needed for the top event to occur; if one of the failures in the cut set does not occur, then the top event will not occur (by this combination). Refer to Reference [15].

5.1.2.1 Elimination of Duplicate Failure Combinations

In developing the logic for a given system, it is useful to define a top event as “Failure to operate at a power >x%” (see Section 3.2.2.1). While this definition of a top event keeps the modeling simple, it is possible for component failures and combinations of component failures to end up in more than one bin associated with the various levels of derate. For example, a cut set leading to the 50% derate bin may also contribute to the plant trip bin. After quantifying the top events to obtain the combinations of component failures for each load reduction level, the next step is to eliminate duplicate cut sets occurring in more than one load reduction bin. One way to make this correction is to assign the cut set to the derate bin having the largest load reduction, as this is more limiting with respect to plant generation. If the same cut set appears in any of the lower load reduction levels it must be deleted wherever it appears in those levels to avoid overestimating its contribution to plant generation risk. One method of deleting duplicate cut sets is described in Appendix B.

5.1.2.2 Treating Differences between the Trip and Derate Frequencies of the Models and Operating Experience

Following quantification of the GRA models, it is useful to compare the resulting frequencies of plant trip and the various levels of derate to plant historical experience; a high level summary of plant-specific experience can be developed readily from sources such as NERC-GADS [9]. A comparison of the GRA results to the initiating event (plant trip) frequencies employed in the plant-specific PRA may also provide useful insights. If the review of the frequency of system contribution to plant trips and various derate levels reveals that the GRA model produces significantly higher or lower frequencies than plant experience would suggest, then a review to determine the source of these differences is in order. This step is sometimes referred to as “calibration” because an “adjustment factor” may simply be applied to make the frequencies predicted by the models match experience. As discussed in the rest of this subsection, this approach is not recommended. Instead, an effort should be made with the guidance provided below to investigate the model and failure rates being used, and modify either or both on the basis of the findings until improved agreement is achieved.

One step that should be taken is to compare the failure rates included in the GRA with the plant-specific (e.g., NERC-GADS) information, and/or the failure rates used in the PRA. Other possible sources of differences are the logic that makes up the GRA models themselves or simplifications associated with the modeling techniques used to quantify the GRA. Whether the source of significant differences between model predictions and experience is attributable to data, logic or quantification techniques, it is important to understand which systems and levels of load reduction exhibit these differences prior to using the GRA models in applications on which decisions may be made that have economic consequences.

When assigning failure probabilities to the systems, trains and individual components that may make up a GRA model, it may be necessary to apply data from a variety of sources. Section 4 lists a number of these sources, which can be both plant-specific as well as generic. The selection of the most representative types and sources of data often involves engineering judgment. Examination of the “reasonableness” of resulting frequencies, as discussed below, is a means of arriving at the “best” results.

If the failure rates for dominant contributors predicted by the model differ greatly from experience, then the applicability of the selected data source should be examined as a possible culprit. It is possible that the criteria used for classification of components as failures may be over- or under-conservative when compared to that which would be appropriate for use in a GRA. (For example, some data sources may classify degraded performance of a component as a failure, whereas the plant may be able to continue to run depending on the nature of the degraded condition).

If the GRA data source and plant-specific failure rates for major components within a system are in reasonable agreement but the system contribution to derates and plant trips produced by the GRA does not reflect plant experience, then it may be worthwhile to revisit the logic of the system model to assure that it has been developed correctly and that the adopted system success criteria match the criteria suggested by plant experience.

Additional means for assuring the fidelity of the results are to “post-process” the cut sets to compensate for simplifications that were made in the modeling. Whether these simplifications have a significant impact on the estimate of the frequency of trips or derates depends on the designs of the systems whose unavailabilities lead to these various levels of derate. Should each load reduction bin be dominated by single point vulnerabilities that are relatively high in frequency, then it is likely that the modeling simplifications will have little impact on the results for any given bin. However, where multiple failures are required before a particular derate is achieved for any given system, then common modeling approximations can influence the results and it may be worthwhile to consider adjustments to compensate for these approximations. Four approaches to simplifying the modeling were presented in Section 3.2.2.1:

- Assign all mission time events an annual frequency
- Assign all mission time events a 24 hour mission time and adjust the top event frequency with a correction factor
- Incorporate both annual and mean time to repair mission time events directly into the model for each component.
- Create a surrogate event for each component representing either an annual or a mean time to repair mission time

Appendix B provides details on adjustments that should be considered in post-processing the cut sets for models that use these simplifications.

5.2 Quantification of Lost Generation Consequences

Quantification of the GRA models described above yields frequencies associated with each level of load reduction. Since the desired result from the GRA model is an estimate of potential lost generation as measured in Mwh, the duration and magnitude of the load reduction must be determined and applied to each failure combination or cut set coming out of the models.

Whether using the supercomponent approach or more detailed fault tree modeling with cut sets, the consequences of a load reduction in terms of lost generation are calculated as follows:

$$\begin{aligned} \text{Total Lost Generation (Mwh)} &= \text{Magnitude of derate} * \text{Duration of load reduction} \\ &= (1 - \% \text{ of Full Power after load reduction}) * \text{Rated Capacity (Mw)} * (\text{MTTR for the system, combinations of trains, or combinations of components leading to the load reduction} + \text{time to restore plant to power, in hours}) \end{aligned}$$

The magnitude of derate is represented by the top event of each of the load reduction bins (Figure 2-2).

The total duration of an outage is made up of two parts: the mean time to repair of the affected systems, trains, or components plus the time required to return the plant to full power. Sources of data for both contributors to the duration of an outage are presented in Section 4.2 (see the subsection labeled “Recovery times”).

5.3 Propagation of Uncertainties

Up to this point, the discussion of quantification of the GRA models has dealt strictly with best estimate or point values. It is important to keep in mind that many of the values used in GRA have uncertainties associated with them. While the results of a point value analysis may suggest risk is acceptable, if these results are near a threshold of acceptability (such as whether the plant can generate sufficient power to meet plan over the course of a year or that it can operate at full power during periods of peak load), it is useful to account for the uncertainties in the data assigned to key components and determine if the risks of not being able to meet these thresholds is significant.

A parametric uncertainty analysis can often be performed to provide a mean and estimate of exceeding day to day or yearly objectives for plant operation. The references in Appendix A provide data and methods that can be used to develop these distributions. There may be hundreds or even thousands of events in a GRA model to which uncertainty distributions could be assigned to accomplish this analysis. In performing the uncertainty analysis it may not be necessary to develop and assign distributions for every component or failure mode. A process for selecting important components that drive risk and developing distributions for only these components may be sufficient. In determining which components and failure modes are important to risk from an uncertainty perspective, it should be kept in mind that this does not just involve components that are important to risk individually. Techniques for identifying components that are important in combination should be used in the selection of a subset of components to which to assign distributions. Several methods are available to identify the combinatorial importance of components:

Cumulative Risk Reduction Worth (Section 9.3.1.1, Method A of Reference [16])

Based on techniques developed for the assessment of the effects of structural and component aging [17]

Second-order importance

Creates two dimensional matrix of components determining the importance in a pair-wise manner [18]

Differential importance measure (DIM)

Developed for the purpose of evaluating changes that affect the properties of multiple components [19]

Top event prevention (TEP)

A deterministic technique for identification of combinations of events important to a Boolean expression [20]

Components similar in design, function and operating conditions should be correlated once distributions are assigned. One simple approach to correlating component failures in an uncertainty analysis is to assign a correlation factor of 1 to all components of the same type and failure mode. Correlation of similar components in this manner recognizes common effects of design, maintenance and environment on the potential for failure of these components.

The uncertainty distributions provide important indications as to the confidence in the derived values, whether they are system, train or component failure rates, mean repair times, or electricity pricing. Therefore, it is important to propagate these uncertainties through the top event cut sets to obtain a mean and distribution for the total lost generation (Mwh or dollars). An example of the distributions generated for total lost Mwh is provided in Figure 5-1.

Commercially available software (often a part of fault tree quantification codes) is available to assign distributions and correlation classes, and propagate uncertainties.

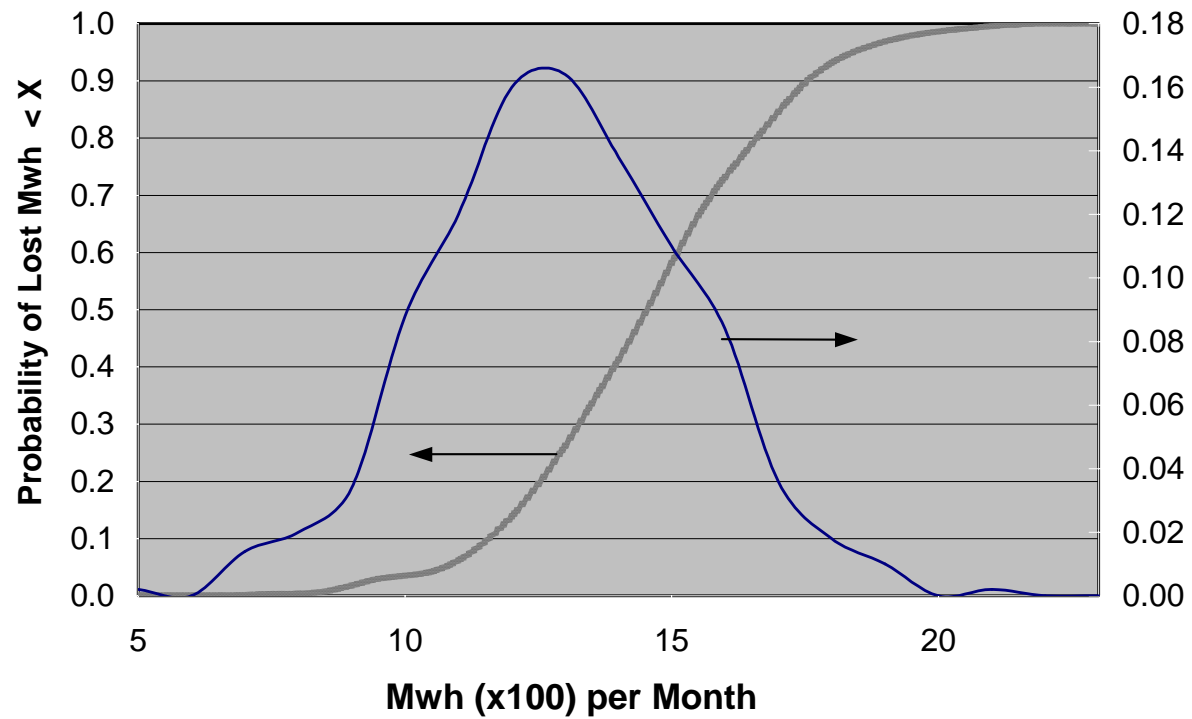


Figure 5-1
Generation Loss (Right Scale Probability Density – Left Scale Cumulative Distribution)

6

RESULTS AND APPLICATIONS

Solving (quantifying) the logic models discussed in previous sections produces numerical results that must be interpreted and sufficiently understood to enable clear and concise presentation to utility executives, system engineers and other decision makers who may not have a detailed understanding of GRA modeling techniques. The results, their interpretation, and applications are the subjects of this section.

In Section 1, Figure 1-2 was introduced to illustrate the relationships between trip/derate models, GRA, and RIAM. From that figure (repeated here as Figure 6-1) it is seen that the GRA models build upon the information contained in trip/derate models by incorporating information about magnitudes and durations of derates to predict future lost generation.⁹

Using Figure 6-1 as a reference, this section discusses the interpretation, presentation, and application of results of the GRA models. Results and applications available or possible at intermediate steps (most specifically, at the trip/derate model step) are described as well.

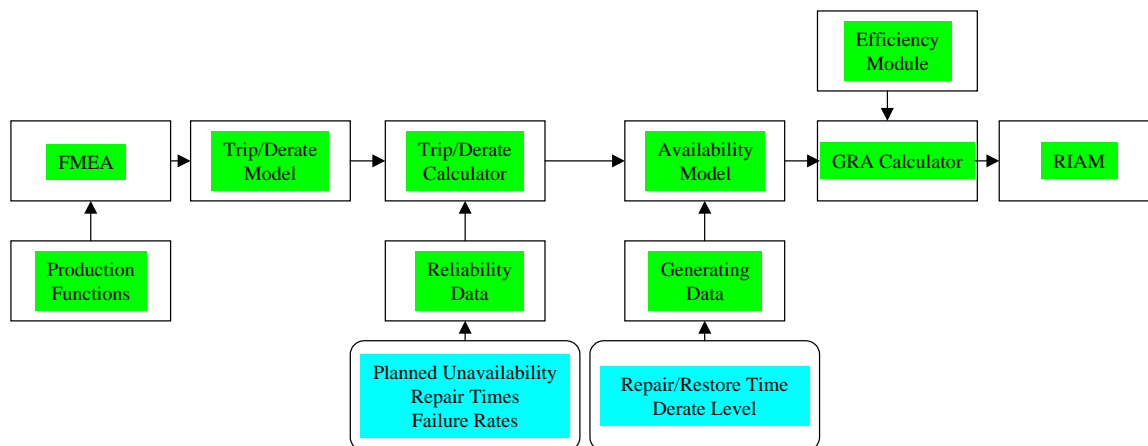


Figure 6-1
Overview of the Development of Trip and GRA Models (From Figure 1-2)

⁹ As a reminder, the efficiency module contained in Figure 6-1 is not addressed in this document. For the purposes of this guide, the terms “Availability Model” and “GRA Model” are synonymous.

6.1 Primary Results

The primary result produced by the GRA logic models (Section 3) and the appropriate data (Section 4) is an estimated forecast of the total generation loss, measured in megawatt-hours, on a yearly basis. This type of result might be used, for example, for ranking the importance of systems and components, for assisting in operating experience reviews, or when considering plant design changes to improve plant availability (all these are elements of equipment long-term planning, also known as life cycle management [4] or of risk informed asset management (RIAM)[2].

More detailed modeling techniques that account for the potential for increasing failure probabilities with time due to component aging degradation can be used to refine the results. Explicitly modeling aging effects can be of value for long-term planning.

The yearly generation loss for a set of alternative long-term plans being evaluated serves as input to RIAM tools as discussed later in this section. The RIAM tools add capital and operating and maintenance (O&M) costs to the cost of lost generation to identify the alternative with the best long-term economic benefit in terms of financial indicators such as increased plant net present value, return on investment, or benefit-to-investment ratio.

A measure of the predicted reliability of equipment over intervals shorter than a year can also be achieved by modifying the “mission times” applied to the GRA models, i.e., by decreasing the interval used to calculate the forecasted Mwh. These types of analyses can be used to estimate the potential for the plant being able to produce a specific amount of energy during peak power periods for bulk power trading purposes or for evaluating the risk tradeoffs of operating with balance-of-plant equipment in a degraded state (e.g., shaft vibration or excessive seal leakage) vs. derating or shutting down for immediate repair.

6.2 Breaking Down the Results

While total lost generation over remaining plant life or a particular period is a key input for resource allocation decision-making, even more valuable support of decision-making can be achieved by breaking the results down into their principal contributors and examining which dominate in terms of risk.

For the purpose of this guide, a top-down approach is suggested to identify these contributors:

- Distribution of risk among units for a multiunit site
- Distribution of risk among various levels of derate for a given unit
- Distribution of risk among the systems for a given unit or for a site
- Distribution of risk among the individual components that make up each system.

6.2.1 Breaking Down the Results by System and Derate Level

The bar charts in Figures 6-2 through 6-4 illustrate a simple method of presenting results in terms of lost generation by system. The charts give GRA results at the site level for an example two unit site, i.e., the prediction of total lost generation from all modeled systems for each unit. In this example, each unit has a rated capacity of 600 Mwe and 80% availability factor, for a total yearly output of approximately 4.2 million Mwh per unit. Unit 1 has about a 30% greater predicted generation loss, with most of the increased loss coming from decreased availability of the feedwater system and turbine.

In Figure 6-3, the derate categories defined for this example evaluation are shown on the X-axis. The Y-axis is the average annual Mwh loss estimated by the GRA, with failures resulting in 500-600 Mw derates being the most significant (a 600 Mw derate is a plant trip when the plant is operating at full capacity). Derates in this category contribute to a generation loss of about 185,000 Mwh per year for Unit 1. The stacked bars illustrate that Unit 1 contributes slightly more than Unit 2 in all derate categories. By reviewing the information in this figure the analyst can see that full plant trips contribute the most to the results, with power reductions of 300-400 Mwh contributing nearly as much. Equipment and system outages that contribute to smaller levels of derate play a relatively insignificant role in the overall picture. Thus, the analyst immediately knows that the major contributors to risk at these units are not many small derates, but large, potentially lengthy power reductions.

Figure 6-4 focuses on Unit 1 to better understand what is contributing to the annual lost generation. Here, contributions of individual systems to total annual lost generation are ranked. For each system, the dominant levels of derate are also evident. For the systems shown, it is clear that feedwater, turbine, and circulating water events are the primary contributors to lost generation, with AC power and transformer events contributing to a lesser, but significant extent. It is seen that turbine and transformer failures most often lead to a full plant trip, and that the feedwater and circulating water systems are dominated by partial load reductions (to roughly 60% power). The risk associated with the AC distribution system is distributed with about 33% of events resulting in partial load reduction (to approximately 60% power) and the remaining portion leading to plant trip.

Figure 6-5 contains an alternative method of displaying results in the form of a matrix quantifying the percentage of total annual lost Mwh among the various systems and levels of derate. At this point, the analyst can decide if further examination of the distribution of these results at the component or train level may be worthwhile to gain a better understanding of the specific contributors to annual lost Mwh.

6.2.2 Breaking Down the Results at the Component Level

With dominant systems identified, it is now useful to select one of the dominating systems and assess the generation risk significance of individual components. This assessment uses for GRA the measures of *risk importance* conventionally used in PRA. A *risk importance* measure tells the impact that a change in a component's or system's reliability would have on overall site or plant risk (here, generation risk in Mwh). In this sense, an importance measure reflects the sensitivity of predicted lost generation to the system/component reliability.

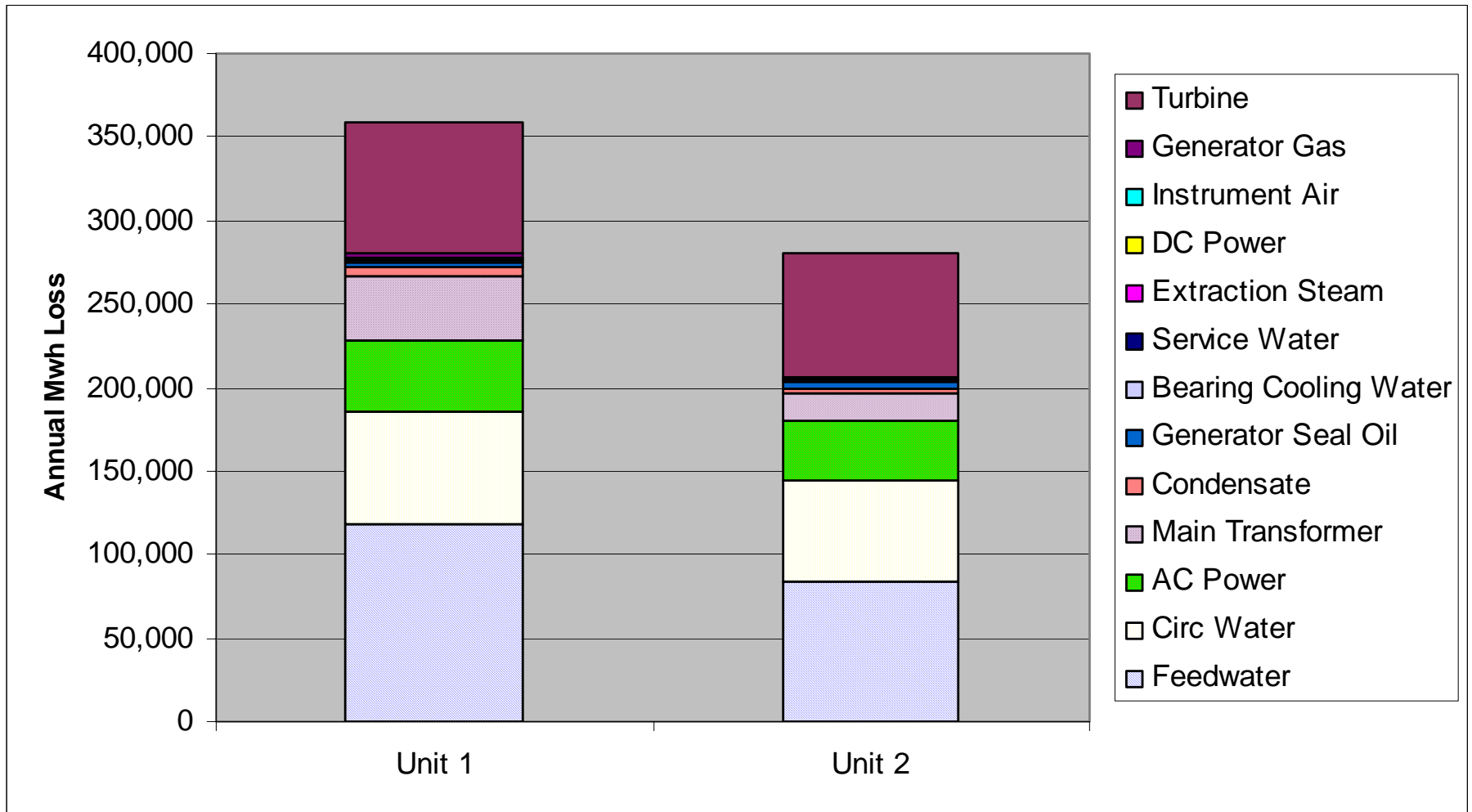


Figure 6-2
Example GRA Results Display: Cumulative Annual Lost Generation per Unit, Two Unit Site

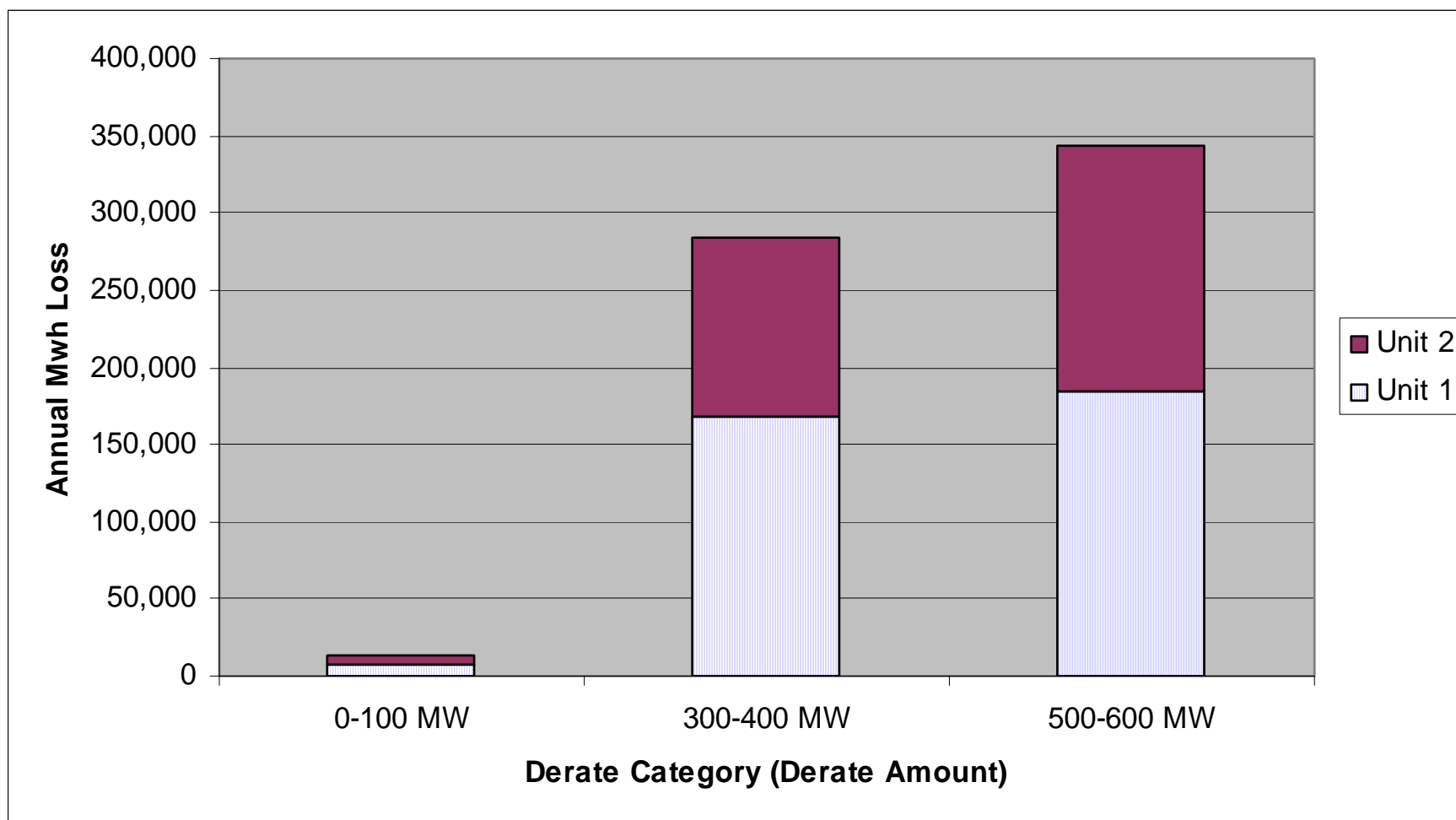


Figure 6-3
Example GRA Results Display: Two Unit Site – Annual Lost Generation as a Function of Derate Amount

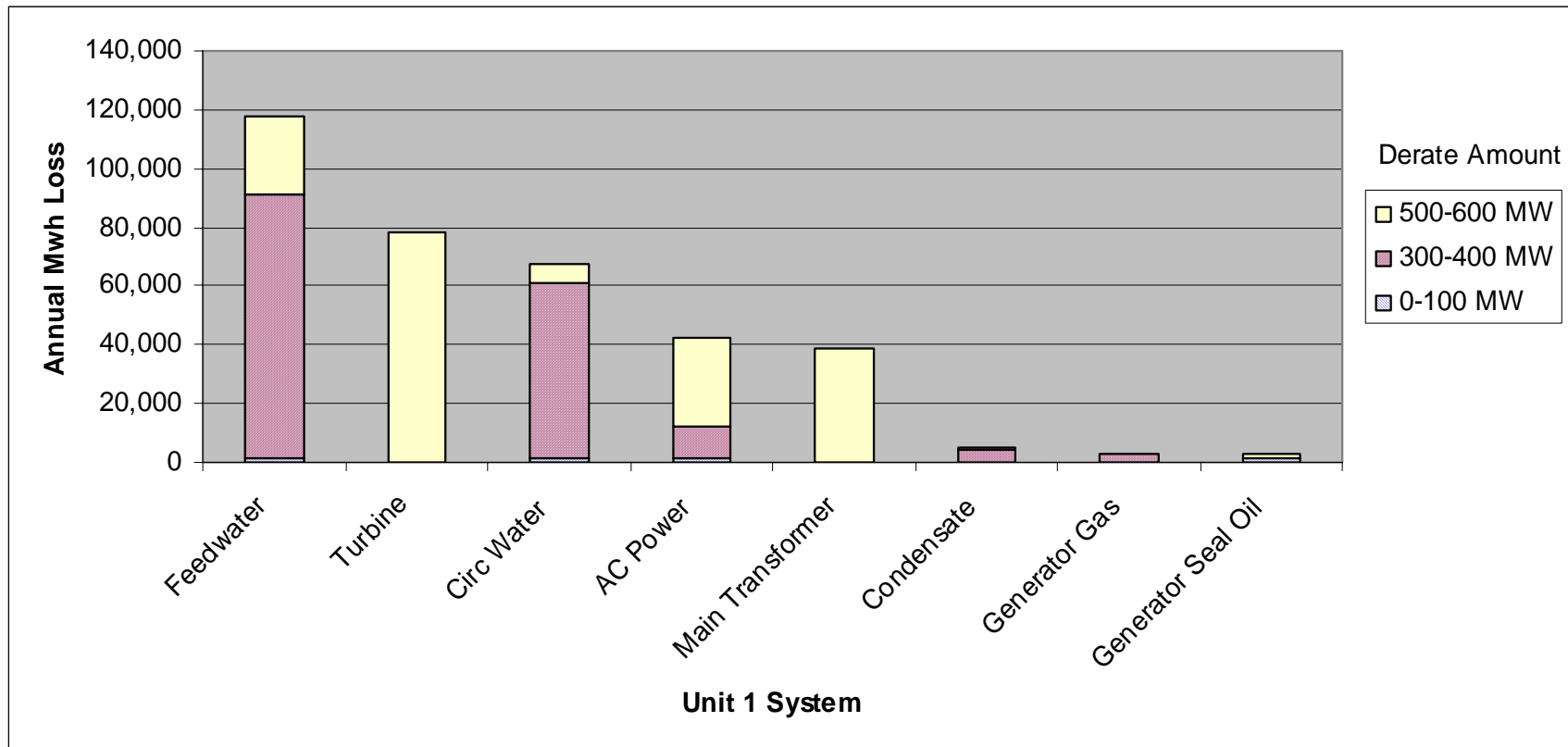


Figure 6-4
Example GRA Results Display: Single Unit (Unit 1), System Contribution to Annual Lost Generation as a Function of Derate Amount

Percentage Contribution to Annual Lost Generation as a Function of Derate Amount

Unit 1 System	Derate Amount			Total
	0-100 MW	300-400 MW	500-600 MW	
Feedwater	0.5%	24.8%	7.5%	32.8%
Turbine	0.0%	0.0%	21.7%	21.7%
Circ Water	0.5%	16.6%	1.8%	18.9%
AC Power	0.4%	3.0%	8.4%	11.8%
Main Transformer	0.0%	0.0%	10.8%	10.8%
Condensate	0.0%	1.1%	0.3%	1.4%
Generator Gas	0.0%	0.9%	0.0%	0.9%
Generator Seal Oil	0.3%	0.0%	0.6%	0.9%
Total	1.7%	46.4%	51.0%	99.2%

Figure 6-5
Example GRA Results Display – Matrix of Results

Two measures of risk are typically used when evaluating the sensitivity of the results to equipment reliability: risk reduction and risk increase potential.

Risk reduction potential, also known as the “Fussell-Vesely” (FV) measure of importance, is an indication of how much each component/system *currently* contributes to lost generation due to equipment failure. The measure is calculated by determining how much the current risk could be reduced if the component (or system) was assumed to be perfect, i.e., always available. The value for risk reduction potential can range from 0 to 1, the former suggesting that the system or component contributes essentially nothing to current annual lost generation and the latter indicating that if a component was available all the time it would reduce ALL the risk (this does not occur in practical application). Systems or components having a high risk reduction potential are those for which efforts to improve their reliability or plant modifications to reduce their contribution to risk may have the most impact. (Note that this says nothing about the value-impact of such a change. To determine whether a modification to the design of the plant or change to maintenance practices is of value, importance measure results from the GRA would need to be combined with information regarding the costs of such an improvement as a part of a RIAM activity.) Efforts to improve systems or components having a low risk reduction potential would not necessarily be worthwhile, as complete elimination of the risks associated with these SSCs would do little to improve the generating capability of the plant.

Risk increase potential (also known as Risk Achievement Worth, or RAW), is basically the complement of risk reduction potential. Risk increase potential measures how much each component could potentially contribute to risk were the component allowed to completely degrade in reliability. The measure is calculated by determining how much the current risk would increase if the component was assumed to be completely unreliable, i.e., never available. The minimum value possible is 1, indicating that if a component was never available the risk would not increase at all. The maximum value for RAW for a given evaluation is often on the order of 100 or 1000, indicating that if the component were to be completely unavailable, total lost generation would be several orders of magnitude greater than currently experienced (a component that had such a significant impact on generation generally would be repaired or replaced before it was allowed to degrade to such an extent). Systems or components that rank high in RAW are candidates for assuring that they do not degrade in reliability (possibly through preventive or predictive maintenance programs). Those that are low in RAW would not necessarily be candidates for such programs since even if they degrade significantly in reliability their apparent contribution to lost generation would not be significantly greater than it currently is.

With these two types of risk importance measures defined, we return to the system contributors to generation risk for Unit 1 and examine what parts of these systems dominate. Figure 6-6 shows the two measures of importance for the feedwater/condensate system, which was associated with 33% of total lost generation for Unit 1. The upper bar chart in this figure ranks all the major components in the system from highest to lowest in risk reduction potential. It can be seen that the overwhelmingly dominant contributors to lost generation for this system are the feedwater pumps themselves (components FWPPMPA and FWPPMPB in the figure). Feedwater regulating valves (components FWREGVA and FWREGVB) contribute somewhat less and the condensate pumps (CNPPMPA, CNPPMPB, and CNPPMPC) less than that. The two feedwater pumps in this plant are roughly 50% capacity, but the capability of the plant to operate slightly

above 50% power with just one pump has been demonstrated. Each feedwater train has its own regulating valves. That the regulating valves have smaller risk reduction potential is simply a result of the difference in failure probability for the valves as opposed to the pumps. There are three 50% capacity condensate pumps for this plant and thus the condensate pumps are relatively low in importance because there is installed redundancy associated with these components.

The second bar chart of Figure 6-6 illustrates the risk increase potential (also known as RAW) measure of importance for the feedwater/condensate system. The stair step character of the diagram reflects the different levels of derate that would occur were the components in question to fail. The components having the highest level of RAW are for the most part made up of a number of condensate and feedwater recirculation valves to the hotwell and condensate storage tank. These valves are designed to prevent dead heading the condensate and feedwater pumps as well as to prevent overfilling of the hotwell. These minimum flow and reject valves fail open on loss of air and turn out to have significant capacity. Experience has shown that opening of one of these valves causes sufficient flow diversion, resulting in loss of feedwater pump suction or makeup to the reactor at insufficient rates. In this plant, failure of one of these valves to remain closed during power operation can result in a plant trip; in addition, the valves cannot be repaired while the plant is on-line. Thus, it is important that parts of the valve operators that are most subject to wear and degradation be closely monitored when the plant is off-line. Loss of the feedwater pumps and regulating valves, on the other hand, result in only a partial load reduction. The condensate pumps remain low in risk increase importance, again because there is installed redundancy.

What the two bar charts in Figure 6-6 illustrate is that the two types of importance measures provide insights from two perspectives:-

- What components are most important to reducing risk?
- What components are most important in ensuring the risk level does not increase from its current level?

Although the risk importance measures when taken individually reveal important insights, there is even more to be gained when the measures are taken together. The relationship between the two importance measures for each component of a system provides information about component reliability and risk that may be of value in managing generation risk. The relationship is presented most effectively by plotting the two importance measures on a four-quadrant plot as in Figure 6-7.

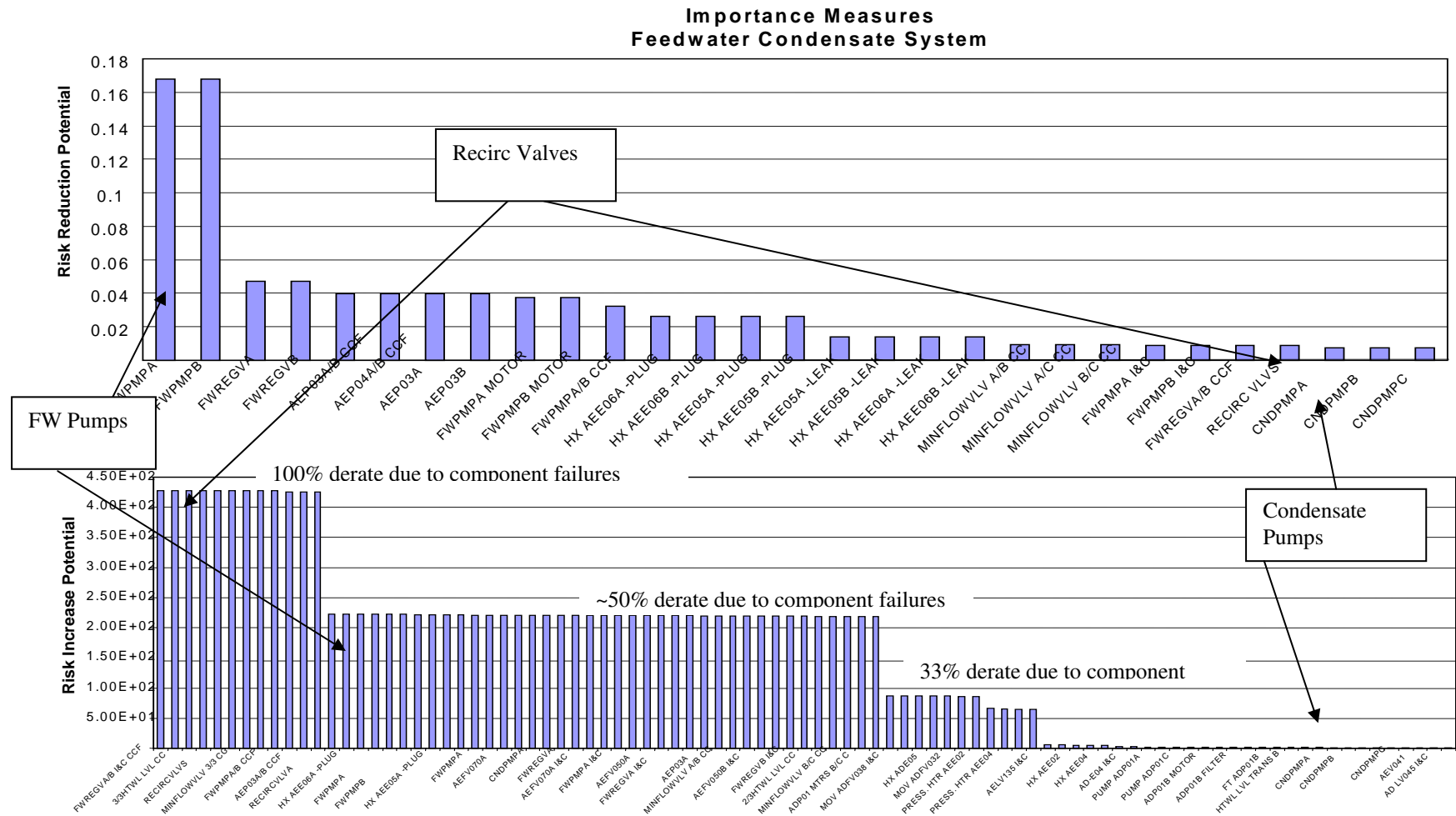


Figure 6-6
Example GRA Results Display – Two Importance Measures

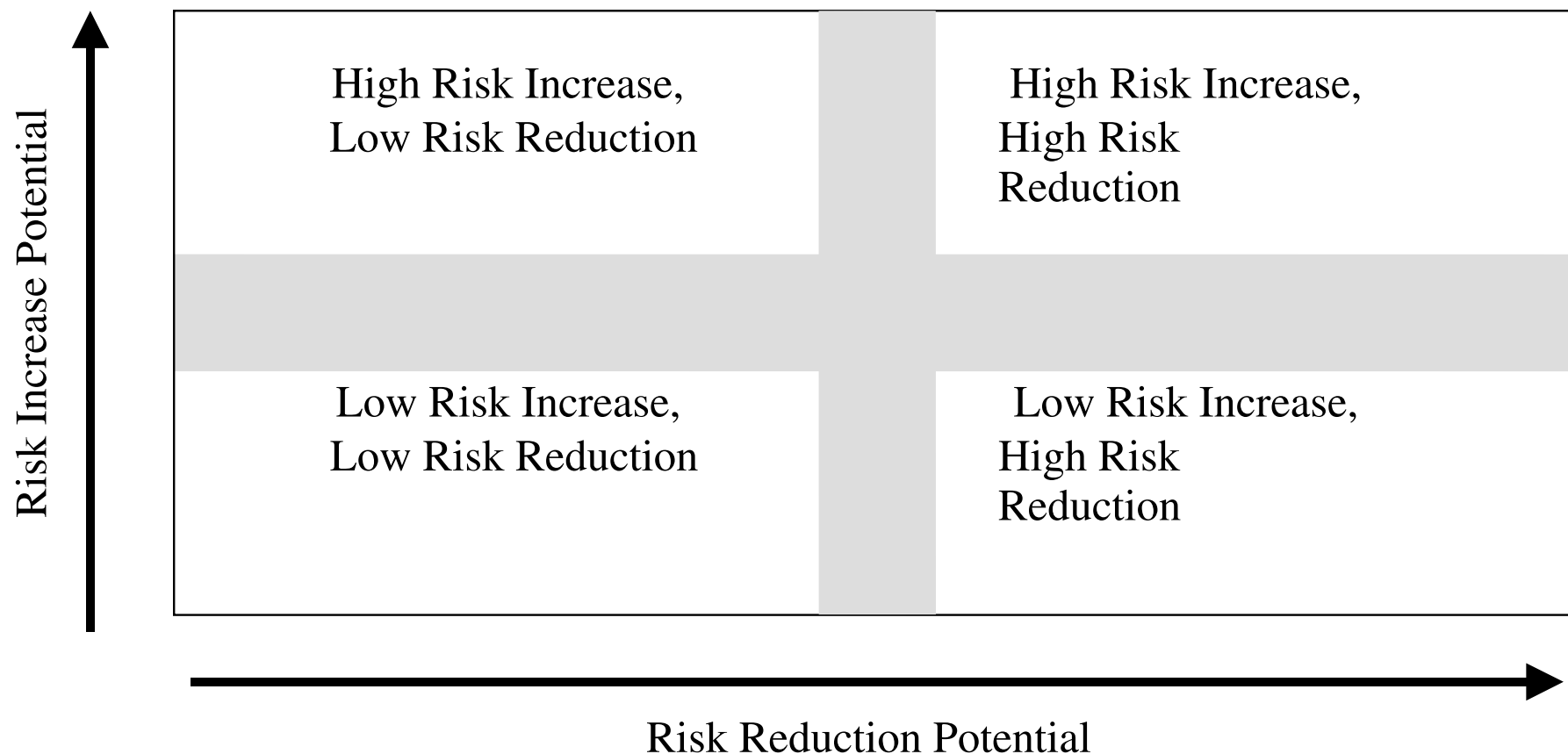


Figure 6-7
Example GRA Results Display – 4 Quadrant Plot Overview

The following paragraphs indicate how to identify general characteristics of the components and systems that should be considered when evaluating strategies to reduce lost generation.

Lower Left-hand Quadrant (low risk increase; low risk reduction): Due to many factors, such as system and component redundancy, components in this quadrant do not currently contribute significantly to risk, **and** risk would not significantly increase if the component reliability of any individual component is allowed to degrade. Thus, improving the reliability of systems or components in this quadrant would have little benefit. However, any strategy that simply provides for replacement or repair of components after their failure should be evaluated for its cost-effectiveness. Considering equipment and labor costs for a “run to failure” strategy for these components versus the cost of other means of maintaining the reliability of these components may be worth examining. In addition, an assessment of the effects associated with the potential for degradation of the reliability of combinations of components requires consideration.

Upper Left-hand Quadrant (high risk increase; low risk reduction): Even though components in this quadrant have the potential for large negative impact on risk, they are low in risk reduction potential most likely due to existing operating and maintenance (O&M) practices and/or their inherent high reliability. However, plant risk could significantly increase if these systems or components were allowed to degrade in reliability. Thus, operation and maintenance of these components in a manner that assures their reliability or monitors changes to their reliability so that action can be taken before the change affects risk significantly may be beneficial.

Upper Right-hand Quadrant (high risk increase; high risk reduction): System or components in this quadrant contribute significantly to current plant lost generation risk and could have a large additional contribution to plant financial risk if they are allowed to degrade. This is due to factors such as their current reliability and little or no redundancy to maintain a given component’s intended function in the event of failure of the component. Risk is most sensitive to changes in the reliability of these items. It is these systems and components that should receive the most attention in order to evaluate programs and practices that sustain or improve their reliability. Like the systems in the upper left quadrant, however, operating practices can also play a significant role in managing risks.

Lower Right-hand Quadrant (low risk increase; high risk reduction): Components in this portion of the plot currently contribute significantly to risk (possibly due to low reliability) but would not have a significant additional impact on risk if they did degrade. This quadrant usually has few, if any, systems or components in it, because poor reliability is not common in power plant equipment important to generation and is typically not tolerated by the plant staff. Components in this region may be candidates for design modifications or replacement.

Also shown on Figure 6-7 are thresholds for both risk increase and risk reduction potential. These thresholds are not precise criteria that can be applied to the importance of generation-related components across a variety of issues. Rather, the thresholds should be viewed as broad bands of grey. The location of the thresholds is established by evaluation of the cost-benefit of proposed activities directed at mitigating the risk from the component in question. Figure 6-8 is a plot of the results shown in Figure 6-6 in the four quadrant format of Figure 6-7. Note the same

distinct levels of risk increase potential (Y-axis) into which the component results are grouped that were evident in the lower bar chart of Figure 6-6. These levels correspond to the load reduction that would occur if the various components were to fail or be removed from service (see lower graph in Figure 6-6). For example, the top most row of data points (points 70, 79, 55, 32, etc.) correspond to the 100% derate (plant trip) category. If any one of these components fails, a plant trip will result. The second row (data points 51-55, 1, 2, etc.) correspond to 40% derates – a failure of any one of these components will result in a load reduction of 40% of full load. The derate categories represented by the linear groupings of data points are defined by the analysts using techniques such as described in Section 2, and will vary from plant to plant.

The distribution of components along the risk reduction potential axis (the X-axis) is continuous, reflecting a spectrum of failure probabilities associated with the components in the system.

In Figure 6-8 it can be seen that:

- In the upper left quadrant are components for which the current reliability is effectively managing risk. Examples include the recirculation valves in the condensate system (data point 32). These valves are not required to actuate to support power operation. As they could cause a plant trip should they open inadvertently, existing programs directed at assuring their low potential for spurious operation should be maintained.
- The feedwater pumps (data points 1 and 2) appear in the upper right quadrant. It is important to monitor the reliability of these components to identify if there is any degradation, and to evaluate programs that may improve the reliability of components in this quadrant. The design of the plant (i.e., the feedwater system has two 50% trains) leads to the greatest contribution to risk increase potential being from partial load reductions (reductions of 40% full load); such reductions occur upon loss of a single feedwater pump. A full plant trip results only if both feedwater pumps fail.
- The condensate pumps are in the lower left quadrant (i.e., data points 6, 7 and 8), due to the presence of installed redundancy (i.e., the presence of a third train of condensate in this plant allows failure of one train to occur without a consequential load reduction). The appearance of the pumps in the lower left quadrant makes the condensate pumps candidates for programs that tend toward “repair on failure” strategies. However, the potential for simultaneous degradation of reliability for combinations of equipment must be considered and monitored as well, since this might have a significant impact on risk even though each pump by itself remains low in importance. Due to the installed redundancy of the condensate pumps specifically, the results based on lost generation risk might suggest that the programs directed at the reliability of the condensate pumps need not be as rigorous as for other components such as the feedwater pumps.
- Nothing is found in the lower right quadrant, suggesting that there are no components in this system with performance issues that would warrant maintenance change, replacement, or redesign.

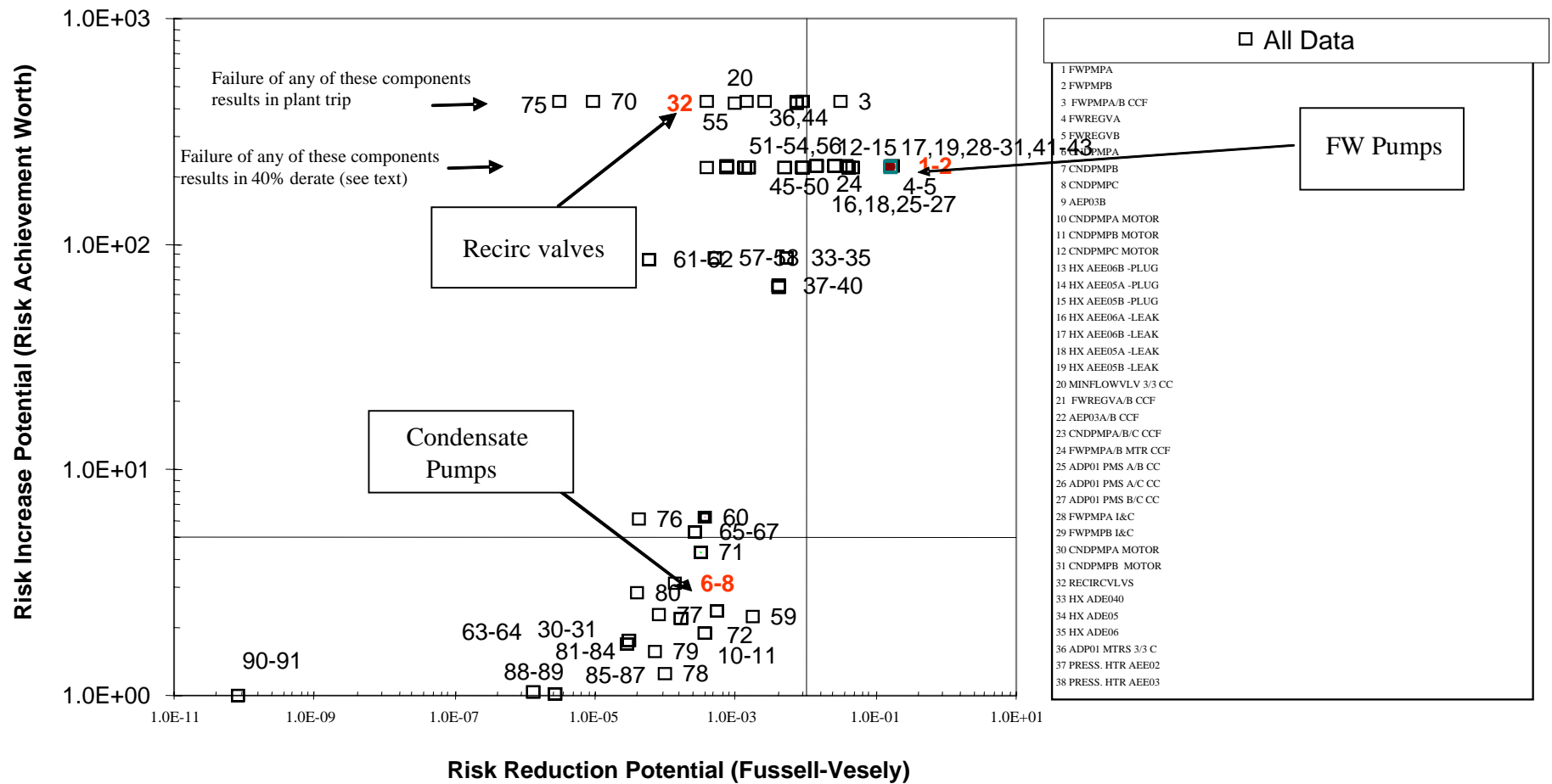


Figure 6-8
Example 4 Quadrant Plot for Selected System

6.2.3 Distribution of the Plant Capability to Produce Power

Another method of presenting the results of a generation risk assessment is to provide a distribution of the plant capability to produce a desired total output over a given period of time. Figure 6-9 illustrates this form of the results and takes advantage of uncertainty distributions assigned to the reliability of systems and components included in the generation risk assessment.

Suppose that the business plan for a utility requires a certain Mwh output from its nuclear facilities. The generation risk assessment for a given unit suggests that the unit can more than meet the assumptions of the plan when using best estimate point values for the components included in detailed modeling and the trains and systems approximated at a supercomponent level. However, there is uncertainty associated with these point values and this uncertainty creates the potential for the plant falling short of the plan should events occur that are currently assessed as being low in probability. Thus, using only the results generated with point values could lead to poor decisions.

By identifying the systems and components that are most important to driving the risks of plant generating losses and assigning distributions to events representing their failure, an estimate of the likelihood that the plant will not meet the goals input to the business plan can be developed. In the example presented in Figure 6-9 the mean value of the estimate of power generation is indicated by the solid vertical line. The figure shows that the best estimate of power generation for the budgeting year is higher at the mean value point than is the estimate of power generation in the plan using the assumptions input to the plan (i.e., the vertical line indicating the mean value is to the right of the vertical dashed line representing the plan's value). This is consistent with the results generated using only point values. The fact that the mean value is higher than the plan value means that there is more than a 50/50 chance that the plant will meet plan. After propagating the uncertainties it can be seen that there is actually a 30% chance that the plant's generation will fall short of plan (this is determined by the probability at the point where the vertical dashed line representing the plan crosses the solid line representing the cumulative probability). There is a 10% chance that it the plant's output could be well short of plan. At this point, decision makers must assess their tolerance for risk, asking themselves if the chance of falling short (or well short) of plan is acceptable, allowing for the plan to move forward in its current form with its current assumptions.

By drilling down into the tails of the curves on the left sides of the plots in Figure 6-9, the analyst can identify the dominant contributors to lost generation that would most likely result in the plant not meeting plan. Techniques available with commercially available software allow for collection of simulation data associated with specific segments of the distribution in order to assist in the identification of the dominant contributors to the tails of the curve. This information can be provided to plant and business managers for their consideration in reducing the risk associated with this part of the curve (by, for example, improving the reliability of key components that contribute to the tails of the curve, or staging spare parts to reduce the mean time to repair of important components), hedging against that risk, or accepting it as a part of the operation of the business.

In the figure below, the "mountain top" curve uses the scale on the right (probability); the "ramp" plot (cumulative probability) uses the scale on the left.

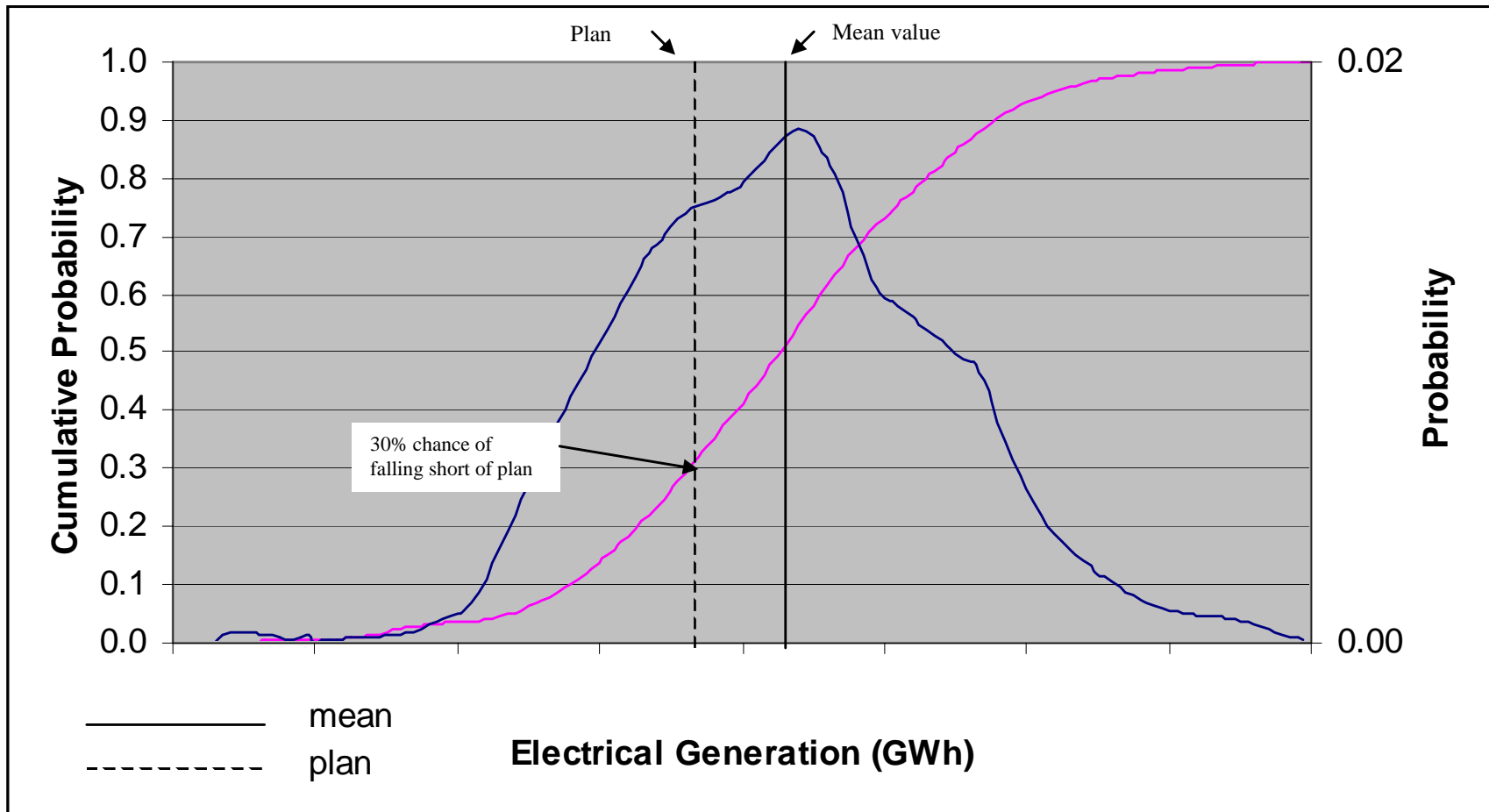


Figure 6-9
Incorporating Uncertainty into Results to Support Decision Making

6.3 Applications

A GRA model has as its primary output the estimation of generation loss (in megawatt-hours) resulting from postulated equipment or system unavailability. This result can be used directly to support various applications, or it can serve as input to other models that, along with additional input, provide other tools to support decision-making. This section provides an overview of potential uses and applications of GRA and its building blocks: an availability model, a trip model, and FMEAs (see Figure 6-1; note again that FMEAs are not required for a GRA, but are used here to represent the tasks completed to identify systems, function, success criteria and corresponding derate levels).

6.3.1 GRA Applications

Among the primary uses of the GRA models and results is the generation of input to RIAM methods and tools. GRA results provide information about the frequency and duration of power reductions. As shown in Figure 6-1, this information (from the “Availability Model” box) is combined with thermal efficiency information and input to RIAM. In combination with economic data (electricity prices, costs of labor and capital goods, etc.), safety impacts, safety-related cost impacts, and other appropriate input, RIAM tools and techniques can be used to support decisions about many issues facing a plant or an enterprise.

Table 6-1 contains examples of applications that can be performed using GRA. Many of these examples have been selected from Table 1-1; Table 6-1 describes the application in more detail. In these applications the common thread is the use of predicted lost generation as a function of component/system to address the issue at hand.

Table 6-1
Examples of Applications of GRA and Intermediate Results

Application	Description	Comments
GRA (Availability Model) <ul style="list-style-type: none"> Input to RIAM 	Provide information regarding Mwh lost (based upon frequency, magnitude, and duration of derates)	Combine with thermal efficiency and economic data for RIAM applications
<ul style="list-style-type: none"> PM, PdM, Corrective Maintenance prioritization 	Use risk importance rankings to determine most suitable type of maintenance, and prioritize within category	Use concepts such importance measures; results are from perspective of lost generation only – may need to combine with other perspectives (e.g., safety risk) for some equipment
<ul style="list-style-type: none"> Equipment design modification optimization 	Optimize design based upon projected reliability and mean time to repair/restore, and their impact on lost generation	Does not consider cost elements

Table 6-1
Examples of Applications of GRA and Intermediate Results (Continued)

Application	Description	Comments
<ul style="list-style-type: none"> Online/shutdown trade offs given equipment degraded performance 	By estimating duration of shutdown, can compare lost generation (shutdown) to predicted lost generation if equipment operates in degraded state	
Trip Model <ul style="list-style-type: none"> Input to GRA 	Provides system models, frequencies, and repair information to GRA	Combine with magnitude and duration of derate to predict lost generation
<ul style="list-style-type: none"> Trip Monitor 	Probability of derate or plant trip given plant configuration	Does not provide information on Mwh lost
<ul style="list-style-type: none"> Online maintenance risk 	Similar to Trip Monitor – provides information regarding probability of derate or plant trip given postulated configuration	GRA enhances by providing projected lost generation effect
<ul style="list-style-type: none"> Component prioritization 	For any given plant configuration, provides importance of all trains/components	Useful in determining what trains need to be protected and which have the highest priority in returning to service for any plant configuration
FMEAs <ul style="list-style-type: none"> Input to Trip Model 	Provides information useful for developing more detailed models	Can be done at supercomponent or detailed level
<ul style="list-style-type: none"> Component prioritization 	Provides information regarding single point vulnerabilities that can lead to trips and derates	Provides information similar to risk increase potential (or RAW)
<ul style="list-style-type: none"> Derates as a function of system/ component unavailability 	Compile and summarize plant derate levels associated with postulated equipment outages	Useful for operator and maintenance staff training

6.3.1.1 Converting Reliability Results to Economic Value

The previous discussions of results and presentations have used lost generation (an indication of reliability) as the parameter of interest. For financial decisions such as those associated with RIAM methods and tools (see the right side of Figure 6-1) these reliability results must be converted into units appropriate for economic analyses. This requires megawatt-hours be converted to lost revenue (dollars).

The most straightforward approach is to assign a dollar figure to each megawatt-hour. This figure represents the income that would otherwise be produced by the Mwh when power is sold into the marketplace. For example, if each Mwh can be sold for \$20, then the lost income (\$) is simply the lost generation (Mwh) multiplied by \$20/Mwh. For generation in the future, economic evaluation tools account for the time value of money.

Economic modeling is discussed in more detail in documents describing risk-informed asset management, such as References [1, 2, 3, 6, and 21]. Although the incorporation of economics into the analysis can be complex, there are some relatively simple and straight-forward ways to include economic indicators and display them in a manner similar to the 4-quadrant plot in Figure 6-8. Figure 6-10 is a copy of Figure 6-8 with economic scales added below the Risk Reduction Potential ('X') axis).

6.3.2 Trip Model Applications

Trip models provide valuable information about the contributors to plant trip and various levels of derate, along with predictions as to the frequencies of these occurrences. The trip model (see Figure 6-1) is a module or subset of the availability model. By combining the trip model with information concerning magnitude and duration of derates, predictions of lost generation can be made. Thus, the trip model is used as input to the availability model.

A primary use of trip models to date has been for trip monitors that are used by operator decision-making when prioritizing and selecting components for online maintenance. The computer screen of a trip monitor is the operator interface with the trip model. Trip monitors are valuable tools for keeping track of (1) ability of the plant to respond to SSC failures; and (2) online trip/derate risk as a function of which components are in and out of service during operation.

A trip model is a logic model representing a plant system or combinations of key plant systems and components whose failure results in a plant trip or derate. Probabilities of failure and unavailabilities of plant components in key systems are also included. The systems that are included in such a model include balance-of-plant systems as well as all nuclear steam supply components important to production. (Trip models may not require the level of detail described in Section 3 for GRA models. For example, trip models can be developed to include only component failures, whereas human errors and test and maintenance unavailability events included in GRA models are not required for logic models developed strictly for trip modeling purposes.)

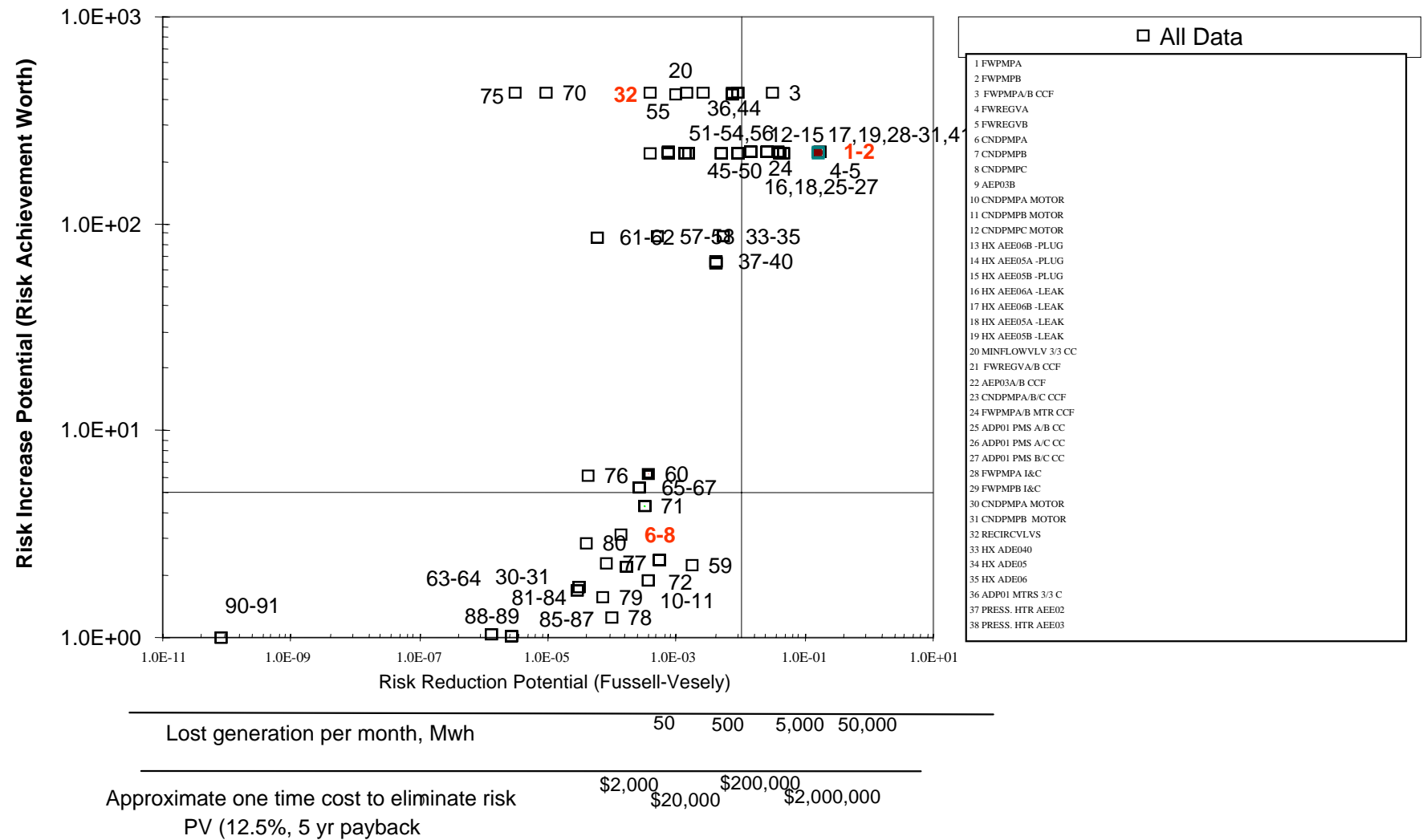


Figure 6-10
Displaying Economic Indicators: Example

By manipulating the trip model to reflect the current or proposed/expected future configuration of the plant, decision makers at the plant can determine the impact of the configuration on the likelihood of experiencing a plant derate or trip.

Figure 6-11 is an example of a computer screen used to display trip monitor status to the operating staff. This screen is another way to present intermediate GRA results. Future development can produce similar screens displaying lost Mwh (see Section 8) so that operating room decisions regarding on-line maintenance and continuing operation can be made on the basis of generation rather than frequency of derate.

Table 6-1 contains other examples of applications at the trip model stage in the GRA process.

6.3.3 FMEA Applications

As was true for trip models and GRA models, FMEAs serve primarily as input to the next step in the GRA/RIAM process, namely, trip models in the case of FMEAs. Although information in FMEAs is predominantly qualitative, the process of completing and documenting FMEAs provides substantial information useful for such applications as system evaluations and training. See Table 6-1.

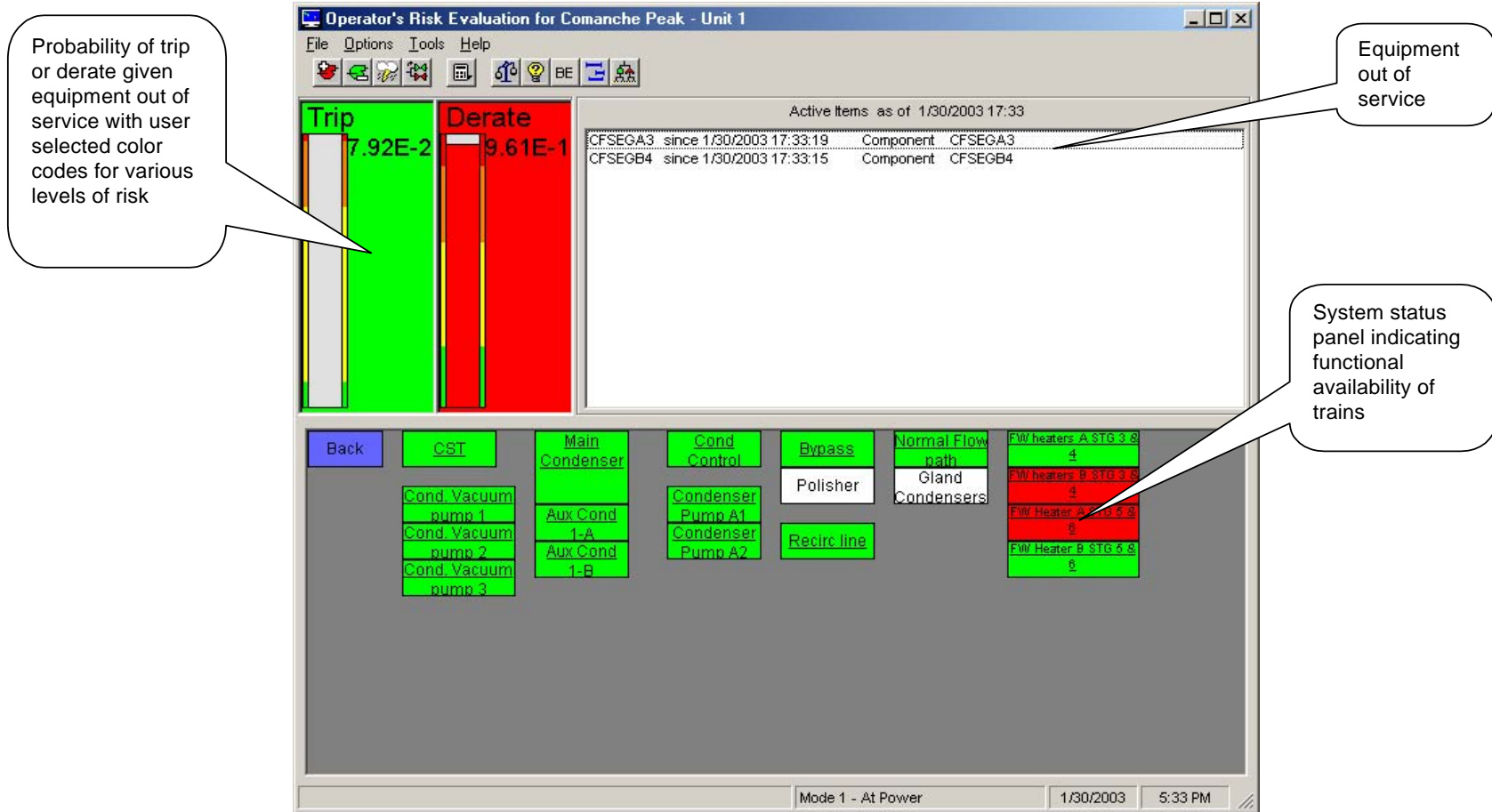


Figure 6-11
Example Trip Monitor Interface Screen

7

RESOURCE REQUIREMENTS

This section provides general guidance on the number and types of personnel that could be involved in the implementation of a plant-specific GRA. Also given are estimates as to the relative level of effort required of each type of personnel for initial system modeling, application of the models, as well as recurring efforts.

7.1 Resource Allocation

In discussing the resources needed to complete and apply a GRA, separate estimates will be provided for development of the models (Section 7.1.1), levels of effort needed for different types of applications (Section 7.1.2) and recurring resource needs (Section 7.1.3).

As with any undertaking involving modeling and analysis of complex systems, the effort to complete, verify, and solve the models for various applications depends on the modeling approach employed, the availability of quality input, the ability to interpret and present the results, and the skills and experience of the project team members. Despite that variability, some general rules of thumb are provided here to enable project and program planners to identify and allocate appropriate resources for GRA implementation at a plant.

The types and level of involvement of personnel are presented here in relationship to the major tasks completed during implementation of a GRA. Guidance is provided for the detailed fault tree approach followed by estimates for the train level supercomponent approach. These estimates for resource allocation needs can serve as benchmarks that can be adjusted to account for any differences between a plant-specific implementation approach and these general approaches, such as number of systems modeled, level of detail, etc.

Personnel involved in the completion of a GRA implementation include the following types (titles may vary from plant to plant):

- **Group Manager** – this individual is responsible for setting the overall direction of the project, coordinating resources, ensuring project objectives are being met, and providing technical oversight, guidance, and mentoring to the project team.
- **PRA Practitioners** – these staff members have experience with PRA techniques, and have most likely worked on the plant's PRA and its applications. They are familiar with logic model development (FMEAs, fault trees), data, and quantification. They understand issues such as common cause failures, human reliability, and the like. These individuals will most likely have the responsibility for development and/or review of the GRA models, regardless of the approach employed.

- **System Engineers** – System Engineers are responsible for the design, control, and performance of specific systems. These people should have the most in-depth knowledge of the specific system(s) to which they have been assigned. They can provide detailed information on system operating characteristics, maintenance issues, operating experience, and other topics related to the system. In some instances, with proper training, the System Engineers can also play a major role in the development of the system models used in the GRA.
- **Operators/Operations Staff** – the Operations Staff (including licensed plant operators) are another source of information about plant and operator responses to postulated events, operating practices and procedures. They can provide a “hands-on” perspective on historical contributors to lost generation, and can identify candidates for improvements that may benefit from GRA modeling and evaluation for cost-benefit calculations and other analyses.
- **Maintenance Staff** – like the System Engineers, these individuals have significant experience with system operation and maintenance issues. They can provide information on historical maintenance problem areas, repair times, maintenance and equipment recovery procedures, etc.

Other personnel from inside or outside the plant may also be able to contribute helpful information in specific instances. For example, central dispatchers may have useful information concerning the switchyard and grid stability issues. Procurement specialists may have data pertinent to spare parts inventories, warehousing, and procurement times. And trainers could provide information related to human reliability. Although these and other contributors may be important to the overall GRA implementation, their input is assumed to be more specialized and specific, and is not explicitly included in the resource allocation discussion.

7.1.1 Initial Resources for Implementation

With these staff categories, and using the major GRA tasks outlined in this guide, Tables 7-1 and 7-2 have been prepared to estimate the level of effort required to complete the initial portions of a GRA and interpret the results. In an attempt to estimate the investment needed in developing GRA models for this purpose, it is assumed that one or more applications (e.g., evaluation of a proposed system modification) have been identified for which completion of the modeling for several systems would be useful. In this section, the labor estimates for the model development and baseline quantification are presented. The level of effort required to complete the application once models are available is provided in Section 7.1.2. In developing the estimates contained in the tables that follow, it is also assumed that all project team members have some basic training in and understanding of GRA and the development of GRA system models.

It should be noted that for a GRA to pay for itself, it should not be necessary to complete the modeling of the entire plant up front as was the case for many of the PRAs developed in response to Generic Letter 88-20 [30]. Rather, only the portions of the plant associated with the application in question should require a model of any detail. In this regard, the model development can occur as needed, over a long period of time. Whether a utility decides to take such an approach in which gradual application-specific models are developed or elects to invest significant up front resources to build a complete model depends on corporate risk management needs.

Table 7-1
Resource Estimates for Initial Steps of a GRA

Task	Person-Weeks					Total
	Group Mgr.	PRA	Sys. Engr.	Operator/ Op. Staff	Maint. Staff	
Define Risk	0.5	0.5				1.0
Identify Generation Functions						
Functions/Systems	0.2	1.0	1.0	0.8		3.0
Data						
System Level Collection	0.2	0.8				1.0
Total	0.9	2.3	1.0	0.8		5.0

Table 7-2
Resource Estimates for Detailed Fault Tree Approach, First Set of Systems

Task	Person-Weeks					Total
	Group Mgr.	PRA	Sys. Engr.	Operator/ Op. Staff	Maint. Staff	
Identify Plant Derate Categories						
FMEAs	0.1	0.5	0.5	0.25		1.4
System Modeling						
Detailed Fault Tree	0.1	2	.4	.2	0.1	2.8
Data						
Gather data		0.2	0.1	0.1	0.1	0.5
Develop probabilities/rates		0.4	0.1			0.5
Assign		0.1	0.1			0.2
Produce Numerical Results	0.2	0.7	0.3	0.2	0.1	1.5
Interpretation of Results	0.2	0.2	0.2	0.1		0.7
Grand Total	0.6	4.1	1.7	0.9	0.3	7.6

Table 7-1 presents suggested resource estimates for the initial steps in the development of a GRA. These initial (one-time) steps are the same whether the supercomponent or detailed modeling approaches are implemented. They involve defining what is meant by risk for the plant (e.g., lost Mwh, availability or other inputs to corporate risk management programs). It is also recommended that an identification of all plant systems that support functions important to the definition of risk be defined. Finally, a high level data collection task is suggested to provide a preliminary estimate of the contribution of each plant system to risk. This preliminary estimate of system risk provides an early indication of what parts of the plant have historically contributed to lost generation.

The tasks listed in Table 7-1 represent a one time level of effort that can be used to focus model development and can be updated as more detailed results become available.

Labor Estimates for Detailed Modeling Approach

In Table 7-2 the estimates associated with development of detailed fault trees for two systems are provided. Again, it is assumed that an application has been identified for which modeling of these particular systems would be of benefit.

In developing Table 7-2, estimates for system models and data analysis are provided assuming they are to be developed from scratch. If existing models are available, the labor estimates may be reduced. If modeling to a level of detail greater than that suggested in Section 3 is to be performed (e.g., with respect to I&C detail, common cause modeling, etc.), then the estimates should be increased. Similarly, models containing a large number of components requiring data may require more time, on a relative basis, than models containing very few components; thus, the estimates in Table 7-2 for data tasks should be considered to be representative of an average system.

For system models that are to be developed subsequent to the first few, a similar level of effort can be assumed for the model development, generation of results and interpretation. However, the effort required for data collection and analysis may be less for subsequent systems as a larger database of component types is assembled as each system is modeled and quantified. After about 10 models for systems have been assembled, it is expected that the data gathering and probability development tasks will have been largely completed with only the data assignment task remaining.

Labor Estimates for Train Level Supercomponent Approach

If it is elected to perform a system analysis using the supercomponent approach, it is estimated that both the model development and data collection effort will be less than that suggested in Table 7-2. For planning purposes, the “Identify plant derate categories” task in Table 7-2 will require the same level of effort while the system modeling and data efforts may be roughly half of those provided in Table 7-2, resulting in a total model development, quantification and interpretation effort of 5.6 person-weeks for two systems. While less than the detailed modeling approach,

- It is likely that system models developed later in the process will require as much data collection and analysis effort as for the earlier systems (unlike for the detailed fault tree approach), since data will be collected at the train level for each system as opposed to at the level of components and component types, which could be applied to multiple systems. (The data collection effort for the supercomponent approach may actually be higher than for the fault tree approach if train-level reliability information cannot be found, resulting in the need to manually combine individual component information to produce the supercomponent failure probabilities.)
- Not as many applications can be performed with the supercomponent approach due to less detail being available in the resulting models.

7.1.2 Resource Estimates for Applications

As discussed in Section 6, the principal purpose of a GRA is to support applications that benefit the plant or the enterprise. For a full calculation of the effort associated with a GRA, the time associated with applications must be included as one of the costs. However, the level of effort required to complete the applications is also a strong function of the application itself. Estimates of the level of effort required to support various types of applications are provided here for both the supercomponent and detailed fault tree approach. Three categories of applications are chosen to illustrate the variability in effort required.

Category One – component prioritization¹⁰

Supercomponent approach: It is estimated that completing applications similar in scope to component prioritization will take 1 person-week. This includes not only performing the ranking but documenting it in a manner that non-PRA/GRA practitioners understand, as well as participating in its presentation to and review by the plant staff. The prioritization can only be done to the supercomponent level, however, unless additional effort is applied to break the supercomponents into smaller pieces.

Detailed fault tree approach: The amount of effort required to complete the application is similar to that for the supercomponent approach, i.e., 1 person-week. However, the level of detail of the fault trees allows for a more refined (detailed) prioritization.

Category Two – cost-benefit analysis of proposed equipment modification

Detailed fault tree approach: The effort required to perform an analysis of a modification to the plant using detailed models can depend, to some extent, on the resulting cost-benefit ratio. Two examples are provided, one in which the change is far from the cost-benefit threshold selected by the decision makers, the other where the cost-benefit ratio may be marginally close to the threshold. In the first case, very simple back-of-the-envelope calculations can be performed using existing GRA output without modification of the models. For the latter case, a more refined calculation may be of value as input to a final cost-benefit analysis.

- *Modification's cost-benefit ratio is far above or far below the specified cost-beneficial criterion*

With detailed models, determination of whether a proposed modification has clear benefit or not can often be made without additional extensive analysis. Information will already be available regarding the value of each component in terms of its total contribution to lost generation (e.g., its risk reduction potential). Direct conversion of the risk reduction potential to lost Mwh can be performed by taking the product of the risk reduction potential and the total annual lost Mwh for the unit. By applying an average cost (\$) per Mwh to this estimated lost generation (and perhaps converting this value to a net present value (NPV) using an appropriate rate of return) a bounding estimate for the maximum value of the modification can be made. It is possible to provide the

¹⁰ Note that GRA models and results support component prioritization, however such an application should not be the sole reason for performing a GRA since such prioritization can be completed using other methods that require less up-front effort.

axes of the four quadrant plot for these importance measures with a scale in terms of NPV as illustrated in Figure 7-1. Figure 7-1 is a copy of Figure 6-10 with data point #32 highlighted for example purposes. For any component (data point) represented in the figure, a bounding estimate for the one-time cost of a modification proposed to improve reliability of the component can be determined by reading down from the data point onto the axis labeled “Approximate one time cost to eliminate risk.” Using data point #32 (feedwater recirc valves) as the example, the bounding estimate for modification cost is about \$2,000. If the estimated cost of a proposed modification intended to improve the reliability of the feedwater recirc valves is significantly greater than this bounding estimate, then no further analysis may be warranted and other options to address the generation risk of the affected component can be pursued. If the cost of the modification is substantially less than this bounding estimate, then sufficient information may have been provided with this simple calculation to justify the modification in terms of avoided lost generation.

Such an analysis requires only a review of the importance measures associated with the component that is subject of the modification. If multiple components are involved in the design change, then sensitivity studies using the cut sets from the GRA models for the affected systems can be performed (again without need to modify the models). The required effort for this type of analysis can be on the order of a few hours to a day.

If it is elected to implement the modification, then several extra days of effort may eventually be needed in order to permanently reflect the change in the models. But this effort could be completed as time permits or as part of the configuration and change control process (see Appendix C) and would not have to be made for the purpose of completing the cost-benefit analysis.

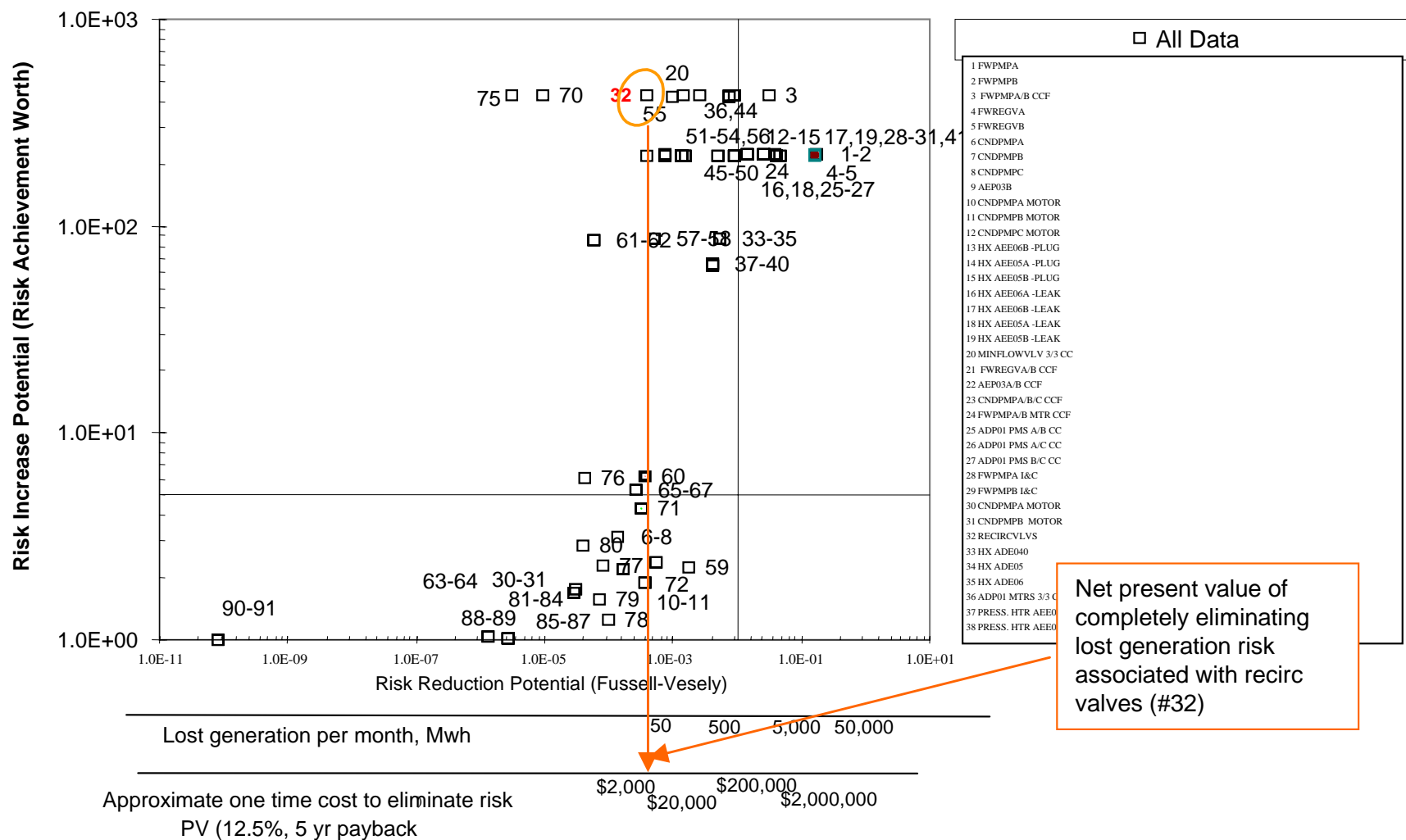


Figure 7-1
Simplified Cost Benefit Analysis Using GRA Results

- *Modification's cost-benefit ratio is close to the specified cost-beneficial criterion*

When a bounding analysis shows that the cost-benefit ratio may be marginally close to the threshold, a more detailed analysis may be in order, including incorporating the proposed change into the models, regenerating the results and performing an uncertainty analysis. Tasks that must be completed for this analysis include reviewing and modifying the logic models to determine if any changes to the logic are necessary to adjust for the proposed equipment, assigning failure rates to the proposed equipment to represent its assumed reliability, and generating results using the models and data. Actual costs must also be determined. Costs may include dollar costs of labor and equipment (making this a RIAM-type of application) and in terms of lost Mwh associated with plant down time to replace the current equipment with the new. However, changes to the models to include more detail should be minimal, given that the models are already developed with more detail than the supercomponent approach. The final evaluation will require estimating a “ΔMwh lost” associated with the change.¹¹ To provide a best estimate of this delta, an uncertainty analysis that includes both the original and revised models may be needed with correlations included to account for the similar responses of individual components that appear in both the original and revised models. For this comparison, the fact that the models are already detailed reduces the level of effort required to complete the cost-benefit analysis but requires some additional effort for the uncertainty analysis. The total effort for an analysis for which the original estimate of the cost-benefit ratio is close to the threshold would be on the order of 2 person-weeks.

Supercomponent approach: Performing a cost-benefit analysis will require more effort using the supercomponent approach than that required for component prioritization. Some of the tasks for this analysis are the same as those described for the detailed fault tree approach, such as reviewing and modifying the logic models, assigning failure rates, and generating results. Any changes made to the logic models will require more effort than for the fault tree approach, since less detail is included in the supercomponent approach (i.e., if the supercomponents are at the system level, and the equipment is a component within a train, it may be necessary to revise the models to include detail at the train level (at a minimum) or the component level (for more accuracy)). As stated before, it is assumed that the supercomponents are modeled at the train level, so such modeling changes will not be absolutely necessary. However, if modeling changes are not made to reflect detail at the component level then the probability of the supercomponent affected by the proposed modification will need to be adjusted to reflect the assumed change in reliability associated with the new design.

- *Modification's cost-benefit ratio is far above or far below the specified cost-beneficial criterion*

The technique described for the fault tree approach can also be used with supercomponents. However, because the supercomponent models may not have sufficient detail to directly represent the proposed design change, it is anticipated that some manipulation of the models and/or the supercomponent probabilities will be required. Thus, a level of effort of 2 days (0.4 person-weeks) is estimated.

¹¹ (Predicted Mwh lost, before change) – (Predicted Mwh lost, after change).

- *Modification's cost-benefit ratio is close to the specified cost-beneficial criterion*

Just as for the detailed fault tree approach, this situation will require more effort than the previous situation. At this point, it is highly likely that model manipulation (i.e., adding additional detail) will be needed. Thus, it is estimated that 3 person-weeks will be required to complete this type of analysis using the supercomponent approach.

Category 3 – Scenario analysis

Periodic operation may occur with components that are important to power generation operating in a degraded mode. The plant staff faces a choice of reducing power or shutting down to repair such a component, or attempting to continue at full power until such time as a load reduction can be scheduled more conveniently. The decision to take a certain outage early or postpone it may often depend on projected loads and the price of electricity. A scenario analysis can be performed using the GRA models to evaluate the tradeoffs between options.

Supercomponent approach: Depending on the complexity of the system represented by the supercomponent, the GRA model may or may not be able to provide a reasonable analysis in a timely manner. If the supercomponent is at the system level and the affected component is in one of a number of redundant trains, there may not be time to expand the models to the necessary detail to provide an evaluation. In this situation the risk will have to be approximated by adjusting the failure probability of the affected system in a manner that approximates the effects of the degraded component. If the supercomponents are at a train level, then an estimate of the change in the failure probability to reflect the degraded equipment may more easily be accomplished. Such an analysis may take several hours and would not require modification to the models or the need to resolve them, but simply changing the failure probability of the affected components for the different scenarios.

Detailed modeling approach: The analysis would be similar in effort to the supercomponent approach described above except that it would be easier to implement the changes to the failure probability of the degraded equipment as it would be represented explicitly in the model. An estimate of several hours of work would be appropriate for this analysis.

Table 7-3 summarizes the levels of effort required for the different categories of application, for both approaches. To simplify the comparison, all labor is assumed to be completed by a member of the PRA staff (although other plant and utility staff members may be involved depending upon the application).

7.1.3 Recurring Costs

For a GRA to be effective, there not only must be personnel available to implement and maintain the models, but support from management to address plant and corporate issues for which the GRA can provide useful input. Furthermore, as plant design changes are implemented and new operating experience is accumulated, it is useful to update the models and data to keep them current. Table 7-4 reflects an estimate of these recurring management and engineering efforts. The labor estimated in this table should be considered to be appropriate on an annual basis, and is the same for both the detailed fault tree and supercomponent approaches.

Table 7-3
Level of Effort for Applications

Application Category	Supercomponent Approach (Person-Weeks)¹²	Detailed Fault Tree Approach (Person-Weeks)
Component Prioritization	1	1
Cost-Benefit Analysis of Proposed Equipment Modification <ul style="list-style-type: none"> Bounding analysis value far from threshold Bounding analysis value near threshold 	0.4 3	0.2 2
Scenario Analysis	0.1 (if it can be completed in a timely manner and if supercomponents are modeled at train level)	0.1

Table 7-4
Resource Estimates for Recurring Efforts

Task	Person-Weeks					Total
	Group Mgr.	PRA	Sys. Engr.	Operator/ Op. Staff	Maint. Staff	
Program Management						
Coordination with other projects	1	2				3
General mgmt	2					2
Configuration/Change Control	1	5	10			16
Total	4	7	10			21

Combining the resource estimates from Tables 7-1 through 7-4, and including an estimate for the number of applications that might be performed each year, the total level of effort for each approach is presented in Table 7-5. The estimates in Table 7-5 reflect the assumptions stated earlier regarding the effort required for data collection and analysis. i.e., that such effort will be constant for the supercomponent approach but will decrease after 10 systems for the detailed fault tree approach. From Table 7-5, the supercomponent approach is estimated to require about 1.25 person-years to develop a complete set of models, and the detailed fault tree approach requires about 1.5 person-years. Maintenance and application of the GRA is estimated to require between $\frac{1}{2}$ to $\frac{3}{4}$ effective full time persons per year, with responsibilities split primarily between PRA personnel and system engineers.

¹² All days are for a member of the PRA staff, and are per application within the given category.

Table 7-5
Total Resource Requirements, Including Applications

Task	Person-Weeks					Total
	Group Mgr.	PRA	Sys. Engr.	Operator/ Op. Staff	Maint. Staff	
Model Development (20 systems, using information in Tables 7-1 and 7-2)						
Supercomponent	6	30	15	8	2	61
Detailed Fault Tree	7	40	17	9	3	76
Recurring Costs (annual - Table 7-4)						
Detailed or Supercomponent Approach	4	7	10			21
Applications (annual) 13						
Supercomponent (Table 7-3)		8				8
Detailed Fault Tree (Table 7-3)		6				6
Grand Total (over an average remaining plant life of 20 years)						
Supercomponent	86	330	215	8	2	641
Detailed Fault Tree	87	300	217	9	3	616

For a plant considering implementation of a GRA, the estimates of Table 7-5 should be adjusted for the types and number of applications planned for the GRA, as well as the actual number of systems that will be modeled. Combinations of techniques are also possible (e.g., 10 systems modeled using supercomponents, 10 systems modeled using detailed fault trees).

It should be noted that the greater level of effort estimated for model development using the detailed fault tree approach (approximately 25% higher) is balanced by the reduced level of effort required to support applications with detailed fault trees, and the higher number of applications that can be evaluated without the need for basic model refinements as would be required with the supercomponent approach. This is because many applications require an evaluation of risk impact at the component level, the level to which the detailed fault tree models are already developed. The models used in the supercomponent approach are generally less detailed and would require some modification (and therefore effort) before they could be used to support the same applications. Thus, as more “component level” applications are projected over time, or as the complexity of envisioned applications increases (such as for risk informed resource allocation decision making), the cumulative effort required using the supercomponent

¹³ Assumes one component prioritization type application, two scenario analysis type applications, two “near threshold” cost-benefit type applications and two “far from threshold” cost-benefit type applications per year.

approach may be greater than the effort required using the detailed fault tree approach over that same time period. Using the assumptions and estimates used for Table 7-5, the supercomponent and detailed fault tree approach “break-even” sometime between seven and eight years, after which the cumulative effort associated with the detailed fault tree approach drops below the cumulative effort for the supercomponent approach.

7.2 Cost-Benefit Assessment

GRA is a business driven effort that must pay for itself as it is performed. The preceding section provided estimates with respect to efforts directed at both the development of a GRA as well as on-going costs. In this section a comparison of the cost of these efforts with selected benefits expected from the application of the GRA to plant and corporate issues is presented. The assessment focuses on the detailed fault tree approach. While this approach requires more up front development effort than does the supercomponent approach, the supercomponent approach would be expected to be slightly less cost-beneficial as it costs more over the long run and may not be capable of realizing the benefits from all of the applications to which the detailed fault tree approach could be applied.

Several simplifying assumptions are made with respect to the cost and application of a GRA:

- All development efforts summarized in Table 7-5 are assumed to occur early in the project and can be treated as a one time up front cost. In fact, it is expected that development of the GRA models can actually be centered around specific applications, resulting in development on an as-needed basis over a relatively long period of time and paying for itself as development occurs.
- Both development and recurring costs (including applications) presented in Table 7-5 are assumed to be distributed equally among relatively experienced utility personnel and external consultants. This results in an assumed average labor rate of \$3,000 per week (\$150,000 per year).
- A discount rate of 10%/year is assumed over a 20 year period. This discount rate is assumed to apply to the recurring and application costs as well as the annual benefits.

Three sources of potential benefits are assumed regarding the applications that are estimated by the efforts presented in Table 7-5.

- Elimination of at least one relatively significant plant modification each refueling cycle that otherwise would have been performed without the assessment available from a GRA. Estimated capital cost of \$75,000 to \$150,000 each cycle.
- Identification of at least one component or component type that would not necessarily receive appropriate attention from a test and maintenance perspective. Without this attention, it is assumed that there is a small chance (10%) for the component to lead to an unplanned two-day outage sometime over the remaining life of the plant. At an estimated replacement power cost of \$300,000 per day, the avoided cost of this outage is \$60,000 ($0.1 * \$600,000$) assumed to occur at 10 years into the remaining life of the plant.
- Reduction in testing, maintenance and engineering of low risk significant systems and components such that the growth of the plant staff can be reduced by one to two persons without significant impact on plant generation. Estimated labor savings assumed to be \$100,000/yr.

It is believed that the estimates for these three potential benefits of application of a GRA may be modest in terms of the magnitude of the cost savings (e.g., avoided capital improvement costs can actually be significantly greater than assumed above, there may be more than one component that is identified as needing additional attention from a generation risk perspective, etc.). In addition, there are many additional potential applications of a GRA to which no benefits are being ascribed in this evaluation:

- Input to negotiations with the insurance provider regarding premiums.
- Providing quantitative input to bulk power traders on which they can assess the potential for meeting short term power sales and the need for hedging against unexpected outages.
- Assessment of the potential for successfully operating during peak power periods with degraded equipment in order to avoid costly power reductions.
- Focusing efforts on only risk significant components when performing operating experience reviews.
- Shortening outages by postponing maintenance activities for components with insignificant risk to production.

The following provides a comparison of the costs and benefits of a GRA based on the above assumptions.

Activity	Costs	NPV	Benefits	NPV
Model Development	\$230k	\$230k		
Annual Recurring	63k/yr	500k		
Applications				
Annual Labor	18k/yr	140k	\$100k	\$790k
Annual Capital			75k	590k
Avoided Outage			60k	21k
(one time @ 10years)				
Total NPV		\$870k		\$1,400k

Even assuming all development costs are up front and taking relatively limited credit for the potential benefits, the GRA is shown to have a benefit-to-cost ratio of more than one. The key to assuring the effort does pay for itself is, of course, in its applications. The more that management relies on insights from the GRA as input to decision making, the more applications will be performed and the greater the realized benefits.

7.3 Coordination with Other Projects

At any given time there will be many projects underway at a plant or within the plant's utility organization that could impact, overlap with, or benefit from the GRA effort. For example, enterprise-wide project prioritization efforts, equipment reliability investigations, and considerations of modifications to the plant for modernization purposes are all projects that should interact with the GRA project. Thus, it is imperative that the GRA project team remain cognizant of those other efforts, and that the development of the models be directly in support of specific applications.

In addition to plant and utility/enterprise-wide projects and programs, there are also industry programs of note with which contact should be maintained. These include nuclear asset management (NAM) [11] and life cycle management (LCM) or long-term planning (LTP) programs [12] and industry equipment reliability improvement efforts such as INPO's AP-913 [4].

To better ensure the coordination among the projects, maintaining the links between the GRA and other projects is explicitly included as a Program Management subtask. The Group Manager or the specified designee on the GRA project team should make efforts to provide and receive project status reports, participate in project update meetings held for the other projects, and proactively provide results from the GRA that may benefit the other projects. It is also important that GRA analysis incorporate any changes to operating or maintenance procedures or plant configuration implemented through the other projects, or at a minimum, that those changes be reviewed for potential impact (see the discussion of Configuration/Change Control in Appendix C).

8

FUTURE DEVELOPMENTS

Improvements and enhancements to the tools, techniques, and inputs to GRA may prove beneficial in increasing the cost-effectiveness of a GRA implementation and expanding the spectrum of applications supported.

Following are some candidates for future development.

- GRA automation as a module of RIAM (utility software requirements are under development by EPRI [29]).
- Use of software packages such as KB3 [25, 26] or other similar codes to develop GRA system models by system engineers or other plant staff for plant applicability.
- Additional sharing of industry modeling experience and results to further simplify GRA model development (a pilot application of GRA plant implementation is currently under way at Nebraska Public Power District's Cooper Generating Station).
- Enhanced interaction between GRA software and the Nuclear Asset Management (LAMDA) database under development by EPRI [27].
- Use the sources of data in Section 4 and Appendix A to help populate LAMDA.
- Use of LAMDA as a source of component reliability input to GRA.
- Inclusion in GRA of the effects of aging (reliability decrease as a function of time).
- Improvements in automation tools, including EPRI's Risk and Reliability (R&R) Workstation.
- Improvements to trip monitor to display predicted Mwh lost along with derate and plant trip frequencies.
- Development of generic system models and/or cut sets that can be quickly modified for application to a variety of plants.
- Application-specific industry-generic GRA process procedures (instruction manuals).
- Applications of GRA to other types of generating facilities.

As GRA implementation matures, these and other enhancements to the techniques and tools will enable plant staffs to more efficiently achieve the benefits from GRA at ever decreasing recurring cost.

9

REFERENCES

1. *LcmVALUE Version 1.5 – LCM Planning for SSC-LCM Planning Tool*, EPRI Software, August 2002. 1003455.
2. *Risk-Informed Asset Management (RIAM) Development Plan*, EPRI, June 2002. Report 1006268.
3. *Demonstration of Life Cycle Management Planning for Systems, Structures, and Components – With Pilot Applications at Oconee and Prairie Island Nuclear Stations*, EPRI, January 2001. Report 1000806.
4. Institute of Nuclear Power Operations Report AP-913, Revision 1, “Equipment Reliability Process Description,” 2001.
5. *Introduction to Simplified Generation Risk Assessment Modeling*, EPRI, February 2004. Report 1007386.
6. ASME, “Risk-Based Methods for Equipment Life Management: An Application Handbook,” CRTD Vol. 41, ASME International, 2003.
7. Minner, G.L., et al, “PEPSE and PEPSE-GT Volume 1 Manual, User Input Description”, SCIENTECH, Inc., Idaho Falls, ID, 2002.
8. *Trip Monitor Customization and Implementation Guideline*, EPRI, January 2004. Report 1009112.
9. North American Electric Reliability Council (NERC), “Generating Availability Data System, Data Reporting Instructions,” October 2003.
10. U.S. Nuclear Regulatory Commission Title 10, Code of Federal Regulations, “Requirements for monitoring the effectiveness of maintenance at nuclear power plants,” 10CFR50.65, first issued July 10, 1991; last amendment December 23, 1999 (64 FR 72001).
11. North American Electric Reliability Council (NERC), “pc-GAR for Windows”, Release 2.04 v11, 2001.
12. U.S. Nuclear Regulatory Commission, “PRA Procedures Guide,” NUREG/CR-2300, January 1983.
13. ASME, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Application,” Report ASME RA-S-2002, April 5, 2002.
14. *PSA Applications Guide*, EPRI, August 1995. TR-105396.
15. U.S. Nuclear Regulatory Commission, “Fault Tree Handbook,” NUREG-0492, January 1981.
16. Nuclear Energy Institute (NEI), “Industry Guidelines for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants,” NUMARC 93-01, 1993.

References

17. U.S. Nuclear Regulatory Commission, "Evaluation of Core Melt Frequency Effects Due to Component Aging and Maintenance," NUREG/CR-5510, 1990.
18. *SYSIMP version 2.0, Users Manual*, EPRI, 2001.
19. Reliability Engineering & System Safety, 72 (2001) pg. 193-212, A New Importance Measure for Risk Informed Decision Making.
20. ASME, PVP Vol 296, pg. 153-159, Top Event Prevention in Complex Systems, 1995.
21. *Life Cycle Management Economic Tools Demonstration, Risk-Informed Long-Term Planning for Equipment*, EPRI, March 2003. EPRI Report 1007931.
22. Kee, E. et. al., "Using Risk-Informed Asset Management for Feedwater System Preventative Maintenance Optimization," Journal of Nuclear Science and Technology, Vol. 41, No. 3, p. 347-353, March 2004. (also, "Extensions to On-line Maintenance Using BOP PRA Results: Initial Deployment in STPNOC Units 1 and 2," PSAM6, 6th International Conference on Probabilistic Safety Assessment and Management, Elsevier Science, Ltd. June 23-28, 2002.)
23. The Standard Nuclear Performance Model – A Process Management Approach – Revision 4, NEI Nuclear Asset Management Community of Practice Report, December 2003.
24. *Long-Term Planning Benchmarking Results*, EPRI, September 2004. Report 1009752.
25. Gallois, M. and M. Pillière, "Benefits Expected From Automatic Studies with KB3 in PSAs at EDF," PSA99, Washington, August 1999.
26. Bouissou, M., S. Humbert, S. Muffat, and N. Villatte, "KB3 Tool: Feedback on Knowledge Bases," ESREL 2002, Lyon (France), March 2002.
27. *Nuclear Asset Management Database – Phase 2: Prototype LAMDA (Long-term Asset Management Database)*, EPRI, December 2004. Report 1009633.
28. Celedonia, G., et al., "Profit-Centered Maintenance," P/PM Technology Magazine, April 1997.
29. *Risk-Informed Asset Management (RIAM) Software Requirements*, EPRI, Report 1009632 (in progress).
30. U.S. Nuclear Regulatory Commission, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR 50.54(f)," Generic Letter No. 88-20, November 23, 1988.

A

GRA MODEL DATA SOURCES

Data inputs to GRA and trip models may include the following. The references in this section for each type of data are listed roughly in order of least to most effort needed to extract useful information related to the failure probability being addressed.

Random failures – These are failures of individual components due to random causes.

Failure rates – plant-specific sources

- Plant-specific PRA. Contains processed data in terms of failures per demand and failure per operating hour for the purpose of performing accident sequence quantification following a plant trip. Largely includes estimates and uncertainty distributions for safety-significant equipment but in many cases includes rates for balance-of-plant equipment that is credited in performing the mitigating functions modeled in the PRA. PRA failure rates are most likely generated from a number of the plant-specific and generic sources that are referenced below.

Failure rates – generic sources

Generic failure rates and uncertainty distributions referenced in PRAs can be found in the following references:

- NUREG/CR-4550 Vol 1 Rev 1, Analysis of Core Damage Frequency: Internal Events Methodology, 1990
- NUREG/CR-5500 Vol 1-12, 1998-2002
- NUREG/CR-1715 Vol 1-3, Component Performance Studies, 1998
- IEEE-500 Standard, 1984
- European Reliability Database, EIReDa, 1998.
- WSRC-TR-93-262 Rev 1, Savannah River Site Generic Database Development, 1998

Other generic data sources that have been used in PRAs include (not all of these have information pertaining to uncertainty distributions):

- WASH-1400, Reactor Safety Study, 1974
- NUREG/CR-2815, PRA Procedures Guide, 1984
- NUREG/CR-4639, NUCLARR, 1990
- EGG-SSRE-9639, Component External Leakage and Pipe Rupture Estimates, 1991

- EGG-SSRE-8875, Generic Component Failure Data Base for Light Water and Liquid Sodium Reactors.
- ALWR Database

A summary of the content and limitations of many of these references is provided in NUREG/CR-6823, Handbook of Parameter Estimation for Probabilistic Risk Assessment. Other proprietary sources of failure rates are available from databases developed by private firms in the business of providing risk assessment consulting services.

Should it be considered necessary to generate failure rates for specific components, a variety of generic and plant-specific sources of data are available.

Raw data – generic sources

- EPIX (Equipment Performance and Information Exchange System)

The INPO computerized database containing industry wide equipment failures reported for systems falling under the maintenance rule. This database includes LERs as well as information on system design and causes of failures. Estimates are included for number of demands and operating hours for safety-significant systems.

- NERC-GADS (North American Electric Reliability Council – Generating Availability Data System)

Database maintained by NERC into which all U.S and Canadian nuclear power facilities report along with conventional units for most investor owned utilities. Number of failures leading to unit trips and derates for collections of facilities available along with average outage time for the units. Contains cause codes as opposed to detailed information on the causes of failures. The reference includes sufficient design information to screen data for units having similar design features. Exposure is reported in terms of unit operating hours.

Raw data – plant-specific sources

- Maintenance Rule records

Under 10CFR50.65, each plant is keeping records of functional failures that occur to components that fall under the scope of the maintenance rule.

- NERC-GADS reports

Each plant creates periodic reports for submittal to NERC-GADS which identifies all failures leading to lost generation and assigns cause codes to each.

- Computerized Maintenance Management System (CMMS)

Many plants are implementing computerized systems for the purpose of maintaining design, maintenance and performance information on power plant components. Modules within these systems can be a source of information for input to a data analysis task.

- Corrective Action documents

All nuclear power facilities have in place a corrective action program that record deviations or non-conformances with respect to plant, system and component operation. Documents supporting this system include corrective action reports and work orders.

- Control Room and System Logs

A record of plant and system operation is often kept in the form of log books which record plant operating events, changes to system configuration, switching and tag out.

- Surveillance, Testing and Maintenance procedures

Operation of a nuclear power plant is performed using reviewed and approved procedures. These procedures can be used to identify failures and as a basis for estimating number of demands and operating hours.

If plant-specific data is collected, development of failure probabilities and distributions for systems, trains and components for input to a GRA will use failure rate over time, λ , or per demand, p :

$$\lambda = n/t \quad \text{or} \quad p = n/d$$

where

λ – failure rate in units of failures per unit time

p – failure probability in units of failures per demand

n – number of observed failures

t – time over which observations are made

d – number of demands over which observations are made

The confidence intervals for λ are derived as follows:

$$\lambda_u = \chi^2_{(1-\alpha)} (2n + 2)/2t$$

and

$$\lambda_l = \chi^2_{(\alpha)} (2n)/2t$$

where

λ_u – upper two sided confidence bound

λ_l – lower two sided confidence bound

α – confidence bound (e.g., $\alpha = .05$ and $1-\alpha = .95$)

χ^2 – chi squared distribution

The confidence intervals for p are

$$\alpha = \sum_{d=0}^f \binom{d}{n} p^n (1-p)^d \text{ lower confidence limit}$$

and

$$\alpha = \sum_{d=f}^n \binom{d}{n} p^n (1-p)^d \text{ upper confidence limit}$$

where

f – the number of failures that satisfy this relationship.

In some cases there may be insufficient observed failures (e.g., near zero) or there may have been the unexpected occurrence of several failures over a short period of time (e.g., a run of bad luck). Further, for a single facility, there may be only a limited number of demands or operating hours to derive a statistically significant set of failure probabilities. In these situations, if it is felt that generic sources of data are more representative of the expected performance of the components in question, then updating the failure rates with Bayesian analysis may be in order. The Bayesian update process consists of three steps:

- Select an appropriate generic prior distribution
- Develop a likelihood function from plant-specific data
- Generate a posterior distribution with the following relationship:

$$f(\lambda|E) = f(\lambda_i) L(E| \lambda_i) / \sum f(\lambda_i) L(E| \lambda_i)$$

where

$f(\lambda|E)$ – posterior distribution

$f(\lambda_i)$ – prior distribution (from generic data)

$L(E| \lambda_i)$ – likelihood function (from plant-specific data).

Techniques for deriving plant-specific failure rates and probabilities and performing Bayesian analysis, and examples of such analyses, are found in numerous references. Several directed specifically at performing analysis of nuclear power plant data are

- NUREG/CR-2300, PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, 1983, Chapter 5 – Development of a Database
- EPRI 1002936, Reliability and Preventive Maintenance: Balancing Risk and Reliability, 2002, Chapter 6 – Reliability Data

- NUREG/CR-6823, Handbook of Parameter Estimation for Probabilistic Risk Assessment, 2003.

Common cause failures – These are failures of multiple components that occur closely in time, occurring as a result of the same mechanism. Typically, components of the same type (e.g., air operated valves, or motor operated valves), that are exposed to the same operating conditions (e.g., system pressures, flows, external environment) and maintenance practices (e.g., preventive maintenance (PM), predictive maintenance (PdM), testing and surveillance) are included within the same common cause component grouping. Common cause factors represent the conditional failure probability of multiple components given the failure of a single component, due to common design, maintenance, operating, or environmental conditions impacting all like components. (Consult the references included here for general information about the treatment of common cause failures in logic models.)

Failure rates – plant-specific

- Plant-specific PRA. Grouping of plant components for the purpose of recognizing the potential effects of common cause failure will have been performed as a part of quantification of the plant-specific PRA. The majority of this work would have been associated with safety-significant mitigating systems that would be needed in response to a plant trip. To the extent that balance-of-plant equipment have been modeled for the purpose of mitigating a transient, common cause failure rates should have been developed for major components associated with these systems.

Failure rates – generic

For balance-of-plant systems that have not been modeled in the PRA, there is likely to be insufficient operating experience at an individual plant to have statistically significant information regarding the potential for common cause failures. If not available for similar component types in the plant-specific PRA, then generic reports are available that estimate common cause factors for different component types:

- NUREG/CR-4780 (EPRI NP-5613) Vol 2, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, 1988.

In this report, an estimate of a common cause β factor for several component types (e.g., pumps, MOVs, AOVs) is provided. An overall β factor of 0.1 is considered to be representative for a spectrum of component types.

If it is elected to generate common cause values for specific balance-of-plant components, there are a number of sources of information containing raw data that may be of use.

Raw data – generic

The following sources have assembled information for potentially safety-significant components that are credited in response to a transient. To generate common cause information for balance-of-plant equipment, it may be necessary to identify similar components in the data provided in these references for analysis.

- NUREG/CR-6268, Common Cause Failure Database and Analysis System, Vol. 1-4, 1998.
- NUREG/CR-4780 (EPRI NP-5613) Vol 2, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, 1988.
- EPRI NP-3967, Classification and Analysis of Reactor Operating Experience Involving Dependent Events, 1985.
- NUREG/CR-3867 EGG-2324, Data Summaries of Licensee Event Reports of Inverters at U.S. Commercial Nuclear Power Plants 1/1/76 to 12/31/82, 1984.

Maintenance and test unavailability – Components may be taken out of service (and therefore become unavailable to perform their intended task) due to planned or unplanned testing or maintenance. Unplanned maintenance and testing times are often incorporated into the estimation of a component's mean time to repair given its failure (see next bullet). Intervals for planned maintenance and testing (i.e., the number of times per year a component is out of service for planned maintenance or testing) are dictated by such documents as maintenance procedures, vendor manuals, etc. The typical duration a component is out of service for the test or maintenance activities is a function of the test/maintenance activity, and should be known to the plant staff after such test/maintenance procedures have been completed some number of times. Taking a component out of service for planned test or maintenance may or may not directly result in a plant derate.

Maintenance probabilities – plant-specific

- Plant-specific PRA. The PRA may contain estimates for fraction of time out of service associated with individual trains of balance-of-plant systems credited in the models.
- Expert opinion. The operations, maintenance and engineering staff may be able to make estimates of the time out of service due to routine maintenance based on experience.

Maintenance probabilities – raw data

- Maintenance and testing procedures or work orders. Review of plant documents that support maintenance activities (including switching and tagging orders) can provide sufficient information to estimate the fraction of time a train of equipment is out of service during power operation.

Repair times – On loss of a piece of equipment that supports power generation, the MTTR supports two variables that are input to a GRA, one associated with determining the frequency of trips or derates the other associated with determining the consequences. In estimating the frequency of trips and derates, components which by themselves leave the plant at power after their failure (either full power or a derated level), additional failures must occur before a plant trip or more significant derate results. The mission time for these additional failures is the MTTR of the component that initially failed. In estimating the consequences of component failures, for components that lead directly to a plant trip or derate the MTTR is used as one of several inputs to determining the total lost Mwh (see Recovery Time below).

Repair rates – plant-specific sources

- Plant-specific output from NERC-GADS. For publicly owned utilities reporting to NERC, the pc-GAR software provides a summary of information related to trips and derates for each

of the utilities units. One of the outputs is the average duration of the outage by cause code. Where the cause codes can be related to specific systems, trains of equipment or components, the average duration can be used to estimate a MTTR (note that this may be an over estimate as the duration can include time to return to power).

- Plant-specific PRA. In the quantification of accident sequences of the PRA, there are a number of components for which repair and recovery evaluations are performed. These often include
 - Onsite and offsite AC power sources
 - Major pumps and valves associated with long term accident scenarios (e.g., decay heat removal).

To the extent these accident sequence evaluations can be shown to apply to power operation, they may be applicable to developing a MTTR for similar balance-of-plant equipment.

- Expert opinion. Interviews of plant maintenance and operations personnel that have experience with the types of failures and repairs generally needed for equipment in balance-of-plant systems may be able to provide reasonable estimates of the MTTR for these types of components.

Repair rates – generic data

- NERC-GADS output. The pc-GAR software provides a summary of information related to trips and derates averaged over the industry for plants having characteristics that can be specified by the user. This information includes number of forced outages and their average duration by cause code. This average duration can be used to approximate a MTTR for equipment associated with given cause codes.
- Published PRAs. Generic assumptions are made in a number of PRAs regarding the ability to repair failed equipment following a transient. For example, Volume III of WASH-1400 provides an estimated MTTR for major mechanical equipment of 19 hours (such as pumps) and electrical equipment of 7 hours. Generic assumptions such as these can be used to make rough estimates for the MTTR of balance-of-plant equipment used in a GRA.
- Screening values. Where estimates are not available a bounding value may be used to approximate the MTTR. For many components, a value of 24 hours may be adequate, which is similar to the mission time of components currently modeled in the PRA.

Repair times – raw data

- NERC-GADS input. Each plant providing input to NERC generates a periodic report that contains details of each plant outage (trip or derate). The raw data associated with these reports can be useful in generating a MTTR for specific systems and trains of equipment.
- Maintenance procedures, testing procedures, work orders. Review of plant documents that support maintenance activities (including switching and tagging orders) can provide sufficient information to estimate the MTTR for selected trains of equipment that are periodically removed from service during power operation.

Human reliability (human error) – Operating experience indicates that human errors contribute to component, system, and plant outages. These errors may be as a result of failing to following operating procedures, failing to follow test or maintenance procedures or can be a result of inadvertent unintended actuation of equipment. In some cases the error results in an active change in state of a component, to a condition that leads to a power reduction. In other cases the error is one that leaves a component in an undesired state following test or maintenance, so that the component does not operate as required at some later time. Human error probabilities (HEPs) can be estimated through a variety of techniques, known collectively as Human Reliability Analysis (HRA). In most models, errors of “omission” (for example, omitting a step in a procedure, thus failing to discover an incorrect system configuration or failing to initiate (or stop) operation of a component or change its state) are the errors of primary interest. Errors of “commission” (such as starting a wrong pump and selecting the wrong display on a panel) are usually not included, as these are typically insignificant compared to errors of omission for an experienced operator or plant personnel. Several of sources of the probability of human error are available to develop human error failure rates for use in GRA as discussed below.

Plant-specific sources

- Plant-specific PRAs. Some human errors considered in a PRA can be directly transferred to GRA use. These are restoration errors after maintenance or tests that lead to failure of a component or a train when required to perform its function. Other human errors such as recovery errors associated with restoration of a component can be adjusted for the different operating conditions and stress levels in a GRA. Therefore, it is recommended that human error information from the existing PRA be used where applicable.
- Plant experience: Explicit quantification of human error failure rates may be possible at some plants if sufficient information is present associated with the number of demands and failures associated with an action. However, it is often the case that explicit data associated with human failure rates are generally limited. The human error rates derived using this data are typically statistically insignificant and thus must be used with caution. The plant experience information can also come from training exercises such as those covered in job performance monitoring (JPMs), in the simulator or from operator interviews.

Screening HEPs

Screening values for human error probabilities associated with operator errors are often used in plant risk assessments for the purpose of prioritizing which human actions warrant more detailed evaluation. The screening values are typically conservative estimates of human error failure likelihood and are generally assigned based on the analyst’s understanding of the complexity of the action, the timing of action, and the environment to which the operators are exposed when performing the action. Other factors of consideration by the analyst (such as training, availability of cues and consequences of action failure) also come into play when assigning screening values. Operator interviews can be used as input to assigning screening values but analysts must be aware that operators may be optimistic regarding the correct performance of an action. Because many PRAs assign screening HEPs to credited operator actions, it is worthwhile to review the basis for these values and then adjust them if necessary if the operator actions are also included in the GRA.

A rule of thumb when assigning screening HEPs is that the HEPs should always be greater than what the analyst perceives the true failure likelihood to be (in other words, if the analyst believes the true HEP will be roughly $1\text{E-}3$ per action, a screening value greater than $1\text{E-}3$, such as $1\text{E-}2$, should be used). Also, the screening values must be derived using a consistent application of the assessment factors described above, with the basis for all screening HEPs carefully documented.

Screening values can also be systematically obtained by using the HRA methodologies described below. The ASEP methodology provides a methodology for quantifying screening HEPs for both pre- and post-abnormal event actions. The screening methodology is less rigorous than the nominal ASEP methodology and produces higher HEPs. A basic screening HEP of 0.03 for each step of a pre-abnormal event action is recommended. For post-abnormal event actions, screening HEPs are provided for diagnosis errors as well as post-diagnosis action errors. The diagnosis HEP is a function of the available time to diagnose an abnormal event while the post-diagnosis or action HEP is based on the action type (skilled, rule or knowledge-based actions). Skill-based actions are memorized actions, rule-based actions are proceduralized actions and knowledge-based actions are non-proceduralized actions requiring interpretation and analysis of the cue. Recommended screening values for skill and knowledge based action steps are 1.0 while the screening value for rule-based actions is .05 per step.

The THERP methodology (also described below) also provides screening values for diagnosis error and post diagnosis error. Like the ASEP methodology, the screening diagnosis HEP is a function of time available to diagnose the cue. Recommendations for rule and knowledge screening HEPs are .05 (w/o recovery) and 1.0, respectively. Other methodologies such SHARP (Systematic Human Reliability Procedure, EPRI-NP-3583, February 1984) also provide screening estimates for skill, rule and knowledge-based actions.

Generic HRA Methodologies

To address the limited plant experience data available in the industry associated with human errors, a majority of the human error failure rates are generated using human reliability analysis methodologies. Although these methodologies are primarily used to evaluate operator actions during accident mitigation, they can be used for assessing operator actions for maintaining plant operation as in a GRA as the factors considered for human reliability are similar. These factors include training, procedures, availability and clarity of cues, availability of time to perform the actions, environment, workload and stress. If it is elected to develop human error probabilities for at power situations, three methodologies recommended for use in a GRA are listed below.

- ASEP (NUREG/CR-4772, Accident Sequence Evaluation Program Human Reliability Analysis Procedure, 1987)

ASEP is a human reliability methodology is designed to systematically quantify human actions. The ASEP methodology is based on the more detailed THERP (discussed below) methodology and is widely used in PRAs. This is due to the fact that it is relatively easy to implement and it produces human error probabilities that are comparable to other more detailed methodologies. Included in the ASEP methodology are screening and nominal approaches to quantifying pre- and post abnormal event human error probabilities. The ASEP methodology is ideal for deriving human error probabilities for human actions in a GRA for reasons cited above.

- THERP (NUREG/CR-1278), Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, 1983

The Technique for Human Error Rate Prediction (THERP) was developed to provide an approach to quantifying human error based on analysis of each task of the operator action. This methodology is typically used in PRAs where more accurate human error probability estimates are desired. Implementation of the THERP methodology requires identification of all tasks (original and recovery) in the operator action, assigning the appropriate basic human error probability (BHEP) for each task using lookup human error probability tables, generating a human error event tree, and quantifying the event tree to obtain the resulting human error probability. Because each individual task must be evaluated, the analysis required may be quite involved to obtain a more accurate estimate. For the purposes of GRA, however, this degree of accuracy of the human error estimates may not be needed and thus this approach may not be cost justifiable. Nevertheless, if accuracy is needed, this approach would be ideal.

- CBDTM (EPRI TR-100259), *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*, 1992.

The Cause-Based Decision Tree Methodology (CBDTM) is designed to systematically assess the factors affecting operator cognitive response to an abnormal event. This methodology is typically used for post-abnormal event actions (i.e., actions that are taken in response to a failure). In this approach, the analyst goes through eight caused-based decision trees to derive the resultant human error probability for each decision tree. Each caused-based decision assesses a specific human-machine interface (i.e., display failure, attention failure, interpretation failure, etc.) and each branch in the event tree represents a failure cause and an associated human error probability. The resultant human error probabilities for each tree are summed to obtain the overall cognitive failure probability. The CBDTM methodology is relatively easy to use with inputs from operations. As the methodology only evaluates the cognitive portion of the operator error, it should only be used when the action portion of the operator action is considered to have negligible impact on the results.

Recovery times – The amount of lost production (Megawatt-hours) associated with a component failure or unavailability is calculated by knowing the level of derate associated with the component outage, as well as the length of time the component is unavailable and the plant is at a reduced power level. The definition of “recovery” time includes the “repair” time for the specific components that contribute to each trip or derate (see the discussion of sources for MTTR above) plus the time needed to restore the plant to full power. For trips or derates in which failures of multiple components are required, the MTTR assigned to the total recovery time may differ from the MTTR used in determining the frequency of the trip or derate. Section 5 describes the variance in MTTR when used to determine frequency of a derate as opposed to repair time. Basically, the MTTR used for the frequency determination is associated with the component that fails first in the sequence of events (the component assigned a frequency term for its failure likelihood). If the redundant components can operate for the length of time required to repair the first failed component (i.e., for the MTTR of the component), the first failed component will be restored to service and available, and the derate will be avoided. If, however, all components in the sequence fail to operate for that length of time, the recovery time for the

set of components must take into consideration the fact that each component within the sequence has its own MTTR. To assign a MTTR in order to assess the recovery of the set of failed components, a decision is needed as to whether to use the sum, average or the maximum of the individual MTTRs comprising the set of components whose failures resulted in the outage. That decision is left to the analyst, as it is dependent upon the characteristics of the situation.

For restoring the plant to power following the repairs, the following sources of data are suggested:

Recovery time – plant-specific sources

- Plant procedures/Expert opinion – Plant operating practices often dictate the rate at which power is changed during startup and shutdown. Procedures or operator interviews associated with these activities can be used to estimate the time required to return to full power.
- Plant-specific output from NERC-GADS. The pc-GAR software provides a summary of information related to trips and derates for each of a utility's units. One of the outputs is the average duration of the outage, segregated by cause code. This average duration includes both the mean time to repair and the return to power and can be used to estimate a recovery time following load reductions to specific levels.

Recovery time – generic sources

- NERC-GADS output. The pc-GAR software provides a summary of information related to trips and derates averaged over the industry for plants having characteristics that can be specified by the user. This information includes number of forced outages and their average duration by cause code. This average duration can be used to approximate restoration times for trips and derates associated with given cause codes.

Raw data – plant-specific sources

- NERC-GADS input. Each plant providing input to NERC generates a periodic report that contains details of each plant outage (trip or derate). The raw data associated with these reports can be useful in generating return to power estimates following repair of equipment causing a trip or derate.
- Operating reports, plant trip reports, control room logs. Monthly reports are submitted to the NRC and plant vendors regarding plant production. These reports will often contain information regarding the duration of the outage. Plant trip reports and control room logs will also contain such information.

B

QUANTIFYING GRA RESULTS – SUPPORTING INFORMATION

Section 5 refers to adjustments to GRA results that can be made to minimize over- and under-estimation of the results arising due to modeling issues. This appendix provides more detail on the methods introduced in that section.

B.1 Eliminate Duplicate Failure Combinations (Section 5.1.2.1)

A way to eliminate the duplicate cut sets discussed in Section 5.1.2.1 is to use a procedure called “delete term.” This technique is typically included in most PRA software packages either as a part of accident sequence quantification or cut set editing. The procedure eliminates subsuming terms between two expressions containing similar combinations of failures. The procedure is used in GRA to segregate cut sets into their appropriate end states (derate levels or bins). The following example demonstrates the delete term procedure. In this example, a dc distribution panel contributes to both 50% load reduction as well as to full plant trip through the effects of its failure on two different systems. The cut sets leading to the plant trip are deleted from the cut sets for the 50% load reduction. The final cut sets remaining after the delete term procedure are shown in the 50% reduction (resultant) column below. As shown, the dc panels that cause the plant trip effectively are removed from the 50% load reduction bin so as to prevent an overestimation of their contribution to risk.

50% reduction	Plant Trip	50% reduction (resultant)
Pump A Fails to run +	MSIV A Closes +	Pump A Fails to run +
Pump B Fails to run +	B Closes +	Pump B Fails to run.
Panel A Fails to function +	Panel A Fails to function +	
Panel B Fails to function	Panel B Fails to function	

To properly perform the delete term procedure and obtain the adjusted cut sets for each load reduction level during the system quantification itself, cut sets in lower derate levels must be eliminated if they also appear in a higher derate level. As further illustration, a cut set contributing to three derate levels (33%, 50% and 100%) would be eliminated from the 33% and 50% derate levels (i.e., it should only be in the 100% load reduction level).

B.2 Treating Differences between the Trip and Derate Frequencies of the Models and Operating Experience (Section 5.1.2.2)

Common modeling approximations may result in under- or over-estimation of component contributions to trip and derate frequencies. This section of the appendix provides more detail for the methods mentioned in Section 5.1.2.2 (and Section 3.2.2.1 (for adjusting these approximations).

B.2.1 Models with Operating Components having Failures Expressed in Units of Annual Frequencies

One approximation that is made to develop models that are appropriate for modeling the plant remaining at power for significant periods of time is to assign a relatively long mission time to the normally running components (e.g., a year). While appropriate for single trains or components that may lead to a given level of load reduction, this approximation results in combinations of failures or cut sets having multiple events with this mission time and resulting mathematical units that may not be considered logical (e.g., $1/\text{year}^2$). Models containing operating component failures with annual frequency units, when quantified, could overestimate the frequency of the failure of the system due to this modeling approximation. As an example, if both pumps in a feedwater system with two 50% trains are assigned a yearly mission time, then a plant trip requiring failure of both pumps would be overestimated. Following failure of the first pump (over the course of a year), repairs to the failed pump would be initiated and the exposure time of the second pump would be much less than a year. To prevent a plant trip, the second pump must run for only the time necessary to repair the first pump and return it to service. Therefore, assuming a yearly mission time for both pumps would overestimate the system trip frequency. Thus, it may be worthwhile to adjust the mission time of the second pump. This adjustment can be easily made by applying an adjustment factor equal to the ratio of the mean time to repair and restore (MTTR) Pump A to service, and 365 days (this ratio is represented as $\text{MTTR}_{\text{hours}}/8760$).

On making this adjustment, however, the contribution of failure of the two components may now be underestimated. This is because either of the two components may fail initially resulting in two possible combinations of a component failing to operate for a year, with a plant trip resulting if a failure of the second component occurs during the mean time to repair and restore the first component to service. For this example then, a factor of 2 must also be applied to increase the frequency of this combination.

When common cause events dominate, only one of the two corrections would apply. The common cause event representing both component failures should be adjusted to reflect the fact that the mission time for operation of the first component may be one year, but the exposure time for the second component to the common cause mechanism is only the mean time to repair for the failed component. The same adjustment factor used for failure of both components ($\text{MTTR}_{\text{hours}}/8760$) should be applied to the component failures due to common cause mechanisms. That the combinatorial adjustment is not required for the common cause events reflects the fact that they are typically defined as the failure of all components in a common cause group without regard to order, and the common cause value already reflects how many combinations are in the group (e.g., two in the case of a two train feedwater system).

The above example is for two operating trains. In general the factors applied to combinations of two or more operating components are as follows:

- Multiply the cut set value by (number of frequency events in the cut set – 1) x $(\text{MTTR}_{\text{hours}}/8760)$
- Multiply the cut set value by (number of combinations of events having frequency values)
- Multiply common cause failure (CCF) events by $\text{MTTR}_{\text{hours}}/8760$.

A way to apply the correction factors to each cut set is to add an event representing the correction factor directly to the cut sets. This could easily be performed using available PRA cut set editing software with recovery rules corresponding to the adjustments stated above.

B.2.2 Models with Operating Components having Only 24 Hour Mission Times

A typical balance-of-plant PRA fault tree model contains operating component failures having twenty-four hour mission times. These short mission times can be used initially to quantify the GRA models to produce the cut sets. However, conversion of these results to longer mission times associated with power operation will be needed. To accomplish this conversion, it may only be necessary to apply a factor to each cut set associated with the appropriate mission time (e.g., a year). This correction factor would be equal to the desired mission time divided by the mission time associated with the normally running events (e.g., 8760h/24h). The adjustment factor also could be incorporated directly into the fault tree models through an AND gate at the top of each system fault tree.

Consider a feedwater system with two 50% trains, where each train has one pump (pump A and pump B). The mission time of the first pump (pump A) would effectively be adjusted from 1 day to 365 days with the correction factor. Further adjustment of the second pump, pump B, mission time may then be adjusted from 1 day to the mean time to repair/restore pump A should the mean time to repair the pump be significantly different than a day. To prevent underestimating the final frequency, a factor of 2 is applied to account for the fact that there are two scenarios with respect to the order of failures: pump A fails to run for a year and then pump B fails during the repair time of pump A, and visa versa. For pump failures due to common cause mechanisms, the adjustment factor would include the factor to convert the daily mission time of one pump to an annual mission time and second factor to convert the now annual mission time of the second pump to the mean time to repair of the failed pump (mttr/year).

In general, the factors applied to the failure combinations for two or more operating component failures with 24 hour mission times are as follows:

- Multiply each cut set value by 365 days
- Multiply each cut set value by (number of frequency events – 1) x $(\text{MTTR}_{\text{hours}}/24 \text{ hours})$
- Multiply each cut set by (number of combination of events having frequency values)
- Multiply CCF events by $(\text{MTTR}_{\text{hours}}/24 \text{ hours})$.

The adjustment factor can be easily applied to the cut sets using available PRA software packages.

B.2.3 Models Containing Both Frequency and Mean Time to Repair Events

A way of avoiding cut sets having multiple components with an annual mission time is to replace the failure event for each normally operating component with the union of an event having the desired mission time associated with power operation (e.g., one year) and one representing the same failure only over a shorter period representing the mean time to repair. Fault tree models taking this approach to system quantification will yield illogical cut sets that must be eliminated in order to avoid overestimating the resulting frequency. The logical cut sets will be those that contain a component failure with an annual frequency and the remaining component failures having mean time to repair mission times, while the illogical cut sets will be those containing multiple events with units of frequency, or containing no frequency events at all.

Going back to the feedwater system example with two 50% operating trains, an event representing pump A failure with a mission time equal to the mean time to repair pump B would be combined using the Boolean logical OR function with the pump A operating failure having a year mission time. Another combination exists by switching A and B in the above sentence. Since both pumps are required to fail to cause a plant trip in this example, a plant trip logic model will be developed and quantified to produce cut sets. This quantification approach will result in cut sets with three types of characteristics: those that are logical and can be used to represent the frequency of the plant trip, those that contain two terms each having mission times of a year and are illogical, and those containing two mean time to repair terms, and are also illogical. The illogical cut sets should be deleted. In other words, the logical cut sets contains a pump failure with annual frequency and a pump failure with a mean time to repair mission time while the illogical cut sets contain both pumps with either annual or mean time to repair mission times.

For systems with two or more operating trains, the following would apply:

- Delete all cut sets containing two or more annual mission time events
- Delete all cut sets containing only mean time to repair events
- Adjust all mean time to repair mission time events to the correct mission time based on the mean time to repair of the annual mission time event (e.g., number of mean time to repair events x MTTR/24h)
- Multiply CCF events by (mean time to repair/8760 if annual mission time event and mean time to repair/24 if daily mission time event)

Elimination of the illogical cut sets and addition of correction factors can be easily performed using available PRA software.

B.2.4 Models Containing Surrogate Events

An alternate approach to avoiding generation of cut sets having multiple annual mission time events is to include a single event for a normally running component that can represent either a yearly or a mean time to repair mission time. Models that contain such a “surrogate” event for each component to represent either an annual or mean time to repair mission time must also be processed after generating the cut sets to achieve combinations of failures in which there exists a single event that has a mission time of a year with the remaining events having an exposure time related to the mean time to repair of the first failure.

Returning to the two 50% feedwater train example, the resultant cut set for total system failure can be expressed as pump A fails to run and pump B fails to run, where both pump events are surrogate events representing failure of the pumps without a particular mission time. If pump A fails first it must be given an annual mission time and pump B must have a mission time of the mean time to repair for pump A. Conversely, if pump B fails first, then pump B must be given an annual mission time and pump A must have a mission time equal to the mean time to repair pump B. To obtain the scenario where both combinations are present, the original cut set must be duplicated. Also, the adjustments to the mission time of the both events must be performed on both cut sets. The adjustment to common cause failure cut set values is the same as that for the models with operating failures having annual frequencies.

For systems containing two or more operating trains, the following modification to the resulting cut sets would apply.

- Duplicate the original cut set x times where x is one less than the number of surrogate events in the cut set.
- Convert one event to an annual mission time and all remaining events in the cut set to use a mission time of the mean time to repair of the event having the annual mission time.
- Multiply the common cause events by the mean time to repair /365.

C

CONFIGURATION/CHANGE CONTROL

Over time it is possible that the GRA models and analysis will begin to diverge from the “as-built/as-operated” configuration of the plant. Changes such as those arising from projects mentioned in Section 7.2.1 will contribute to this divergence. Operating experience and aging effects may also require updates to failure rates and unavailability frequencies, which obviously impact the prediction of lost generation. Modifications to the models may also occur over time to assist with the performance of specific applications. These are among the reasons for developing and maintaining a configuration/change control process for the GRA models and supporting information.

All nuclear plants will have some form of change control process in place for documents such as plant procedures, drawings, etc. Most, if not all, also have processes in place for their plant-specific PRA. The PRA process should be reviewed and used as the starting point for a GRA configuration/change control process. However, a few notable differences between the PRA and the GRA objectives may influence the GRA change control process.

- A PRA is predominantly focused on safety, whereas a GRA is focused on lost generation (or, ultimately when using LCM or RIAM methods, revenue and cost). Thus the frequency of updates applied to the GRA may be much lower than may be necessary for a PRA.
- PRAs undergo periodic “peer reviews” conducted by individuals from outside the utility organization as well as internal assessments directed at PRA quality. Preparing for and responding to the peer reviews and assessments can be a resource-intensive effort. Although analogous reviews may at some time be recommended as a mechanism for promoting information exchange as the use of GRA increases in the industry, such reviews are not predicted for the near future. Thus, some of the configuration/change control activities undertaken for a PRA in anticipation of peer reviews may be unnecessary for GRAs.
 - Because GRAs can be used in the evaluation of capital projects, some of which with substantial dollar figures attached to them, it seems prudent that an internal review of GRA results be conducted before decisions are made based on those results. However, a utility may decide that the detail or frequency of those reviews need not approach those of a PRA peer review if the cost of the project being evaluated is less than some threshold amount. In other words, the cost and effort associated with a detailed update and/or review of the GRA may not be cost-effective if the projects being evaluated have costs and impacts on lost generation below some pre-determined values.

Sources of information useful in designing and implementing a GRA configuration/change control process include:

- American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2002, April 5, 2002.
- Any of the nuclear power plant Owners Group (PWR/BWR) documents describing their Peer Review processes.
- Plant-specific document and process maintenance/update procedures.
- Nuclear Energy Institute (NEI) documents on PRA peer review and PRA maintenance and update processes such as NEI 00-02 “Probabilistic Risk Assessment (PRA) Peer Review Guideline”, Rev. A3, March 2000.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

About EPRI

EPRI creates science and technology solutions for the global energy and energy services industry. U.S. electric utilities established the Electric Power Research Institute in 1973 as a nonprofit research consortium for the benefit of utility members, their customers, and society. Now known simply as EPRI, the company provides a wide range of innovative products and services to more than 1000 energy-related organizations in 40 countries. EPRI's multidisciplinary team of scientists and engineers draws on a worldwide network of technical and business expertise to help solve today's toughest energy and environmental problems.


EPRI. Electrify the World

Program:

1008121

Nuclear Power

© 2004 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute and EPRI are registered service marks of the Electric Power Research Institute, Inc. EPRI. ELECTRIFY THE WORLD is a service mark of the Electric Power Research Institute, Inc.

 Printed on recycled paper in the United States of America