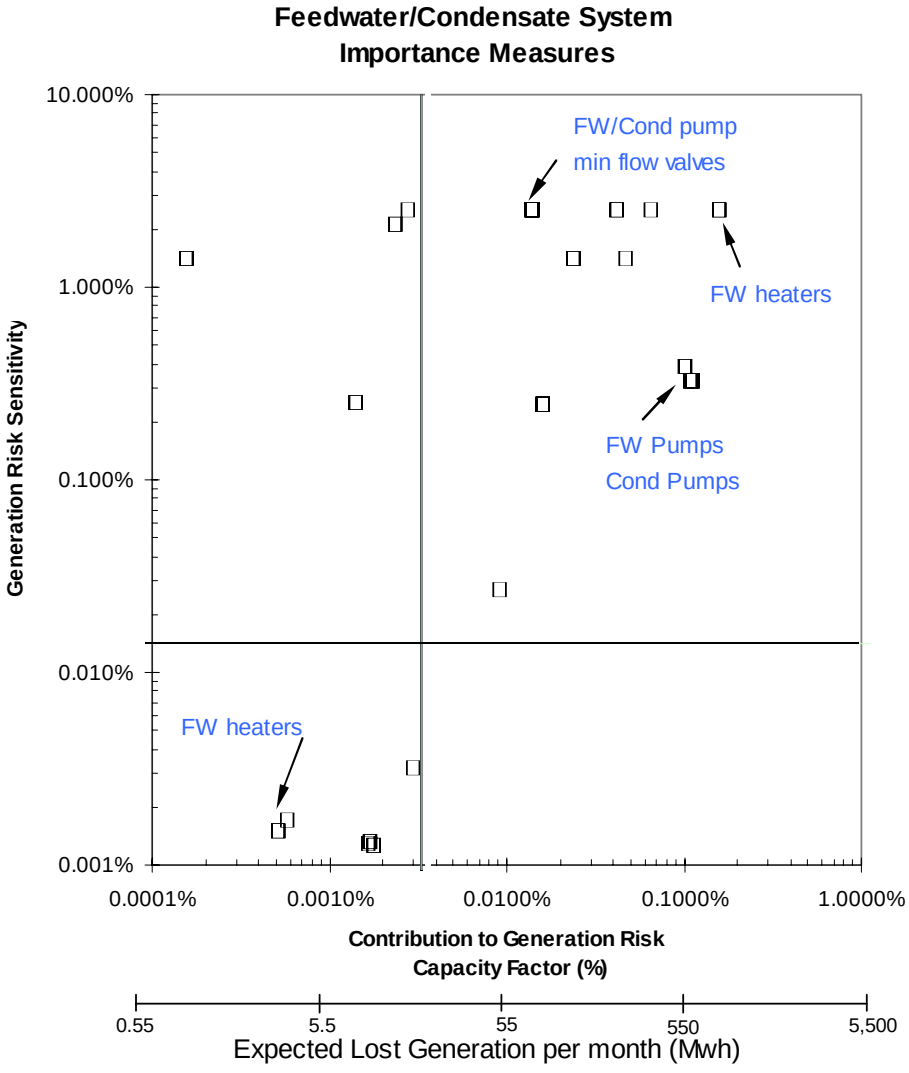
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Generation Risk Assessment (GRA) at Cooper Nuclear Station

Technical Report



Generation Risk Assessment (GRA) at Cooper Nuclear Station

1011924

Final Report, December 2005

EPRI Project Manager
G. Sliter

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1395 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

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).

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 the Electric Power Research Institute (EPRI).

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

Generation Risk Assessment (GRA) at Cooper Nuclear Station. EPRI, Palo Alto, CA: 2005. 1011924.

REPORT SUMMARY

A previous EPRI guide described how generating plants can implement various forms of component and system models for generation risk assessment (GRA). This report describes a trial application of GRA modeling at the Cooper Nuclear Station and evaluates the usefulness and accuracy of the EPRI GRA guide.

Background
Generation Risk Assessment (GRA) is the process of projecting power plant generation loss (MWh/year) due to system or component failures over a future operating term, often the entire remaining life of the plant. GRA uses a set of cost-effective risk methods, models, and software to aid plants in estimating future plant availability—a key driver of plant value, profitability, and decisions on preventive maintenance and capital improvement projects. EPRI Report 1008121, Generation Risk Assessment (GRA) Plant Implementation Guide (December 2004), was issued to assist utilities in the completion of GRAs. The Cooper Nuclear Station (CNS) participated in a trial application of that Guide.

Objectives
To use several of the approaches described in the GRA Guide to provide CNS with GRA system models for selected balance of plant systems, while comparing and contrasting the effort required and the results obtained from the various GRA modeling techniques.

Approach
In a project cosponsored by the Nebraska Public Power District, the researchers used their expertise in GRA, along with the information contained in the GRA Guide, to complete plant-specific GRA models at CNS. The GRA process involves identifying equipment functions related to production, constructing system logic models, applying component data on failure rates and repair times, and calculating lost generation due to combinations of component failures in the modeled systems.

Results
This report gives the results of GRA system evaluation for six systems at CNS and compares the results to plant and industry experience. The report also discusses the effectiveness of the guidance contained in the GRA Guide, including conclusions regarding the validity of the guide's estimates for the level of effort required to complete a GRA.

EPRI Perspective
EPRI's earlier work on Life Cycle and Nuclear Asset Management (EPRI report 1009623) showed that the estimated impacts of proposed replacements or preventive maintenance on future

lost generation are important drivers of decisions on investments in improved plant reliability, availability, and profitability. Together with the previous GRA reports (EPRI reports 1007386 and 1008121), the real-life application described in the current report is a significant step in providing the nuclear power industry with a tool that can rival Probabilistic Risk Assessment (PRA) in benefits to the industry. To be fully effective, GRA needs to be integrated into INPO's Equipment Reliability Process, AP-913.

Keywords

Generation risk assessment
GRA
Trip model
Equipment reliability criticality
Risk informed asset management

ACKNOWLEDGMENTS

EPRI and the authors acknowledge the support provided by the staff of the Cooper Nuclear Station, especially Kent Sutton and Ole Olson. We also gratefully acknowledge technical support from Neil Wilmshurst, EPRI.

In addition, the following co-funders are acknowledged for their contributions to the project:

2005 Generation Risk Assessment User Group

Electricité de France (EDF)	Herve Chardonnal
Iberdrola/Iberinco	Jose Gomez
Nebraska Public Power District	Kent Sutton
Omaha Public Power District	Joe Gasper

2005 Nuclear Asset Management User Group

Ameren	Michael Evans
British Energy	John Smart
Candu Owner Group	Vince Gonsalves
Detroit Energy	David Sullivan
Duke Energy	Mitch Baughman
Energy Northwest	Andy Rowe
Electricité de France	Serge Hugonnard-Bruyere, Francois-Noel Remy
Iberdrola/Iberinco	Jose Gomez
Nebraska Public Power District	Paul Gritton
South Texas Project NOC	Drew Richards
Tennessee Valley Authority	Michael Burzynski

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

Generation risk assessment (GRA) is an integral part of risk-informed asset management (RIAM) [1, 2]. The goal of a GRA, using traditional probabilistic risk assessment (PRA) methods, is to estimate production losses (megawatt-hours, Mwh) occurring as a result of equipment and system failure and unavailability. By combining plant generating system logic with information about equipment reliability and data on the magnitudes and durations of plant derates associated with equipment outages, the contribution of individual components as a function of their expected contribution to lost Mwh can be characterized. Plant management can use this information as input for making informed decisions about maintenance, spare parts inventory, design modifications, and other resource-constrained issues associated with the production of electricity. When entered into economic evaluation software such as LcmVALUE [3] or RIAM, the information leads to improved estimates of the value of proposed equipment reliability improvement projects.

The Nebraska Public Power District (NPPD) and its Cooper Nuclear Station (CNS) are increasing their use of risk-informed decision making tools and techniques such as GRA for making business decisions. CNS recently co-funded (along with EPRI's Nuclear Asset/Risk Management and Generation Risk Assessment User Groups) a pilot implementation of generation risk assessment at the station. The GRA was conducted using guidance contained in EPRI's GRA Plant Implementation Guide [4], henceforth referred to as the GRA Guide.

1.1 Background

As part of its long-term planning and business analysis processes, NPPD is actively using concepts inherent in risk-informed decision making methodologies. The Cooper Nuclear Station desired to participate in the GRA trial application to determine if GRA is a useful tool for achieving NPPD's objectives, including:

- Proactive management of risk, including the establishment of a quantitative risk framework for evaluating performance
- Integration of generation risk into the business planning process, anticipating issues in an integrated systematic manner and eliminating crisis management
- Elimination of vulnerabilities by seeking better information based on value while reducing uncertainty
- Hedging against losses by creating risk-informed strategies and contingency actions that can be applied throughout the enterprise

Another objective for implementing GRA at CNS was to develop a standardized process that allows various projects within NPPD's portfolio to be compared using like terms (e.g., reduction in Mwh-lost, maximum project cost (dollars) beyond which return on investment is not realized). This helps simplify complex budget issues and understand the bottom-line differences of competing projects.

Most importantly, the development and use of GRA models and results is intended to move the decision making process beyond dependence on expert judgment alone; the GRA can be used in conjunction with expert judgment, providing better information about the sensitivities that impact the decisions. For example, economic evaluations with GRA coupled with other risk-informed methods can provide the economic value attributes that are combined with non-economic value attributes in NPPD's use of EPRI's Enterprise Project Prioritization method and software [5].

The GRA at CNS was conducted in two phases. Phase 1, initiated in November 2004, included the modeling of five systems The goals of Phase 1 were to test the EPRI GRA Guide on an actual operating facility, to provide CNS staff with production-focused information about the modeled systems, and to allow CNS individuals to obtain proficiency on GRA techniques. Several modeling approaches were used to compare and contrast the effort required and the results obtained from the various techniques.

Phase 2, completed in 2005, developed models for one more system. In addition to the goal of obtaining information about lost Mwh associated with this system, application of the results to existing maintenance programs was undertaken.

As emphasized in the GRA guide, a GRA will need to "pay for itself" as it is developed. In other words, GRA modeling and evaluation efforts should be undertaken with specific applications in mind with the expectation of realizing cost-savings equal to or exceeding the cost of the evaluation. Initial model development would be centered around systems associated with these particular applications without a need to complete the GRA modeling of all systems and components important to productivity before it is used. Thus, the trial at CNS began with consideration of a few current plant generation-related issues. The selection of the initial systems was directed at addressing those issues in a quantitative manner before expanding the scope of the GRA.

1.2 Objective

The primary objective of this report is to provide EPRI member utilities with information concerning the usefulness of the methods described in the GRA Guide as a tool for assisting nuclear power plants with their development of plant-specific GRAs. Application at CNS, an operating power plant, of the steps contained in the guide provides feedback on the reasonableness and practicality of the guide's methodology, references, and resource estimates, providing lessons useful for validating or modifying the guidance.

1.3 Approach

To gain the broadest perspective on the usefulness of the GRA guide, three basic modeling techniques described in Section 3 of the guide were applied in the CNS trial:

- Supercomponent or "black box" modeling
- Detailed fault trees
- Conversion of PRA models/results.

The GRA at the Cooper Nuclear Station takes full advantage of previous work completed by the plant in the development of their plant-specific probabilistic risk assessment (PRA) in response to Generic Letter 88-20 [7].

A GRA evaluation produces for each modeled system 1) the frequency of system failure and 2) the estimated impact on production measured in megawatt-hours (or equivalent full power hours, EFPH) lost on an annual basis. Relative rankings of the contribution of individual trains or components to the frequency and production loss can be produced as well.

Six systems were evaluated for the CNS GRA:

- Main feedwater/condensate (MFW/CND)
- Generator
- Switchyard
- Service water (SWS)
- Instrument air (IAS)
- Turbine equipment cooling (TEC)

Of these, one was assessed using a fault tree logic model developed “from scratch,” one employed the supercomponent approach, and four converted existing PRA models into GRA models (see the GRA Guide for a description of these modeling approaches). CNS staff completed two of the system evaluations; EPRI’s contractors completed the remaining four. The results were compared to industry experience in the NERC-GADS database [8] to assess the ability of the GRA models to estimate system-related production losses.

1.4 Organization of this Report

This report is arranged in a manner consistent with the organization of the GRA Guide, an overview of which is presented in Figure 1-1. Section 2 discusses the definitions of generation risk, frequency, and consequences as applied at CNS. That section also contains top logic developed for the Cooper Nuclear Station. Section 3 discusses the selection and modeling of systems for the GRA trial application, including examples of modeling techniques in the CNS project. Section 4 provides information about data sources and the treatment of uncertainty. Section 5 follows with discussions of the techniques used to integrate and generate numerical

results for the GRA. Section 6 provides results, as well as a discussion of current and potential future applications of the GRA models and results at the Cooper Nuclear Station. Section 7 summarizes resources and schedule for the GRA.

Section 8 is a summary of the trial application. References follow Section 8.

Appendix A contains summaries of the individual system analyses and their results, while Appendix B contains failure rates developed specifically for the GRA analysis (see Section 4).

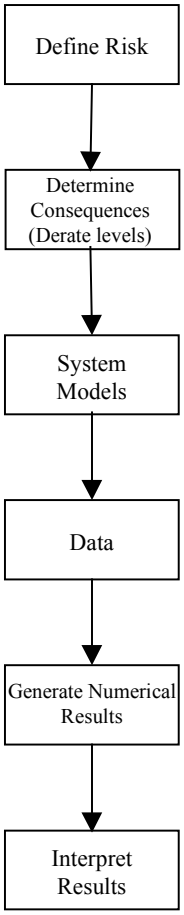


Figure 1-1
Major Steps of a GRA Implementation

2
RISK, FREQUENCY, CONSEQUENCES, AND TOP LOGIC – GENERAL OVERVIEW

Prior to system modeling, GRA must define what is meant by 'risk' from a generation perspective.

2.1 Definition of Risk for GRA

The CNS GRA adopted the risk definition in the GRA Guide:

> **Risk** is the product of the **frequency** of failure of systems, structures, and components (SSCs) and the **consequences** of those failures. For the CNS GRA, the focus is on systems and components – structures were not included in the evaluation.
>
> The **consequences** measured by the CNS GRA relate to generation or economic loss resulting from equipment failures. Changes in equipment performance that may lead to reduced plant efficiency or heat rate are not addressed by the GRA but are assumed to require thermal efficiency models such as PEPSE [6]. Public safety consequences and investment protection from severe accidents are considered to be treated by the plant-specific probabilistic risk assessments (PRAs).

Generation loss is associated with the power reduction caused by the failure of the system or component, and the amount of time the plant remains in the reduced power state. This is expressed by the formula:

Total Lost Generation (Megawatt-hours, Mwh) =
Frequency of load reduction x
Magnitude of load reduction x
Duration of load reduction

= Frequency of load reduction due to the failure of the system or combinations of trains or components leading to the load reduction x
(1 - fraction of full power after load reduction) x
Rated Capacity (Mw) x

(mean time to repair (MTTR) for the system, combinations of trains, or components + time to restore plant to power, in hours)

2.2 Contributors to Lost Generation (GRA)

For the Cooper GRA, classification of reductions in power was performed with a "top down" assessment of the contributors to plant derates. The functions important to power generation were first defined and then the systems key to providing these functions identified. Table 2-1 lists the generation-related functions important to CNS and identifies systems that support those functions. The table also gives the fraction of total lost generation that can be attributed historically to each plant system specifically for Cooper. This historical generation loss was derived for CNS from NERC-GADS reports [8] between 1987 and 2001. The upper level functions listed in Table 2-1 are defined as follows:

- **Primary Functions** are those that directly support the power conversion system. In other words, systems supporting these functions may be thought of as having a "front line system" 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).

- **Regulatory Functions** are functions that must, by regulation, be maintained for the plant to remain at power.

Table 2-1
Functions Important to Generation (CNS)

Type of Functions		System Designator	Description	Historical % Total Lost Generation
	Reactivity Control	RR	Reactor Recirculation	0.29
		RRFC	Reactor Recirculation Flow Control	0.49
		CRD	Control Rod Drive	0.20
		NBI	Nuclear Boiler Instrumentation	5.89
	Flow of Steam to Turbine			
		TGC	Turbine Electro-Hydraulic Controls	*
		MS	Main Steam	7.02
	Conversion of Steam Energy to Power			
		TG	Turbine generator	0.56
Primary Functions		TGI	Turbine generator supervisory instrumentation	0.24
	Condenser Operation			
		AR	Air removal	4.72
		OG	Offgas	
		AOG	Augmented Offgas	
		CW	Circulating Water	
		CD	Condensate drains	
		ES	Extraction Steam	
	Reactor Inventory Makeup			
		RF	Reactor Feedwater	2.70
		RFC	Reactor feed control	
		MC	Main Condensate	
		CM	Condensate makeup	
Supporting Functions	**Motive Power**			
		EE	Electrical Equipment	13.55
	Control Power	EE	Instrument AC	
		DC	DC Power	
		IA	Instrument Air	1.69
		SA	Service Air	
		TGF	Turbine Electro-Hydraulic Control fluid	
		DGSA	Diesel Generator Starting air	

Type of Functions		System Designator	Description	Historical % Total Lost Generation
		RRMG	Reactor recirculation motor generator set	
	Equipment Cooling			
		SW	Service Water	
		TEC	Turbine Equipment Cooling	
		REC	Reactor equipment cooling	
		DGJW	Diesel Generator jacket water	
	Lubrication			
		LOGT	Turbine lube oil (instrumentation)	
		LO	Turbine lube oil (mechanical)	
		RFLO	Reactor feed lube oil	
		RRLO	Reactor recirculation lube oil	
	HVAC			
		HV	Reactor Bldg Heating, ventilation, air conditioning	
Auxiliary Functions	**RCS Integrity**			
		Seals		
		SRV	Safety Relief Valves	
		RPV	Reactor Pressure Vessel	
		NB	Nuclear Boiler	
	Reactor Water Chemistry			
		RWCU	Reactor Water Cleanup	
		CF	Condensate demineralizers	
Regulatory Functions				
		RHR	Residual Heat Removal	2.89
		HPCI	High Pressure Injection	
		RCIC	Reactor Core Isolation Cooling	
		CS	Core Spray	
		DG	Diesel Generators	55.45
		DGFO	Diesel Generator fuel oil	
		PC	Primary Containment	4.31
		PCIS	Primary Containment Isolation System	

* Blanks indicate zero or insignificant contribution to lost generation.

3
SYSTEM MODELING AND ANALYSIS

This section of the report describes the approaches to modeling and analysis of the systems that were selected to be included in the CNS Generation Risk Assessment. The models, when combined with data (Section 4) and consequences (Sections 2 and 5), produce the GRA results in terms of generation loss.

3.1 Selection of Systems for GRA

As described in Reference 4, there are many factors that influence the choice of GRA systems. Because the GRA must provide payback as it is developed, there is no need to complete modeling of all generation related systems prior to its application. Therefore, systems should be chosen with a system or equipment performance or long-term planning issues in mind. The systems selected should have (or be perceived to have) important impacts on the generation capability of the plant, while also being candidates for plant operating or maintenance changes that can be assessed using the GRA results as input.

Examples of factors to consider are listed below.

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

Historic Contributors to Lost Generation

The historical performance of the plant is a major basis for selecting 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).

The systems selected at CNS were:

- Service Water System (SWS) – this system has pervasive impacts throughout the plant and on other systems required for generation. The system at CNS had also received increased regulatory oversight prior to initiation of the GRA pilot project, and therefore the plant staff was interested in any new operating knowledge that may arise from a study such as GRA.
- Main Feedwater/Condensate Systems (MFW/CND) – these systems have obvious direct impact on the ability of the plant to generate power. There were also a significant number of components associated with these systems on the "production critical" (PC1) list performed in the implementation of AP-913 (the Main Feedwater/Condensate systems were treated as a single system because of their close interactions).
- Generator – the main generator was chosen because there were some known issues affecting its efficiency; these were to be addressed in an outage completed during the course of the GRA trial. The purposes for including the generator in the GRA trial were: (1) to determine if any other issues might be uncovered by the modeling effort, that could then be addressed in future outages, and (2) to develop a model that could be used as a template at NPPD's fossil units; some of those units use generators similar in design to the generator at CNS.
- Switchyard – CNS is in the preliminary stages of developing strategies for improving the reliability of their switchyard transformer (known as the T2 transformer). Development of the GRA model for the switchyard could provide information useful in evaluating and selecting plant modifications related to the T2 transformer.
- Instrument Air System (IAS) – this system also has a pervasive impact upon the plant and other systems; performance issues associated with the compressors have resulted in the decision to replace them.
- Turbine Equipment Cooling (TEC) – important for supporting operation of the turbine, this system was selected because of the number of its components included on the CNS "production critical" (PC1) list of components.

This list of systems presented the GRA analysts with a spectrum of system and component types, and varying degrees of existing operating and failure data. This list provided variety to assess the applicability and practicality of the GRA approaches described in the GRA Guide (Reference 4).

3.2 Logic Model Development

As discussed in the GRA Guide, there are a number of approaches that can be used when developing a reliability model for plant systems. The approaches range from simple single point vulnerability modeling to more detailed fault tree logic model development. Two general modeling approaches in the guide were used in the CNS GRA:

(1) The "supercomponent" method, where systems and trains are treated as if they are a single ("super") component in the power plant, and

(2) The detailed fault tree approach, where individual system components and their potential failures are modeled.

The principal difference between these two methods is that the supercomponent approach requires less effort to develop than does a detailed model. However, the Implementation Guide states that the applicability of results generated by the supercomponent approach may be limited by the lack of detail. Thus, for the trial it was important to complete at least one system model using this approach to evaluate both the resource requirements as well as the potential for application of the results. The GRA Implementation Guide contains more detail on the supercomponent and detailed fault tree approaches.

When using the detailed fault tree approach, it may be necessary to construct GRA models "from scratch," i.e., begin the modeling without the benefit of any existing template or similar model to use as guidance. However, an additional method for using the detailed fault tree approach, suggested in the GRA Guide for producing GRA results, takes advantage of balance of plant logic models developed as part of the plant-specific PRA. In this approach existing PRA models are modified to support a GRA. In some cases it may be possible to make these modifications to the cut sets (the combinations of failure events that result in derate or plant shutdown), without need for significant changes to the models themselves. The cut set or model conversion approach modifies the PRA logic and results to shift their focus from the safety perspective under which they were constructed for the PRA, to the production focus necessary for a GRA. This approach has the benefit of including system logic details consistent with the PRA level of detail, without requiring the level of effort associated with building the fault trees from the ground up. Because several of the systems selected for the CNS GRA in fact had been modeled for the Cooper PRA, it was decided to test the PRA-to-GRA conversion approach using those systems.

Table 3-1 is a summary of the modeling approaches employed in the CNS GRA. Brief descriptions of the models follow.

Table 3-1
Modeling Approaches Used in the CNS GRA

System	Detailed Fault Tree	Supercomponent	Convert PRA Results
Service Water			✓
Instrument Air			✓
MFW/Condensate			✓
Generator		✓	
Switchyard	✓		
Turbine Equipment Cooling			✓

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.

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.

Generator System

For the Cooper Nuclear Station GRA it was decided that the generator should be treated using a supercomponent approach. This decision was based on the fact that the generator consists of, in general, a few large components or sub-components that could be easily characterized as "supercomponents." In addition, it was assumed that failure data to support a detailed modeling assessment would be sparse, whereas failure data at a higher (e.g., "supercomponent") level may be easier to find. Finally, there were some known performance issues with the generator at CNS, such as rotor shorts and other winding issues, and the supercomponent approach was chosen to determine if those issues could be adequately modeled and assessed using this approach. (Note that most or all of the known issues were addressed in a refueling outage completed during the development of the GRA; however, the model was developed for the pre-outage condition .)

It was decided to let data availability determine the level at which the supercomponents would be defined for the generator. In this particular case, data from the North American Electric Reliability Council (NERC) was used [8]. The NERC database uses "cause codes" to represent components or groupings of components within plant systems. In most cases the cause codes are defined at high levels within a system; therefore, the cause codes lend themselves well to being used as supercomponent designators. Hence, for the generator model the NERC cause codes associated with generator systems defined the generator model supercomponents. Examples include "Generator Rotor Windings" (NERC cause code 4500), "H2 Coolers" (NERC cause code 4611), "Generator Output Breakers" (NERC cause code 4810), etc. Figure 3-1 shows a portion of the generator fault tree logic model and the use of supercomponents (defined by NERC cause codes) to represent various failures of the generator or its auxiliaries.

It should be noted that although the generator and its immediate support systems are treated as supercomponents within the GRA modeling process, other supporting functions (e.g., service water cooling, ac power to MCC panels for pump operation) are treated in a detailed manner through the use of "transfers" or "links" to the fault trees existing in the GRA or PRA set of models for these functions. Thus, the generator fault tree is a hybrid of sorts, wherein the generator-specific portion of the tree is dealt with through the use of supercomponents, while ancillary (supporting) systems use detailed fault trees, simply because those fault trees already existed and required no development effort. If those logic models did not exist they could also have been constructed using a supercomponent approach. Figure 3-2 is an extract from the generator fault tree logic model showing linkage to other system fault trees.

Derate Levels

Based upon information gathered from plant sources it was determined that two levels of derate are associated with generator related components. The first is a plant shutdown (i.e., a 100% derate), which is to be expected given the function of the generator itself and the fact that there is no redundancy for many of the major components. The second level modeled is a 50% derate, occurring if the Phase Bus Duct Cooling System is unavailable.

Appendix A contains detailed descriptions of the models developed for each of the systems incorporated in the CNS GRA. Refer to Appendix A for more information concerning the identification of the derate levels.

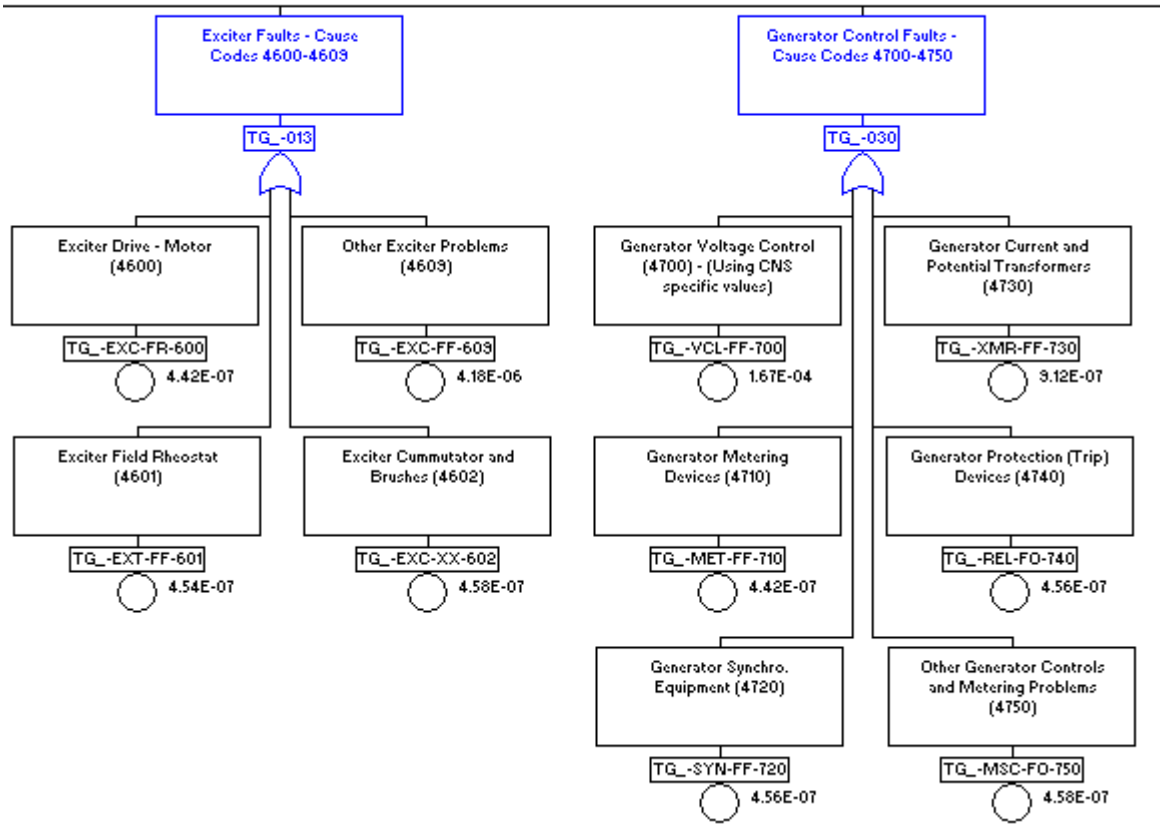


Figure 3-1
Example of Supercomponent Treatment for Generator System

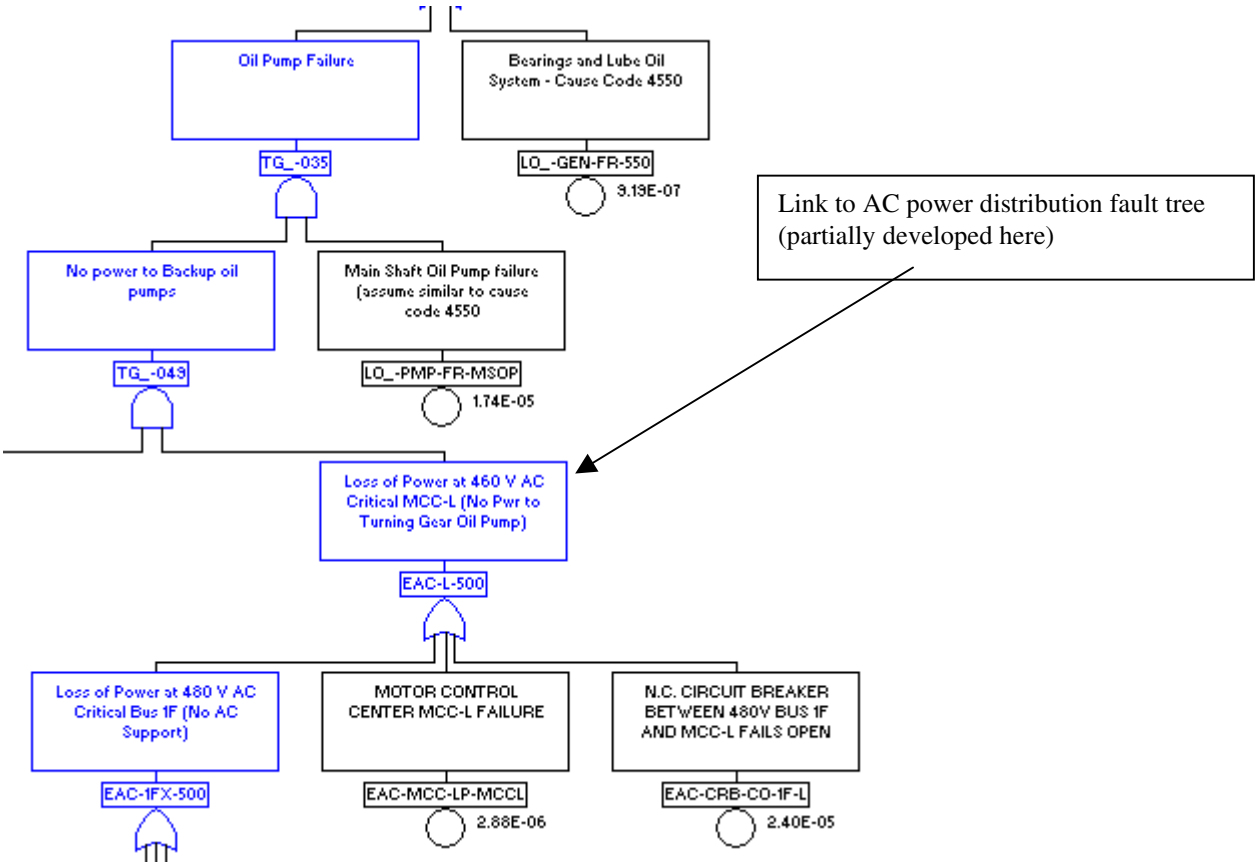


Figure 3-2
Link to Other Fault Trees

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) that include major components for all trains of the system. 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.

Switchyard

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 the switchyard system an existing, but recently developed (from scratch) model was converted for use in the GRA.

A switchyard fault tree was developed in 2004 to replace (enhance) the plant-centered loss of offsite power basic event employed in the PRA. The PRA model evaluates the likelihood of failing to provide AC power to the plant from either the switchyard or from the main generator, resulting in a plant trip. In addition, following a plant trip or shutdown (not caused by a loss of

offsite power), the model assesses the likelihood of subsequently losing AC power from the switchyard. The PRA model includes the five 345 kv transmission lines comprising a "ring bus" arrangement around the 345 kv switchyard. Power from 161 kv sources are also considered as adequate supply sources for the PRA, employing a "safety" perspective. Subsequent to its completion this fault tree was further enhanced through the completion of a grid stability study.

The switchyard model is a recent development intended for updating the Cooper PRA. The effort to produce this model was known and counted toward the GRA as being "from scratch." The level of effort required to construct the PRA-based model was added to the effort required to modify the model for GRA purposes to understand the total level of effort required to complete a GRA-based fault tree for the switchyard system.

In reviewing the existing PRA-based version of the switchyard model, it was determined that modification of the failure criteria was the factor requiring the most attention to convert from a PRA version to a GRA version.

In the PRA the failure criterion is a failure to supply power to the 4160V 1A and 1B buses from the Startup Station Service Transformer (SSST) AND the Normal Station Service Transformer (NSST), i.e., both must fail for there to be a "plant-centered loss of offsite power". If the NSST becomes unavailable, the plant will trip, but AC power should still be available to the SSST through the switchyard. For success, the SSST can receive power from any one of five 345 kv lines, or from the single 161 kv line.

For the GRA, instead of looking at failure to transmit power to the plant from the switchyard, the issue at hand is the failure to transmit power from the switchyard to the grid. In this case, a failure of the switchyard OR a failure of the NSST (from the main generator) will result in production loss. Failure of the NSST leads to a plant trip, and thus a loss of power production to the grid. Failures in the switchyard that prevent power flow to the grid result in a production loss even if the NSST is available.

Thus, the major change made to modify the PRA version of the fault tree to a GRA model for the switchyard was to convert an AND gate into an OR gate. Figure 3-3 shows the PRA model ("before") and the GRA model ("after") top gates.

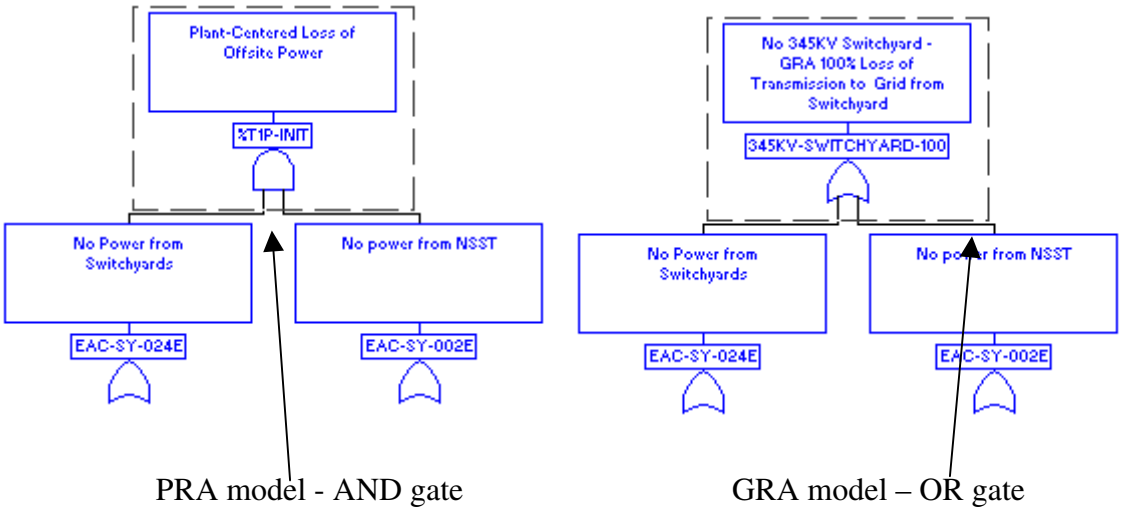


Figure 3-3
Conversion of Switchyard PRA Model to GRA Model

This change in fault tree logic structure results in the elimination of the SSST and the 161kv switchyard as elements of the model. The PRA model includes power coming from the SSST and the 161kv switchyard to the plant. The GRA model does not credit transmission through this path to the 161kv line as a valid 100% generation path – only 345kv transmission is included in the definition of success. Thus, the 161kv switchyard and the SSST events were deleted from the fault tree, with the exception of events dealing with isolation of line faults in the 161kv line – if not isolated successfully, those faults could potentially propagate to the 345kv switchyard and possibly fail that switchyard as well.

Other minor changes to the PRA fault tree were also made, but those changes had minimal impacts on the results, especially compared to the AND to OR gate conversion at the top of the fault tree. The resulting fault tree contains substantial detail in its treatment of the many pathways available for power flow from the main generator and through the 345 kv ring bus.

Derate Levels

For the GRA switchyard evaluation it was assumed that only a 100% derate (plant trip or shutdown) was required. Derates associated with the generator and its auxiliary systems are addressed by the generator model (see previous section); for the switchyard itself, failures tend to have "all or nothing" impacts on the ability to generate power to the grid. For the purposes of the GRA, success of the switchyard was defined as delivery of 100% demand to any of the five 345 kv transmission lines. Failures of the transmission lines do not impact the plant's ability to *produce* 100% power – although the ability to *transmit* 100% power may be impacted. Transmission losses are the subject of separate evaluations and are not treated by the current CNS GRA modeling (by definition, the GRA models address *generation*).

3.2.3 Conversion of PRA Results

The GRA Guide suggests that when balance of plant systems have been modeled in the PRA, it should be possible to start with the PRA-generated version of either the logic model or the cut sets themselves when producing GRA results for the systems. The model or cut sets must be reviewed to remove any events or combinations of failures that are not applicable when considering production instead of post-initiating event safety. For example, failures of emergency AC power sources are not applicable in a GRA because such sources are only employed following a plant trip. On the other hand, it may also be necessary to include certain events that are not considered in a PRA precisely because those events are considered to be unavailable following a plant trip or shutdown but they would be available during normal operations.

Instrument Air, Main Feedwater/Condensate, Service Water, Turbine Building Equipment Cooling

Each of these systems was modeled in the Cooper Nuclear Station PRA because of its function of supporting post-initiating event accident mitigating systems, or its ability to be a mitigating system itself (e.g., main feedwater/condensate). As a result, detailed fault tree models and comprehensive cut set lists exist for each system. These systems were prime candidates for assessing the viability of the PRA-to-GRA conversion approach included in the GRA Implementation Guide.

To use a PRA-based model for GRA purposes requires changes to shift from a safety perspective to a production perspective. For example, the following factors must be considered:

- Failure criteria: Convert top logic to reflect the failure criteria defined for GRA (e.g., where only a single train or flow path is necessary for accident mitigation, multiple trains or flow paths 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.
- Common cause: Most PRA models include common cause events. The level of detail depends on the common cause method used, i.e., in some approaches common cause failures of multiple components are treated by use of a single event, regardless of the number of components being addressed. In other approaches each combination of component failures is explicitly modeled. When the PRA is used as a basis for GRA model development, the existing PRA common cause modeling should be sufficient. However, when it is found that additional common cause events need to be incorporated into GRA models, a simple factor approach should suffice (that is, a single common cause event representing the failure of all

redundant components within a system is all the detail needed to capture the majority of the effects of common cause).

- 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 (such as 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 (such as reduction in reactor recirculation flow in a BWR to prevent a reactor trip on loss of a train of feedwater).

The process of conversion of the four selected systems began by reviewing the success criteria of the systems to ensure they were appropriate for a production focus. The impact of partial failures of various parts of the systems was then determined in terms of resulting power derates. These two steps established if the existing logic required modification at the top level, and if additional logic was necessary to address different levels of derate.

The next general step was to review the cut sets produced from the original models for the PRA. This review often provided clues as to the need to make additional changes to the model to either (a) remove events not relevant in a power production mode, or (b) add events not considered in a post-accident (safety) mode.

Selected examples of logic changes made due to such reviews are provided below (see Appendix A for a more detailed discussion of each modeled system):

Service Water

1. New fault tree top logic was generated to model three different pump success/failure criteria for the Summer, Summer hottest period and Winter months (more service water pumps are required to maintain the plant at power than are required for accident mitigation purposes, particularly during summer months).

2. Common cause events were replaced in the fault tree to represent the failure of the appropriate number of service water pumps given the seasonal variation in success criteria.

3. The model includes the addition of human actions to reopen the non-critical SW headers following loss of a pump; loss of a pump results in low pressure conditions in the service water system causing the non-critical SW headers to isolate.

4. Removal of non-generation related logic such as SW flow paths to the emergency diesel generators (EDGs).

5. The strainers located on the discharge of the service water pumps were included, along with the bypass path around the strainers. This modeling addition was included as a result of plant experience with low intake water level and subsequent ingress of higher levels of debris than in previous years of operation. The possibility of plugging the strainers as a result of the amount and size of the debris, and failing to bypass the strainers to complete clearing operations, are addressed with the added events.

Derate Levels

A plant shutdown or trip is assumed should there be insufficient heat removal provided to balance of plant systems by service water. While there is only one derate level modeled (100% shutdown), it was noted above that there are three different success criteria associated with avoiding such a shutdown depending on the season (winter, summer and the hottest part of the summer).

Main feedwater/condensate

1. Added two feedwater heater trains and a third bypass line. These are passive failures (leakage, plugging) that were not originally included in the PRA model for feedwater.
2. Added two Augmented Offgas (AOG) condensers and AOG condenser booster pumps. These trains actually support the condenser vacuum function, but were included in the feedwater logic.
3. Added condensate booster auxiliary oil pumps and power dependencies. This logic was assumed to be modeled implicitly in the PRA model for the condensate system.
4. FW control dependencies - Added logic “OR-ing” reactor feed pump (RFP) trains with feedwater level control and RFP discharge valve isolation. Deleted startup valve logic (too small to support power operation).

Derate Levels

Five different top events were developed representing the various load reductions that would occur should a given combination of trains from the feedwater condensate system be removed from service or fail. Engineering judgment was used in selecting each derate level based on plant information regarding the capacity of each of the trains of equipment included in the model. The selected derate levels and failure criteria were as follows:

Failure Condition (derate)	Failure Criteria (Equipment Failures)*
Failure to maintain power >0%	• Loss of 2 of 2 FW trains (50% each) • Loss of 3 of 3 Condensate trains (33% each) • Loss of 3 of 3 Condensate booster trains (33% each) • Loss of 3 of 3 heater trains and bypass (50% each) • Loss of Either feedwater heater (A-5 or B-5) from the turbine moisture separator • Loss of 1 of 1 gland seal condenser (100%) • Loss of 2 of 2 air ejectors (100% each) • Loss of 2 of 2 Augmented Offgas Condenser trains (100% each) • Loss of Condensate demineralizers and demineralizer bypass (100% each) • Flow diversion Any condensate pump, condensate booster pump or FW pump minimum flow valve spuriously opening and causing pressure drop to suction of pump Failure of FW pump discharge check valve with the affected FW pump tripped
Failure to maintain power >33%	• Loss of 2 of 3 condensate trains • Loss of 2 of 3 condensate booster trains
Failure to maintain power >50%	• Loss of 1 of 2 FW trains • Loss of 2 of 3 FW heater paths
Failure to maintain power >67%	• Failure of 1 of 3 condensate trains • Failure of 1 of 3 condensate booster trains
Failure to maintain power >10%	• Loss of any 1 of 8 feedwater heaters (loss of a feedwater heater is assumed to result in a minor derate <10% rated power)

* Any single bulleted criterion will produce its associated failure condition.

Turbine Equipment Cooling

Fault tree logic gates were added to reflect summer and winter operations. Specifically, summer operations consist of conditions where loss of any one of four pumps or one of two heat exchangers could result in a plant trip. Winter operations consist of conditions where at least three of four pumps or two of two heat exchangers must be lost before tripping the plant.

Derate Levels

A 100% derate situation was modeled in the CNS GRA. Plant derates less than 100% are not considered in this assessment. This is based on the fact that power reductions are not effective in mitigation of the consequences caused by the loss of the turbine equipment cooling function. Thus partial derates do not prevent plant trips.

Instrument Air

No changes to the PRA logic model were required to convert from the PRA to GRA evaluation.

Derate Levels

Loss of instrument air directly results in inability to control reactor feed water flow rates which correspondingly results in a plant trip. Thus, a 100% derate condition was modeled for the Instrument Air System. Power reductions are not effective in mitigation of the consequences caused by the loss of the instrument air function. Thus, partial derates do not prevent plant trips. Hence, derates of less than 100% were not modeled for the 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 availability data to the basic events included in the model. This section discusses the inputs and data sources employed for the CNS GRA. Characterization of data uncertainty is also discussed here.

4.1 Data Sources for the CNS GRA

In general, a GRA model needs data for the following types of information to estimate 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 (to quantify routine and off-normal operator and maintenance personnel actions associated with system performance)
- Magnitude of derate (load reduction)

Sources employed in the CNS GRA for each of these categories of data needs are discussed below.

4.1.1 Random Failure Events

To ensure that the estimates of lost generation produced by the GRA models accurately reflect actual or expected plant conditions a GRA analyst should use the best sources of event data available. As discussed in the GRA Guide, the selection of data employed is a function of the application being addressed by the GRA models and the availability of resources to gather and analyze the data.

The GRA at CNS used two major sources of data for failure rates:

- Data in the CNS PRA database

- Data from the NERC database [8].

Many other sources of data are available (see the GRA Guide), but were not employed since the above sources were adequate and convenient sources for the trial effort. (Note that during the completion of the Cooper GRA EPRI was developing a database tool (LAMDA [9]) that should be considered as a primary source of information for future GRA efforts.)

Since most of the CNS GRA models wound up being based on existing PRA fault tree models, it was simplest to use the PRA database whenever it contained data corresponding to the basic events included in the model. Also, priority was given to use of data from the PRA to minimize the effort required for the data assignment step. Although primarily comprised of failure rates derived from generic sources, the PRA database contains some events based on plant-specific operational data. Consistent with guidance in the GRA Guide (and as is discussed in Section 5 of this report), the results of the initial model quantification were reviewed and compared to plant and industry-wide experience. Component failure rates that were out of line with plant-specific experience were targeted for additional investigation and possible use of data from alternate sources (e.g., the NERC database). This approach, which is a common practice in PRAs, allowed the analysis to proceed without expending extensive resources on data gathering and analysis, while also ensuring that additional effort was focused on those events identified in the initial quantification as using data inconsistent with site-specific experience.

When additional data or an alternative data source was sought (e.g., when the review of the initial quantification of system models revealed system failure frequencies not consistent with known plant-specific behavior), the first source was Cooper-specific experience. When available, this data was gathered from Cooper-specific entries in the NERC database. Although ideally analysts would always prefer to use plant-specific data for every event in a GRA, this is impractical for a variety of reasons (not the least of which is the large amount of resources that would be required to gather and analyze the data). If no Cooper-specific event information was found in the NERC database other sources of information were investigated (e.g., WASH-1400 or IEEE-500 [9, 10]).

4.1.2 Common Cause Failure Rates

Common cause failures 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.)

Common cause failure rates are developed using a variety of methods. One of the most common is known as the multiple Greek letter (MGL) method. In this method, Greek letters (beta, gamma, delta, etc.) are used to represent the conditional failure rate of multiple components given failures of other components within the grouping of like components.

Although the level of redundancy in balance of plant (production oriented) systems at a nuclear plant is typically lower than in safety systems, there are systems that indeed do have multiple trains or components that, if failed, lead to system failure and possibly plant shutdown (or larger magnitude derates than associated with single component or train failures). Thus, common cause analysis is necessary for those systems.

As for random failure rates, common cause failure (CCF) rates used in the GRA models were taken from the existing PRA database whenever possible. When CCF rates did not exist in the PRA database such rates were approximated with screening values consistent with generic (typical) PRA industry rates. In such cases, a "beta factor" of 0.1 was used to represent the conditional failure probability of a second like component given failure of the first, and a "gamma factor" of 0.5 was used to represent the conditional failure probability of a third like component given failure of the first and second components. In the rare instances in which common cause failures of four or more like components were modeled, a conditional failure rate of 1.0 was used to represent failures of the fourth (and beyond) like component(s) given failure of the first three.

It is also possible with some effort to estimate CCF rates using NERC data. While not needed for the CNS GRA because of the availability of CCF rates from other sources, the techniques for CCF rate estimation are discussed further in Section 4.2 in the event that other GRAs may wish to utilize the NERC-based approach.

4.1.3 Test and Maintenance Unavailability

Test and maintenance (T&M) for generation systems and components may occur just as they can for standby systems. The Cooper PRA database reflects T&M mean unavailability times for those systems and components modeled in the PRA, and therefore this information was used unchanged in the GRA. If T&M (unavailability) data was necessary for components/systems not included in the PRA database it was developed directly from plant procedures and experience (i.e., from discussions with the responsible system engineers and cognizant maintenance staff).

4.1.4 Repair Time

The mean time to repair (MTTR) for generation-related components can affect both the frequency of trips and derates as well as the consequences in terms of total lost generation.

- In systems with redundant trains or components, the MTTR determines how long, on average, redundant trains must operate following a failure of the first train in order to avoid a derate associated with loss of all trains.

- In those cases in which a derate has occurred, the MTTR is a factor determining how long the plant remains in the derated condition before beginning power ascension.

Repair times were not available from the CNS PRA. Thus, it was necessary to derive and assign MTTR values for all components included in the GRA.

As a starting point it was decided to use a very simple repair and recovery model similar to that found in WASH-1400 [10]. From that reference, the following MTTR values are applied to broad categories of equipment:

- Major mechanical equipment (e.g., pumps) - 19 hours
- Electrical equipment (e.g., electrical distribution) and non-major mechanical components (e.g., motor operated and air operated valves) - 7 hours
- Instrumentation and control - 6 hours

The NERC-GADS database was also used to develop MTTR values for a number of components, in particular those for which the failure rates were also derived from NERC data. Section 4.2 discusses the development of data from NERC information.

Where MTTR data was not assigned, an arbitrary value of 168 hours (one week) was used. Except for a few of the most critical components (which were all assigned specific MTTR values), this value was considered sufficiently bounding on the high side that if the component were determined to be important to generation as revealed by a review of the model quantification results, it would highlight the need to derive a component-specific MTTR value. Use of bounding values such as employed for MTTR is also consistent with guidance suggested by the GRA Guide.

4.1.5 Recovery Time

In addition to component-specific MTTR values, it is also necessary to determine if there are other factors that could influence how long the plant may be down for repair. Historically at CNS, the plant has used outage time following an unanticipated shutdown to address backlogged maintenance and other items. Data suggests that a three-day period is representative of such outages. Therefore, GRA return-to-power modeling for full plant shutdowns was developed to reflect a minimum of three days plus heat-up time to return to 100% power. (The trend at the plant indicates shorter-duration outages, and therefore this assumption will be reviewed and modified as appropriate in future GRA applications at the plant.)

The impact of the three-day outage assumption is that it dominates when component MTTR values are much less than 72 hours, and production losses are not influenced by improvements in repair (due for example to spare parts staging or improved maintenance training). If the MTTR is greater than 72 hours for a component, then the MTTR value becomes the dominant factor in determining how long the plant is shut down. Monitoring plant-specific trends in the actual

duration of outages will therefore be a necessary data collection activity for maintenance of the GRA models.

Once a component is repaired and the system declared operable there is still a time lag before the plant is returns to 100% power. This power ascension or heat-up time is a function of plant procedures, operating practice, and plant design.

For plant heat-up information, the GRA relied on plant-specific experience for typical return-to-power times (see Figure 4-1) . Based on information for a typical startup from cold shutdown, criticality, heat-up and synchronization to the grid take approximately 34 hours. Assuming a thermal power near 25% rated at the time of synchronization, gradual power ascension to 100% occurs over the next 40 hours for an approximate rate of 1.65%/hour. This power ascension rate is also used for all derates less than a full plant shutdown.

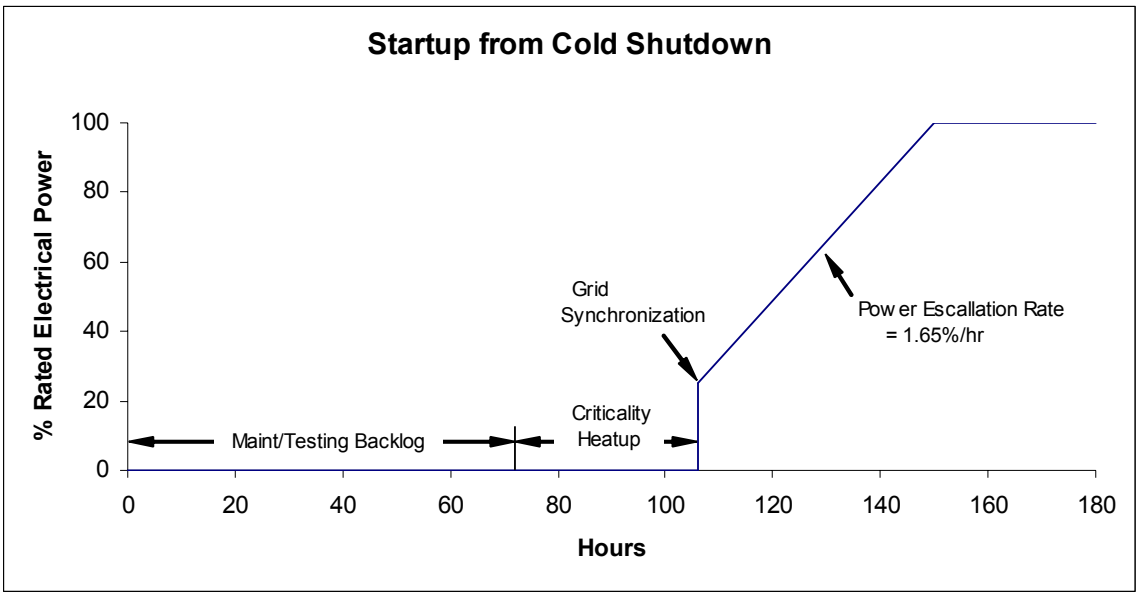


Figure 4-1
Typical Power Ascension Timing for CNS

4.1.6 Human Reliability

PRA values were used for human error probabilities (HEPs) where available. For example, the PRA includes an event in the Service Water System for the operator failing to open non-critical SWS valves to reestablish SWS flow to the Turbine Equipment Cooling (TEC) heat exchanger after a SWS pump fails. This action is assigned a value of 1E-2/demand in the PRA; that value is maintained in the GRA since the conditions under which the action would be accomplished are not significantly different during at-power conditions.

In only a few cases were any HEPs required that were not already in the PRA database. In those cases values were assigned to represent the HEP based on engineering judgment. For example,

in the switchyard fault tree there are events representing inadvertent isolation of transmission lines by the Doniphan Control Center dispatchers – unlikely but theoretically possible occurrences. These events were assigned values of 1E-3/demand. Because of the redundancy inherent in the switchyard design, changing these values to 1E-2 or even 1E-1 per demand has no impact on the overall results for the switchyard model.

4.1.7 Magnitude of Derate

Derate levels for the selected systems were discussed in Section 3. Data sources used to determine the levels to be modeled for the selected systems included:

- System design documentation (in terms of capacity of individual trains)
- Lesson plans (developed for operator and engineer training)
- Plant power history data/records
- System descriptions
- System engineers and operators with their knowledge of system and plant operations
- Technical specifications (e.g., for limiting conditions of operation that may require a plant shutdown)

4.2 Use of NERC Data

During the course of the model development or model conversion from a PRA perspective to a GRA, component events were added for which failure rates did not exist in the PRA database. In those cases the NERC database was the first source of information reviewed.[1]

Among other things, the NERC database summarizes industry events that have resulted in forced outages and forced derates. The average number of downpower hours per event is also reported. The information is reported as a function of cause codes, which are grouped by system for power plants of different fuel types (e.g., nuclear, fossil). Therefore, the database has significant data that could be used to provide estimates of component or system failure frequency and MTTR.

Estimating Failure Frequency

To derive a failure frequency for a component requires the following steps (note that this approach is used only for estimating failure rates per unit time; NERC does not capture sufficient information to estimate demand failure events (e.g., it does not include information about the total number of success events prior to the reported failure)). The following steps yield two NERC output reports; an Annual Unit Performance report from which the total number of

[1] As mentioned in Section 4.1.1, during the CNS GRA project, EPRI was developing and testing the LAMDA database [9]. This database was not sufficiently complete for use in the CNS GRA, but should be considered as a primary source of information for GRAs implemented from this point forward.

operating hours is presented for the plants meeting the selection criteria, and an Individual Cause Code report from which total number of failures and total outage time can be derived.

1) Specify search criteria

    a. Unit type, reactor type, years for which data is to be used, etc., can all be specified within the NERC software. For example, for CNS, the criteria included "Unit type = nuclear, Reactor Type = BWR, Years = 1982-2003."

2) Determine NERC cause code(s) that represent the component in question

    a. A list of cause codes can be found with the NERC documentation. For example, cause code 3600 is "Switchyard Transformers and Associated Cooling Systems", cause code 3850 is "Instrument Air Compressors," etc.

3) Run Individual Cause Code report for selected cause codes

4) Count the number of events for the forced outage and/or forced derate categories of interest

    a. Usually this will include forced outage categories U1, U2, U3 and forced derate categories D1, D2, and D3 (see example below for definitions of these outage and derate categories).

    b. The result provides the numerator in the equation "rate = failures/hour"

5) To estimate total number of service hours for the population of plants associated with the search criteria selected, use that same search criteria and run the Annual Unit Performance report

6) From that report, take the mean value of "Unit Service Hours", and multiply by "Unit Years" (also found in this report), to get the total number of service hours for all plants included within the search within which the number of failures of Step 4 occurred

    a. This provides the denominator in the equation "rate = failures/hour"

7) Divide the result of Step 4 by the result of Step 6 to produce the estimated failure rate, with units of events/hour

An example is provided below for "Switchyard Transformers" (cause code 3600 in NERC):

From the Individual Cause Codes report, for all US commercial nuclear power plants except CNS (CNS-specific events are included as part of the Bayesian update process discussed later in this section) –

Individual Cause Code Report for Years 1982 - 2002, Periods 01 – 12
Unit-years:1924.5

Cause Code	Event Type	Occurrences	Total Equiv. Hrs.	Total MWH Loss	Occurrences per Unit Year	Hours Lost per Unit Year	Hrs Lost per Occurrence	MWH Lost per Unit Year	MWH Loss per Occurrence
3600	D1	25	101.6	111,793.82	0.013	0.0528	4.064	58.0898	4,471.75
3600	D2	1	0.07	79.03	0.0005	0	0.07	0.0411	79.03
3600	D3	1	0.59	489.11	0.0005	0.0003	0.59	0.2541	489.11
3600	U1	11	447.21	442,638.61	0.0057	0.2324	40.6555	230.0019	40,239.87

The event types are defined by NERC as follows:

D1 - Unplanned (Forced) Derating — Immediate. A derating that requires an immediate reduction in capacity.

D2 - Unplanned (Forced) Derating — Delayed. A derating that does not require an immediate reduction in capacity but requires a reduction within six hours.

D3 - Unplanned (Forced) Derating — Postponed. A derating that can be postponed beyond six hours but requires a reduction in capacity before the end of the next weekend.

D4 - Maintenance Derating - A derating that can be deferred beyond the end of the next weekend but requires a reduction in capacity before the next Planned Outage (PO). A D4 can have a flexible start date and may or may not have a predetermined duration.

U1 - Unplanned (Forced) Outage — Immediate. An outage that requires immediate removal of a unit from service, another Outage State, or a Reserve Shutdown state. This type of outage usually results from immediate mechanical/electrical/hydraulic control systems trips and operator-initiated trips in response to unit alarms.

U2 - Unplanned (Forced) Outage — Delayed. An outage that does not require immediate removal of a unit from the in-service state but requires removal within six hours. This type of outage can only occur while the unit is in service.

U3 - Unplanned (Forced) Outage — Postponed. An outage that can be postponed beyond six hours but requires that a unit be removed from the in-service state before the end of the next weekend. This type of outage can only occur while the unit is in service.

In this example it is assumed that all transformer events resulting in either a forced derate (Event Types D1, D2, D3 in the example) or forced outage (Event Type U1, in the example above) are applicable failures for estimating a transformer failure rate. Thus, 38 events (25+1+1+11) are in the time period used to generate the report.

Using the same search parameters, the Annual Unit Performance report is generated:

Annual Unit Performance Report for Years 1982 - 2002, Periods 01 – 12						
Unit-years:1924.5						
Variable	Mean	Median	Minimum	Maximum	Range	Std Deviation
Gross Maximum Capacity	950	950	51	1,341.00	1,290.00	270.1
Net Maximum Capacity	907	902	48	1,261.00	1,213.00	258.3
Gross Dependable Capacity	946	941	50	1,334.00	1,284.00	269.67
Net Dependable Capacity	902	900	47	1,255.00	1,208.00	258.41
Gross Actual Generation	5944857	5879770	0	9,673,332.00	9,673,332.00	2,204,868.84
Net Actual Generation	5654964	5578398	0	9,294,617.00	9,294,617.00	2,096,766.02
Period Hours	8,764.76	8,765.71	8,707.08	8,768.27	61.19	7.76
Unit Service Hours	6,599.08	6,982.83	0	8,195.00	8,195.00	1,315.58
Pumping Hours	0	0	0	0	0	0
Condensing Hours	0	0	0	0	0	0
Reserve Shutdown Hours	2.71	0	0	205.75	205.75	20.02
# of RSH Occurrences	0.04	0	0	0.57	0.57	0.1
Total Available Hours	6,601.79	6,982.83	0	8,195.00	8,195.00	1,315.31
Forced Outage Hours	793.05	437.1	0	8,755.20	8,755.20	1,236.88
# of FOH Occurrences	3.61	3.29	0	9.33	9.33	1.58
Planned Outage Hours & Ext.	1,230.06	1,133.89	0	3,711.97	3,711.97	494.82
# of POH Occurrences	1.35	1.33	0	2.75	2.75	0.53
Maintenance Outage Hours & Ext	133.91	64.31	0	811.78	811.78	164.8
# of MOH Occurrences	0.55	0.45	0	4	4	0.49
Total Unavailable Hours	2,162.94	1,783.36	565	8,754.40	8,189.40	1,315.58
# of FD Occurrences	31.49	13.75	0	255.72	255.72	43.49
Equiv. Scheduled Derated Hrs	105.34	87.44	0	686.54	686.54	89.85
Actual Units Starts	4.11	3.96	0	9.93	9.93	1.33
Attempted Unit Starts	4.29	4.1	0	16.67	16.67	1.71
Years in Service	14.35	14.75	3.04	33	29.96	5.93

The mean value of Unit Service Hours is 6,559 hours, for 1925 unit-years. Thus, a good estimate for the total number of service years in this population of plants and years is (6559 x 1925), for a total of 1.3E7 hours.

The failure rate for switchyard transformers, cause code 3600, is then calculated as:

Number of failures/total service hours
= 38/1.3 E+07
= 2.9 E-06/hour

This methodology was used for many components in the Cooper switchyard model, and all "supercomponents" in the generator model.

Estimating MTTR

To estimate MTTRs for specific component types, the same report, namely, the Individual Cause Code report (such as shown in the previous example) can be used. However, different columns of information in that report are now utilized. For this calculation it is assumed that the column "Hours Lost per Occurrence" is a good approximation of the MTTR.

If multiple Event Types have been combined, then calculate the MTTR by using a weighted average, based on the number of event occurrences. E.g., for switchyard transformers, cause code 3600:

i. U1 = 11 events, Hrs Lost per occurrence = 41 hours
ii. D1 for same cause code = 25 events, Hrs Lost = 4.1 hours
iii. D2 for same cause code = 1 events, Hrs Lost = 0.07 hours
iv. D3 for same cause code = 1 event, Hrs Lost = 0.6 hours

Weighted Average (MTTR) =
(11*41 + 25*4.1 + 1*0.07 + 1*0.6) / 38
= 14.5 hours.

Common Cause Failure Rates

While not needed in any of the GRA models generated to date for Cooper, a process for generating common cause beta (β) factors from NERC data was developed. The process requires generation of component cause code reports for each year over which common cause failure rates are of interest. Table 4-1 is a sample of the common cause code report for several feedwater-related cause codes.

Table 4-1
Sample Common Cause Code Report for Feedwater-Related Cause Codes

Component Cause Code Report
for Years 2000-2000, Periods 01-12
Unit-years:22

Cause Code	Description	Unit Years	Total Occurrences	Forced Outages - Outage per UnitYear	Forced Outages - MWH per UnitYear	Forced Outages - MWH per Outage	Forced Deratings - Occurrence per UnitYear	Forced Deratings -MWH per UnitYear	Forced Deratings - MWH per Occurrence	Forced & Scheduled Outages & Derates Occurrences per UnitYear	F & S O & D MWH per UnitYear	F & S O & D MWH per Occurrence
3410	Feedwater Pump	22	4	0	0	0	0.045	2,051.74	45,138.20	0.182	2,524.00	13,882.00
3412	Feedwater Pump Drive - Steam Turbine	22	10	0.045	396.74	8,728.2	0.273	522.53	1,915.95	0.455	1,348.96	2,967.71
3414	Feedwater Pump Local Controls	22	3	0	0	0	0.091	1,273.21	14,005.36	0.136	1,698.99	12,459.26
3416	Other Feedwater Pump Problems	22	3	0	0	0	0.136	4,188.43	30,715.18	0.136	4,188.43	30,715.18

It can be seen that information is provided with respect to both partial load reductions (Forced Deratings - Occurrence per Unit Year) and all plant shutdowns plus derates (Forced Scheduled Outages & Derates - Occurrences per Unit Year). If it is assumed that derates do not necessarily involve multiple failures, then the difference between these two columns provides an indication of the number of plant shutdowns caused by multiple simultaneous failures (potential common cause events).

Using the feedwater pump cause codes as an example:

Forced derates = (0 + 0.04 + 0 +0) /Unit year* 22 Unit years
= 1 event

Forced & Scheduled Shutdowns and Derates =
(0.18 + 0.46 + 0.14 + 0.14)/ Unit year * 22 Unit years
= 20 events

Common cause factor (events resulting from multiple failures) = 1 /20
= 0.05

The above approach can be applied to each year over which relevant industry data is available to approximate common cause factors for use in the GRA.

Bayesian Update using NERC Data

If the analyst believes that industry data is representative of plant-specific performance, but the population of data for the plant may not be sufficient to establish a statistically significant failure rate, then Bayesian updating may be appropriate (the GRA Guide provides a list of selected references for more discussion of Bayesian updating). This step is important where plant-specific experience considered by itself would clearly lead to optimistic failure probabilities (e.g., the plant has not yet experienced any failure of a particular component type) or an unusual number of failures has been experienced, but corrective action should have returned the component failure rate to near industry averages (e.g., the plant has encountered a run of bad luck for a given component type).

NERC data can be used to develop an industry prior for input to a Bayesian update. Although it is a relatively straightforward process it requires some effort.

A Bayesian update requires that a prior distribution be developed from generic data. In NERC there is currently no function that provides such a distribution around component cause codes. However, a distribution by calendar year can be created.

1) Revise search criteria to remove the plant being evaluated from the population of plants providing the raw data. In other words, create the reports using all plants except Cooper (in this specific case). In the steps that follow this is called the industry report.

2) Separately, create a search using only the Cooper plant for the population set.

2) Separately, create a search using only the Cooper plant for the population set.

3) Generate separate industry Individual Cause Code reports for the cause code(s) of interest, for each calendar year to be included in the distribution. For example, if the period of interest spans 1990 through 2000, then create a report for the year 1990, a separate report for the year 1991, and so forth, up to and including the year 2000.

4) Generate an Individual Cause Code report for Cooper only. A single report covering all years (e.g., 1982-2002) can be generated; it is not necessary to create year-by-year reports for the specific plant.

5) Combine the results of each year generated in Step 3 into a single report (this was performed using spreadsheets for the Cooper GRA). This defines the distribution of events by calendar year.

6) For each year included in Step 3, generate an industry Annual Unit Performance report to extract the mean Service Hours and the number of unit-years included in each year.

7) Using the distribution of industry events (Step 5) combined with the corresponding information about service hours, and the total number of plant-specific events (from Step 4), Bayes Theorem can be used to calculate a posterior distribution, or updated failure rate to use in the GRA.

It should be noted that while the year-to-year variation in number of switchyard transformer events is captured by this approach, the plant-to-plant variation is not. NERC-GADS reports simply do not provide sufficient information to assess plant-to-plant variation. As a result, the resulting distribution from this process is narrower than would be expected. The components in the GRA that have had failure data derived using this process have been flagged for future regeneration of failure rates once the LAMDA database is available or should NERC-GADS output be changed to provide distributions on a cause code basis.

Example – Cause Code 3600 (switchyard transformer)

Distribution of industry events (1982-2002):

Cause Code	Event Type	Occurrences	Total Equiv. Hrs.	Total MWH Lost	Occurrences per Unit Year	HoursLost per Unit Year	Hrs Lost per Occurrence	MWH Loss per Unit Year	MWH Lost per Occurrence	
3600	U1	3	49.94	39,881.95	0.0455	0.7567	16.6467	604.272	13,293.98	1983
3600	D1	2	2.26	1,754.42	0.0274	0.031	1.13	24.0332	877.21	1984
3600	U1	1	26.06	19,597.12	0.0137	0.357	26.06	268.4537	19,597.12	1984
3600	U1	1	32.69	34,978.30	0.0127	0.4138	32.69	442.7633	34,978.30	1985
3600	D1	1	0.95	631.75	0.0115	0.0109	0.95	7.2615	631.75	1986
3600	D3	1	0.59	489.11	0.0115	0.0068	0.59	5.622	489.11	1986
3600	D1	9	25.9	28,421.82	0.0947	0.2726	2.8778	299.1771	3,157.98	1987
3600	U1	1	15	8,115.00	0.0105	0.1579	15	85.4211	8,115.00	1987
3600	D1	1	0.78	837.72	0.0101	0.0079	0.78	8.4618	837.72	1990
3600	U1	2	214	229,836.00	0.0202	2.1616	107	2,321.58	114,918.00	1990
3600	U1	1	33.83	32,645.95	0.0103	0.3488	33.83	336.5562	32,645.95	1991
3600	D2	1	0.07	79.03	0.0102	0.0007	0.07	0.8064	79.03	1993
3600	D1	4	1.69	1,646.45	0.0408	0.0172	0.4225	16.8005	411.6125	1994
3600	D1	1	0.58	429.78	0.0102	0.0059	0.58	4.3855	429.78	1995
3600	D1	5	55.04	62,013.80	0.0515	0.5674	11.008	639.3175	12,402.76	1996
3600	U1	1	33.89	38,668.49	0.0103	0.3494	33.89	398.6442	38,668.49	1996
3600	U1	1	41.8	38,915.80	0.0105	0.44	41.8	409.64	38,915.80	1997
3600	D1	1	14.24	15,948.80	0.011	0.1565	14.24	175.2615	15,948.80	1998
3600	D1	1	0.16	109.28	0.012	0.0019	0.16	1.3166	109.28	2001

(No events in years 1982, 1988, 1989, 1992, 1999 or 2000)

Number of service hours:

YEAR	UNIT YRS.	SERV. HRS.	TOTAL HRS.
1982	58.5	5,577.85	326304.2
1983	66.75	5,438.95	363049.9
1984	71.58	5,475.14	391910.5
1985	77.33	5,847.45	452183.3
1986	85.33	5,691.69	485671.9
1987	90.75	5,906.90	536051.2
1988	95.58	6,206.19	593187.6
1989	103.08	5,972.84	615680.3
1990	103.42	6,298.06	651345.4
1991	103	6,526.90	672270.7
1992	103.92	6,558.26	681534.4
1993	103.42	6,531.14	675450.5
1994	104	6,768.69	703943.8
1995	103	7,098.10	731104.3
1996	103.92	6,815.50	708266.8
1997	102.67	6,476.75	664967.9
1998	98.75	7,010.73	692309.6
1999	97.5	7,621.23	743069.9
2000	92	7,836.50	720958
2001	89	7,858.60	699415.4
2002	92	7,912.51	727950.9

Number of Cooper-specific events in this time period: 0

Assuming a gamma distribution, the following parameters are derived from the above data:

$$\text{prior} = \alpha / \beta$$

$$\text{variance} = \alpha / \beta^2$$

where

α = pseudo number of failures from industry experience (shape parameter)
$= N * \lambda^2 / [N * (M^2 - \lambda^2) - \Sigma\, 1/t_i * \lambda^2]$

β = pseudo time units (duration)
$= N * \lambda / [N * (M^2 - \lambda^2) - \Sigma\, 1/t_i * \lambda^2]$ or α / λ

and

N = number of samples (e.g., number of unit years for this analysis)
λ = sample mean
= number of events / number of operating years for plants in the sample

M^2 = second sample moment
= $\Sigma \lambda_i^2 / N$ (where λ_i - mean number of failures for calendar year i)
t_i = total operating time for each calendar year.

Finally, the posterior distribution is defined as follows:

posterior = $(\alpha + n) / (\beta + T)$

where

n = plant-specific number of failures
T = plant-specific operating years.

From the data for cause code 3600, years 1982-2002:

N = 21 calendar years

λ = 2.8E-2

M^2 = 2.3E-3

α = 0.76

β = 26.6

From the Bayesian update:

Prior	2.8E-02	
CNS Events	0	
CNS Years	16.31	
Posterior	1.77E-2	This is "events per unit year"
=	2.02E-6	"events per hour"

Variance = 5.4E-12

Using Bayesian updating, the failure rate of the switchyard transformers (the Cooper Station has never experienced a failure) is slightly less than the generic failure rate for the time period studied.

Bayesian updating was applied primarily to CNS switchyard and generator components that derived their failure rates from NERC data. The turbine driven feedwater pump failure rate used in the PRA was also replaced with the results of a Bayesian analysis when it was noted that the PRA failure probability for a 24 hour period was very optimistic as compared to what operating experience would suggest.

4.3 Uncertainty Distributions

Uncertainty parameters included in the CNS PRA were used for the corresponding basic events unless the failure rates for those events were modified through the use of NERC data. For the PRA the uncertainty distribution generally used is a lognormal distribution, with an error factor of 3 or 10.

For events using NERC data to derive the failure rate, uncertainty distributions were input if a Bayesian update was performed for an event. In those cases, the variance for a gamma distribution can be generated using the "alpha" and "beta" values calculated during the Bayesian update process, along with plant-specific information on number of failures and operating time. For the previous switchyard transformer example the variance is calculated as 5.4E-12 for years 1982-2002. The calculated variance for the time period of interest is input to the database for later use during model quantification and uncertainty propagation.

4.4 Data Summary

Most basic events included in the CNS GRA used the same failure rates and failure probabilities developed for the CNS PRA, i.e., the information contained in the CNS PRA database was used without change. In some cases, however, the NERC database was used to derive failure rates for use in the GRA.

Appendix B contains a listing of basic events for which NERC data was used to estimate failure rates. That table contains the basic event identifier, its description as included in the system models (fault trees), the NERC cause code used to gather the data, the NERC-derived failure rate (before Bayesian updating), the failure rate (posterior), and the variance calculated from the parameters for a gamma distribution.

5
QUANTIFYING GRA RESULTS

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 *lost generation*, and a measure of the *relative importance* of each system, train and component's contribution to lost generation. These generation risk measures are obtained by quantifying the GRA models described in Section 3 using reliability and generation data such as discussed in Section 4. This section describes the quantification method used for the CNS GRA.

5.1 Quantification of the GRA Models in Terms of Event Frequency

Quantification of detailed fault tree models is typically performed using software designed to apply 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.[2] 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. Most fault tree software packages not only apply the laws of Boolean algebra to produce the cut sets but perform 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.

The CNS GRA used the CAFTA software package [12] (available through the EPRI Risk and Reliability Workstation) to generate and quantify the cut sets for each of the system models, whether supercomponent, detailed fault tree, or PRA to GRA conversion.

5.1.1 Cut Set Generation

Using CAFTA, each of the models for the six GRA systems described in Section 3 was evaluated. The following process was used to produce an initial list of cut sets from each of the GRA models:

- 24 hours was used for all mission time events (this is in part because the failure probabilities for events in the PRA database typically use this mission time, but it is principally for the purpose of assuring all time related, normally running events in the GRA model are assigned a consistent mission time).

[2] 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 minimal 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).

Cut set truncation was performed based on order (the number of events in a cut set – a second order cut set has two events; a third order cut set has three events). For the GRA, third and sometimes fourth order cut sets were generated for each GRA model.

The resulting cut sets basically produce a failure probability "per demand" for each GRA system, very similar to what is produced for the PRA.

5.1.1.1 Conversion of Cut Sets to GRA Units

As one of the desired outputs of the GRA is to produce a frequency of each level of derate, conversion of the "demand" cut set results to time dependent units is necessary. The following steps were taken for each model to make this conversion:

- Eliminate illogical cut sets

  Whether converted from the PRA models or developed specifically for the purpose of performing the GRA, each system fault tree is composed of a combination of mission time and demand events. It is possible for some of the cut sets in the GRA results to be made up of only demand events. Given that the premise of the GRA is that the evaluated systems are supporting power operation, cut sets containing only demand events are considered to be illogical. As an example, it is possible for the instrument air model to produce a cut set containing the failure to start of each of the three air compressors. Given that a plant shutdown is assumed if none of the air compressors are running, this cut set is actually appropriate only for post-trip PRA model purposes and is not a legitimate failure mode of the system for GRA purposes given that there must always be one compressor in service in order for the plant to be at power. Cut sets containing at least one compressor failure to run event in combination with failure to start of the other compressors are legitimate, as the other compressors would receive a demand to start on the failure to continue running of the operating compressor. Therefore, a review of the cut sets for each system was performed to identify those containing only demand events. When encountered, demand-only cut sets were deleted from the results.

  Example:

  SWS-MDP-FS-SWPA SWS-MDP-FS-SWPB SWS-MDP-FS-SWPD SWS-MDP-TM-SWPC

  Three service water pumps fail to start with a fourth out for maintenance. This cut set may be legitimate following a loss of offsite power in which the service water pumps are being sequenced on to the diesels. However, the plant cannot be in operation if no service water pumps are available (e.g., three service water pumps are idle while the fourth is in maintenance). There must be at least one mission time event in each cut set to be legitimate for GRA purposes. As this cut set is applicable only to post-trip conditions, it is deleted from the GRA results as illogical.

- Delete duplicate cut sets for cut sets representing different levels of derates

In developing the GRA logic for a given system, each top event was developed to represent "Failure to operate at a power >x%". While this definition avoided the need to model the failures that lead to a precise power level and therefore simplified the modeling effort, it is possible for this approach to lead to component failures and combinations of component failures ending up in more than one bin associated with the various levels of derate. For example, a pair of buses leading to the 50% derate bin may also support components that, if lost, result in a plant trip. 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. For the Cooper GRA, this correction was made by assigning the duplicate 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 was deleted from those levels to avoid overestimating its contribution to plant generation risk. This step was accomplished using the DeleteTerm feature of the CAFTA cut set editor. Cut sets appearing in the full shutdown (100% derate) bin were deleted from the cut sets associated with the failure to maintain power >33%, >50%, >67% and >90% bins. The cut sets in the failure to maintain power >33% bin were then deleted from the >50%, >67% and >90% bins, etc.

- Change the mission time from 24 hours to a year

  It is desirable for lost production to be characterized in terms of total energy per unit time (e.g., Mwh/month, Effective Full Power Hours/year, etc.). Thus, following the generation of the cut sets the next step is to ensure that the mission time of the system is set to one year. Because the mission time events in the GRA models consistently used a 24 hour mission time, each cut set was multiplied by 365 to change the results from a 1 day to a 1 year measurement period. This correction factor applies whether there is one or several mission time events in a given cut set. For cut sets containing more than one mission time event, it would be inappropriate to increase the mission time to one year for each event as the analysis would then effectively be assuming that if one of the components were to fail sometime within a one year operating period, it would be allowed to remain in its failed state for the remainder of the year without being repaired. That assumption is unrealistic, and therefore is considered to be overly conservative for GRA purposes.

- Address effect of repair and recovery

  Cut sets containing two or more time-dependent failure events must consider the possibility that following failure of one component, repair of that component may be successful before any other component failure occurs, thus preventing the occurrence of the cut set. If a cut set has only one time-dependent failure within it then no such repair is possible since either the cut set has only one event in it (namely, the time-dependent event), or all other events in the cut set are "failure on demand" events which are assumed to fail essentially immediately following failure of the time-dependent event, and thus lead to the shutdown or derate instantaneously (leaving no time for repair). When multiple time-dependent events are included in a failure combination resulting in system failure, one event is arbitrarily assumed to start the chain of failure events. Upon failure of the first component and recognition of that failure by the plant staff, repair efforts will begin. If redundant components (the components comprising the failure combination) fail after the originally failed component

has been placed back in service, then the conditions necessary for the failure combination to result in shutdown or derate are not met. Following failure of the first component the amount of time the other components in the failure combination must continue to operate to avoid system failure is equal to the amount of time it takes to repair the first component. Thus, the mission time of the other components is revised to equal the mean time to repair of the component assumed to be the originally failing component.

To implement the effects of repair and recovery, the GRA cut sets are examined to identify those containing multiple time-dependent events. When two or more such events are recognized in a given cut set, the MTTR value for each time-dependent event is determined (see Section 4) and all MTTR values associated with a given cut set are then summed to derive a sequence-related MTTR. The ratio of the summed MTTR to the original 24 hour mission time is applied as a correction factor to the cut set. This essentially revises the mission time for which the components must operate so that it is equal to the MTTR of the first component that fails in the cut set.

Example:

EAC-CRB-CO-3310	EAC-CRB-CO-3312	X_365	MTTR12
EAC-CRB-CO-3316	EAC-CRB-CO-3318	X_365	MTTR12
EAC-CRB-CC-3306	EAC-CRB-CC-3324	EAM-TML-FR-RANDFRPRT	X_365

In the example, each cut set has at least one time-dependent event (shaded). Thus, each cut set is multiplied by a factor used to increase the mission time from 24 hours to 1 year (i.e., the value of event X_365 is 365). The first and second cut sets contain two time-dependent events. The MTTRs for each event are found from the data analysis effort performed in Section 4, and then added together with the result being appended to the cut set. In this case, both events have the same MTTR (6 hours). Adding the two individual MTTRs together results in a sequence MTTR of 12 hours. Thus, event MTTR12 = (6 hr + 6hr)/24hr = 0.5 and is assigned as a correction factor to the first two cut sets. The third cut set has only one time-dependent event – the other two events in that cut set represent failures of circuit breakers to open on demand. Because there is only one time-dependent event there is no MTTR modifier applied; the demand failures present no opportunity to repair the other, originally failed, circuit breaker and the cut set is assumed to lead to a derate essentially immediately.

For the Cooper GRA, three of the four steps involved in the conversion of the initial fault tree cut sets were automated. The PRA2GRA code [13], an EPRI R&R Workstation based subroutine, takes the cut sets generated from the fault trees, identifies and eliminates the illogical cut sets, increases the mission time of each cut set to a year, identifies cut sets with more than one mission time event, and develops the correction factor to account for repair and recovery. Preventing selected cut sets from showing up in multiple derate bins was performed manually using the CAFTA cut set editor's Delete Term option.

5.1.1.2 Treating Differences Between Operating Experience and the Trip and Derate Frequencies of the Models

Following quantification of the GRA models, it is useful to compare the resulting frequencies of plant trip and the various levels of derate to historical experience. A high-level summary of

plant-specific and industry-wide experience can be developed readily from sources such as NERC-GADS.

Such reviews were completed following initial quantification of the CNS GRA models. As a result additional data assessment was completed for some components. As examples:

- Initial quantification of the Instrument Air System (IAS) using predominantly the original PRA-based failure rates produced a plant shutdown frequency indicating that the plant should have experienced multiple IAS-related shutdowns over its current life, which it has not. An investigation of the results revealed that the major contributors were the air compressors and air dryers, which used failure probabilities included in the original PRA, taken from generic sources. Generation of new failure rates was completed by investigating and then using another data source (specifically, IEEE-500 [11]). The new rates were felt to be more representative of actual compressor and dryer experience and were used to replace the dryer and compressor failure rates from the PRA.
- Comparison of the Main Feedwater GRA results with NERC information showed that the contribution to trips and derates from the turbine driven feedwater pumps was significantly less than industry experience. Comparison of Cooper-specific NERC reports with industry NERC information suggested that Cooper experience with turbine driven feedwater pumps was in fact better than the industry, but not to the degree indicated by the GRA model. The turbine driven feedwater pump failure rate included in the PRA was very small. It was decided to replace this value with one derived from NERC data using the techniques described in Section 4.
- Initial Service Water System results from a frequency standpoint somewhat underestimated industry experience as recorded in NERC. Further, the consequences (discussed in the next section) derived by the GRA were substantially less than indicated by NERC. The Service Water System MTTRs used in the initial analysis were generic values from WASH-1400. A review of NERC data suggested that Service Water component MTTRs were often much longer than these generic values. NERC-based MTTRs were therefore derived for major components in the Service Water System, those MTTRs were substituted for the WASH-1400 values, and the final results aligned much better with industry experience.

Similar reviews were completed for each system modeled in the CNS GRA. The system documentation in Appendix A contains system-specific findings.

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.

The consequences of a load reduction in terms of lost generation are calculated as follows:

Total Lost Generation (Mwh) =
Frequency of load reduction * Magnitude of load reduction * Duration of load reduction

= Frequency of load reduction due to the failure of the system, combinations of trains or components leading to the load reduction *
(1 - fraction of Full Power after load reduction) *
Rated Capacity (Mw) *
(MTTR for the system, combinations of trains, or components + time to restore plant to power, in hours)

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. Sections 4.1 and 4.2 discuss sources of data for both contributors to the duration of an outage.

The quantification of lost generation consequences was accomplished in the CNS GRA by examining each cut set, determining the consequences in units of lost generation and applying a factor to each cut set that reflects the magnitude of those consequences. The following illustrates the process:

- A repair and recovery model was developed to determine how long it would take to restore failed equipment to service. The lower bound of the repair and recovery time would be if all failed components within a cut set were repaired simultaneously. In this case, the longest MTTR of the components within a cut set would dictate the repair time. An upper bound can be estimated if it is assumed that all components are repaired in series. In this case, the sum of the MTTRs for components that make up the cut set would determine the repair time. A realistic estimate is most likely in between these extremes. For the purpose of the Cooper GRA, the upper bound estimate (i.e., the sum of the MTTRs) was used as an initial repair model.
- For plant shutdown situations, the repair time needs to be compared with operating practice with respect to returning to the plant to critical. For the Cooper GRA, it was assumed that a three day planned outage would occur following failures leading to a plant shutdown; this time would be used to perform backlogged maintenance and testing. This assumption was implemented for cut sets leading to a plant shutdown by taking the largest of the sum of the MTTRs and the return to power times, and considering this to be representative of the total repair time. For cut sets leading to partial derates, the sum of the MTTRs of the components was used as noted in the preceding bullet. See Section 4.1.4 for additional discussion of the three day outage time assumption.
- Also associated with plant shutdowns, the time to pull the reactor critical, heat-up the plant and synchronize with the grid requires consideration. As noted in Section 4, typical shutdowns at Cooper take roughly 34 hours to reconnect to the grid. This time was used for cut sets resulting in plant shutdown as additional time at 0% power (additional to the MTTR time, for example) when determining the total lost generation.
- Power escalation to 100% is the last component input to determining consequences of plant shutdowns and derates. Again, a typical plant shutdown was reviewed to determine the power ascension rate following completion of repairs (for derates) or synchronization to the grid (for plant shutdowns). This power escalation rate averaged 1.65% rated power per hour and was used in the determination of total lost generation following a return to power.

The process of assigning consequences to each of the cut sets was automated using the PRA2GRA code referenced in the preceding section. The units of lost generation developed in this code are in terms of effective full power hours (EFPH). Conversion to Mwh can be performed simply by taking the product of the total EFPH for the cut sets and the rated capacity of the plant.

Example 1: 100% derate

EAC-CRB-CF-1FLS EDC-DPL-LP-AA1 X365 MTTR14 **RT00-123**

In this example there are two time-dependent failures (4160 v Bus 1F load shed breaker failure and 125 vdc Distribution Panel AA1 failure), and thus there is a MTTR factor to represent the possible recovery of one component before the failure of the second. Here that factor is shown as event MTTR14 (a 14 hour MTTR, which is the sum of a 7 hour MTTR for each of the two basic events). Because the component failures in this cut set lead to a full plant shutdown a 72 hour (3 day) minimum outage is assumed since this time is larger than the sum of the MTTRs for the time-dependent components that lead to the shutdown. Beyond the initial 72 hours, a 34 hour period is assumed at 0% power for criticality and heat-up. On grid synchronization (which is assumed to occur near 25% power) return to power takes roughly 45 hours (75% power rise at 1.65%/hr). The average power during this power ascension period is 62.5% rated (or an equivalent 37.5% derate). The lost generation for the power ascension period is therefore 17 EFPH (37.5% * 45hr). This combination produces a total loss of 123 EFPH (72 EFPH + 34 EFPH +17 EFPH), represented by the event RT00-123 (the 00 means this is a 100% derate).

Example 2: 50% derate

TG_-TRA-HW-TRA TG_-TRB-HW-TRB X_365 MTTR38 RT50-26

Here a failure to run of Train A of the isolated phase bus duct cooling system is coupled with a failure to run of Train B. The combined MTTR is 38 hours (19 hours for each train). The value for EFPH lost, starting with a 50% derated condition, is 19 EFPH (50% * 38 hr) plus returning to 100% from that point 7.5 EFPH (30 hours at an average derate of 25%), for a total of 26 EFPH.

By coupling the EFPH lost for a given sequence (cut set) with the likelihood of the occurrence of that sequence, and then summing all cut sets together, it is possible to estimate the total EFPH lost for a given derate bin.

Table 5-1 provides an example of the cut set results (in this case, the first 15 cut sets for the 100% derate situation for the switchyard model). The table shows how event probabilities are combined with MTTR and repair/recovery values to calculate the EFPH total for a given derate situation.

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 all the failure probabilities used in GRA have uncertainties associated with them.

For the CNS GRA, a parametric uncertainty analysis was performed for each system. As the bulk of the failure probabilities were taken from the Cooper PRA, the distributions were also accepted from this source. Where NERC data was developed, a gamma distribution was developed as described in Section 4.2

The @RISK and UNCERT codes were used to propagate component uncertainties to the system level. [14, 15] As a simplifying assumption, components of the same type and failure mode were assumed to be completely correlated. A mean value and 5^{th} and 95^{th} percentile values for the evaluation can be produced for each system. It is also useful to "drill down" into the tail of the distribution to determine the key drivers to uncertainty. This was performed using @RISK for the Main Feedwater system (see Appendix A).

Results of the GRA for each of the six systems, including uncertainty distributions, are presented in the next section.

Table 5-1
Top 15 Cut Sets, Switchyard 100% Derate Model

345KV-SWITCHYARD-100-CON = 2.35E+01

#	Cutset Prob	Event Prob	Rate	Event	Description
1	2.26E+01	5.04E-04	2.10E-05	EAC-TRN-ST-MAIN	Main Power Transformer short/fault - requires switchyard isolation
		3.65E+02		X_365	365 days
		1.23E+02		RT00-123	123 full power hours
2	1.08E-01	1.35E-06	5.62E-08	EAC-TRN-NT-T2	Auto Transformer T2 failure
		3.65E+02		X_365	365 days
		2.19E+02		RT00-219	219 full power hours
3	1.08E-01	2.40E-06	1.00E-07	EAC-CRB-CF-10&12	PCB-3310/3312 FTRC CCF
		3.65E+02		X_365	365 days
		1.23E+02		RT00-123	123 full power hours
4	1.08E-01	2.40E-06	1.00E-07	EAC-CRB-CF-18&16	PCB-3318/3316 FTRC CCF
		3.65E+02		X_365	365 days
		1.23E+02		RT00-123	123 full power hours
5	1.08E-01	2.40E-06	1.00E-07	EAC-FST-HW-27XX	Inadvertent Fast Transfer Signal
		3.65E+02		X_365	365 days
		1.23E+02		RT00-123	123 full power hours
6	8.59E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		1.94E-03	8.07E-05	EAM-TML-1L-LIGHT161	161kV Line Fault due to Lightning
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
7	7.50E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		1.69E-03	7.05E-05	EAM-TML-1R-RAND161	161kV Line Fault due to Random Failure
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
8	3.11E-02	6.94E-07	2.89E-08	EAC-TRN-LN-NSST	NSST Failure during normal operation
		3.65E+02		X_365	365 days
		1.23E+02		RT00-123	123 full power hours
9	2.52E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open

345KV-SWITCHYARD-100-CON = 2.35E+01

#	Cutset Prob	Event Prob	Rate	Event	Description
		5.69E-04	2.37E-05	EAM-TML-1M-MAINT161	161kV Line Fault due to Maintenance
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
10	1.62E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		3.65E-04	1.52E-05	EAM-TML-1O-TORN161	161kV Line Fault due to Tornado
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
11	1.02E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		2.30E-04	9.59E-06	EAM-TML-1T-TRANS161	161kV Line Fault due to Transient
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
12	1.02E-02	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		2.30E-04	9.59E-06	EAM-TML-1W-WIND161	161kV Line Fault due to Wind
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
13	8.41E-03	5.00E-04	5.00E-04	EAC-CRB-CC-1606	OCB 1606 Fail to open
		1.90E-04	7.90E-06	EAM-TML-1C-CONT161	161kV Line Fault due to Contamination
		3.65E+02		X_365	365 days
		2.43E+02		RT00-243	243 full power hours
14	5.66E-03	5.00E-05		EAC-CRB-CF-04_02	3304/3302 Fail to open - CCF
		2.02E-03	8.41E-05	EAM-TML-BR-RANDBOONE	Booneville Line Fault due to Random Failure
		3.65E+02		X_365	365 days
		1.25E+00		MTTR30	30 hour MTTR
		1.23E+02		RT00-123	123 full power hours
15	5.66E-03	5.00E-05		EAC-CRB-CF-06&12	3312/3306 Fail to open - CCF
		2.02E-03	8.41E-05	EAM-TML-BR-RANDBOONE	Booneville Line Fault due to Random Failure
		3.65E+02		X_365	365 days
		1.25E+00		MTTR30	30 hour MTTR
		1.23E+02		RT00-123	123 full power hours

6
RESULTS AND APPLICATIONS

Solving (quantifying) the logic models discussed in previous sections produces numerical results that can be used by decision makers to support plant and enterprise planning activities. The results, their interpretation, and applications are the subjects of this section.

6.1 Primary Results

The primary result produced by the GRA logic models (Section 3) and the appropriate data (Section 4) is an estimate of 1) the frequency of plant shutdowns and various levels of derate, and 2) the total generation loss, measured in megawatt-hours and/or Equivalent Full Power Hours (EFPH), on a yearly basis.

Table 6-1 presents a summary of the results for the six systems modeled, along with a comparison to NERC values. More discussion of this comparison is presented in Section 6.1.5.

Table 6-1
Summary GRA Results

System	Frequency (events/operating yr)		Consequences (EFPH/operating yr)	
	GRA	NERC*	GRA	NERC*
SWS	0.05	0.015	8.2	4
Generator				
Shutdown	0.07	0.25	9	33
50%	0.08	-	2	-
IAS	0.08	0.03	11	3
TEC	0.22	0.01	27.4	0.1
Switchyard	0.19	0.25	24	30
MFW/Cnd				
Shutdown	0.24	0.34	30	26
Derates	3.2	4.8	48	28

* NERC population includes all U.S. BWRs (including CNS), 1982-2003, adjusted for specific component types as appropriate (e.g., for TD FW pumps in MFW/Cnd comparison) - except “Generator”, which includes PWRs and BWRs with generators similar in design to CNS

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 implementation of GRA at CNS, a top-down approach was used to identify these contributors. The approach is comprised of the following parts:

- Distribution of risk among the various levels of derate modeled for the selected systems
- Distribution of risk among the systems
- Distribution of risk among the individual components that make up each system.

6.1.1 Breaking Down the Results by System and Derate Level

The bar charts in Figures 6-1 through 6-3 provide the CNS GRA results from different perspectives. Figure 6-1 provides the total lost generation attributable to all modeled systems. In this figure it is obvious that while there are differences between the GRA and NERC industry data, lost generation due to main feedwater/condensate system outages is the major contributor to the cumulative total associated with the six modeled systems.

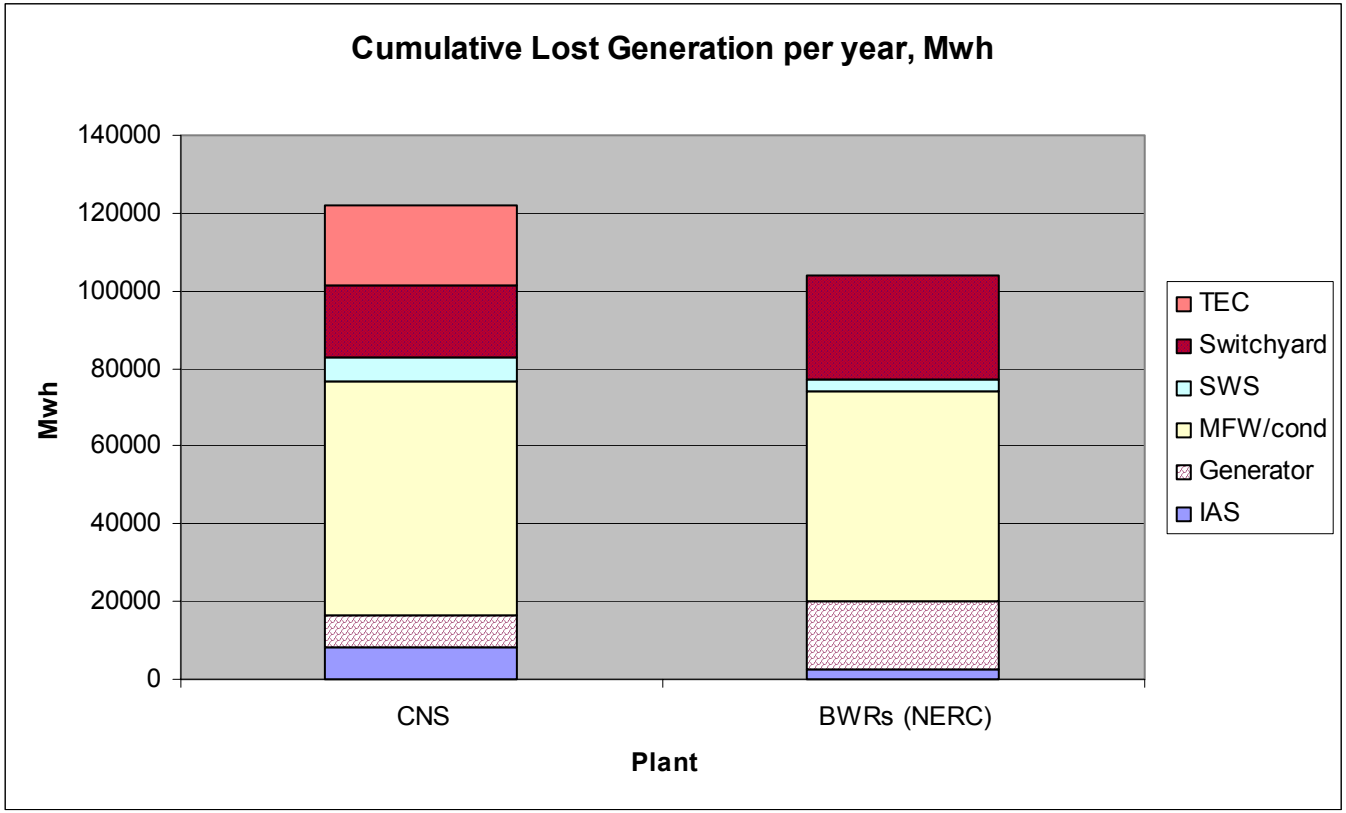


Figure 6-1
GRA Results: Cumulative Annual Lost Generation, CNS

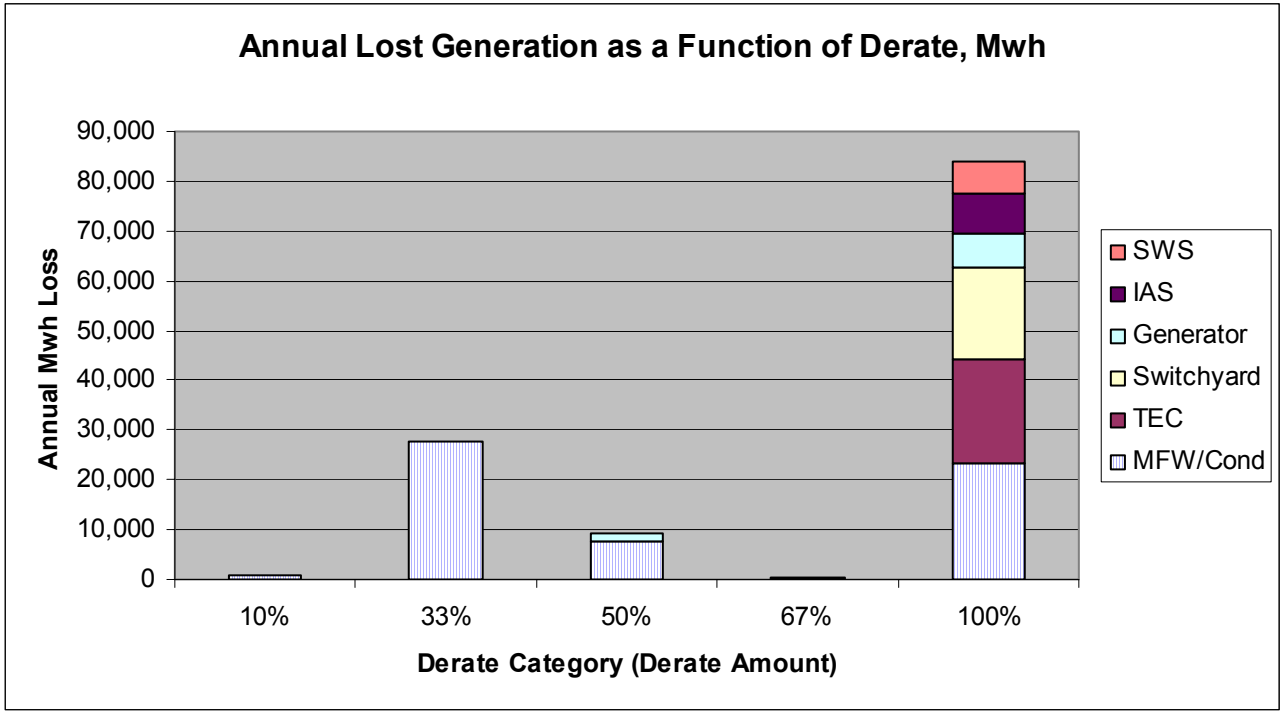


Figure 6-2
GRA Results: Annual Lost Generation as a Function of Derate Amount

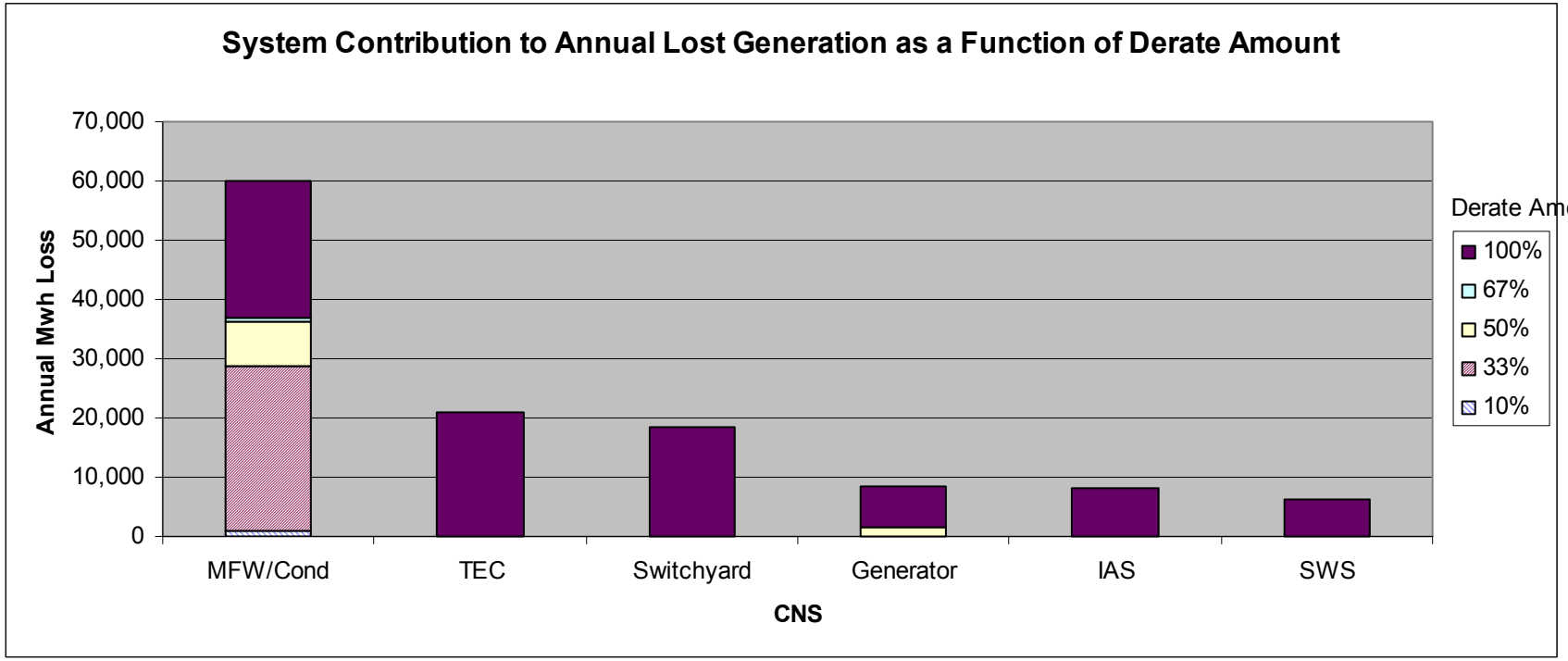


Figure 6-3
GRA Results: System Contribution to Annual Lost Generation as a Function of Derate Amount

In Figure 6-2, the derate categories (the amount of derate, in Mw) defined for the six CNS evaluations are shown on the X-axis. The Y-axis is the average annual Mwh loss estimated by the GRA, with failures resulting in full plant shutdown (represented by the 100% derate category in the chart) being the most significant. Derates in this category (i.e., full plant shutdowns) contribute to a generation loss of nearly 80,000 Mwh per year for the six systems. Power reductions of 33% (approximately 250 Mw derate) contribute about 30,000 Mwh per year. Equipment and system outages that contribute to smaller levels of derate play a relatively insignificant role in the overall picture. Thus, for the six systems modeled, the major contributors to risk at CNS are full plant shutdowns and partial derates to 2/3 rated power.

Figure 6-3 is developed to better understand what is contributing to the annual lost generation. Here, contributions of the six 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 the MFW/Condensate system is the primary contributor to lost generation, with TEC and switchyard events contributing a nearly equal but significantly lesser extent. It is also seen that 33% derates and 100% derates (full plant shutdowns) from the MFW/Condensate failures dominate the contribution to lost generation from that system. The remaining five systems are dominated by failures that lead to a full plant shutdown.

Table 6-2 contains an alternative method of displaying results in the form of a matrix quantifying the percentage of total annual lost Mwh among the six modeled systems and levels of derate. This matrix shows that full plant shutdowns are the largest single category of derate contributors to risk associated with the modeled systems. While the MFW/Condensate system is the largest system contributor to risk from among the six systems, the category of 33% derates due to MFW/Condensate failures is the largest percentage contributor to risk for that system (by a small margin over full plant shutdowns).

Table 6-2
GRA Results: Matrix of Results

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

CNS System	Derate Amount					TOTAL Contribution to Annual Lost Generation
	10% Derate	**33% Derate**	**50% Derate**	**67% Derate**	**100% Derate**	
MFW/Cond	0.8%	22.7%	6.3%	0.4%	19.0%	49.1%
TEC	0.0%	0.0%	0.0%	0.0%	17.1%	17.1%
Switchyard	0.0%	0.0%	0.0%	0.0%	15.0%	15.0%
Generator	0.0%	0.0%	1.2%	0.0%	5.6%	6.8%
IAS	0.0%	0.0%	0.0%	0.0%	6.7%	6.7%
SWS	0.0%	0.0%	0.0%	0.0%	5.1%	5.1%
Total	0.8%	22.7%	7.6%	0.4%	68.6%	100.0%

6.1.2 Breaking Down the Results at the Component Level

With the results reviewed at the system level it is now useful to assess the generation risk significance of individual components. This assessment uses for GRA the measures of *risk importance* described in the GRA guide, namely risk reduction potential (similar to Fussell-Vesely, FV) and risk increase potential (similar to risk achievement worth, RAW).

Use of Importance Measures

Figure 6-4 shows the two measures of importance for the MFW/Condensate system, which is estimated to contribute slightly more than 50% of total lost generation occurring from the six modeled systems. The importance of selected components is discussed to illustrate the type of insights that can be obtained from these measures of importance.

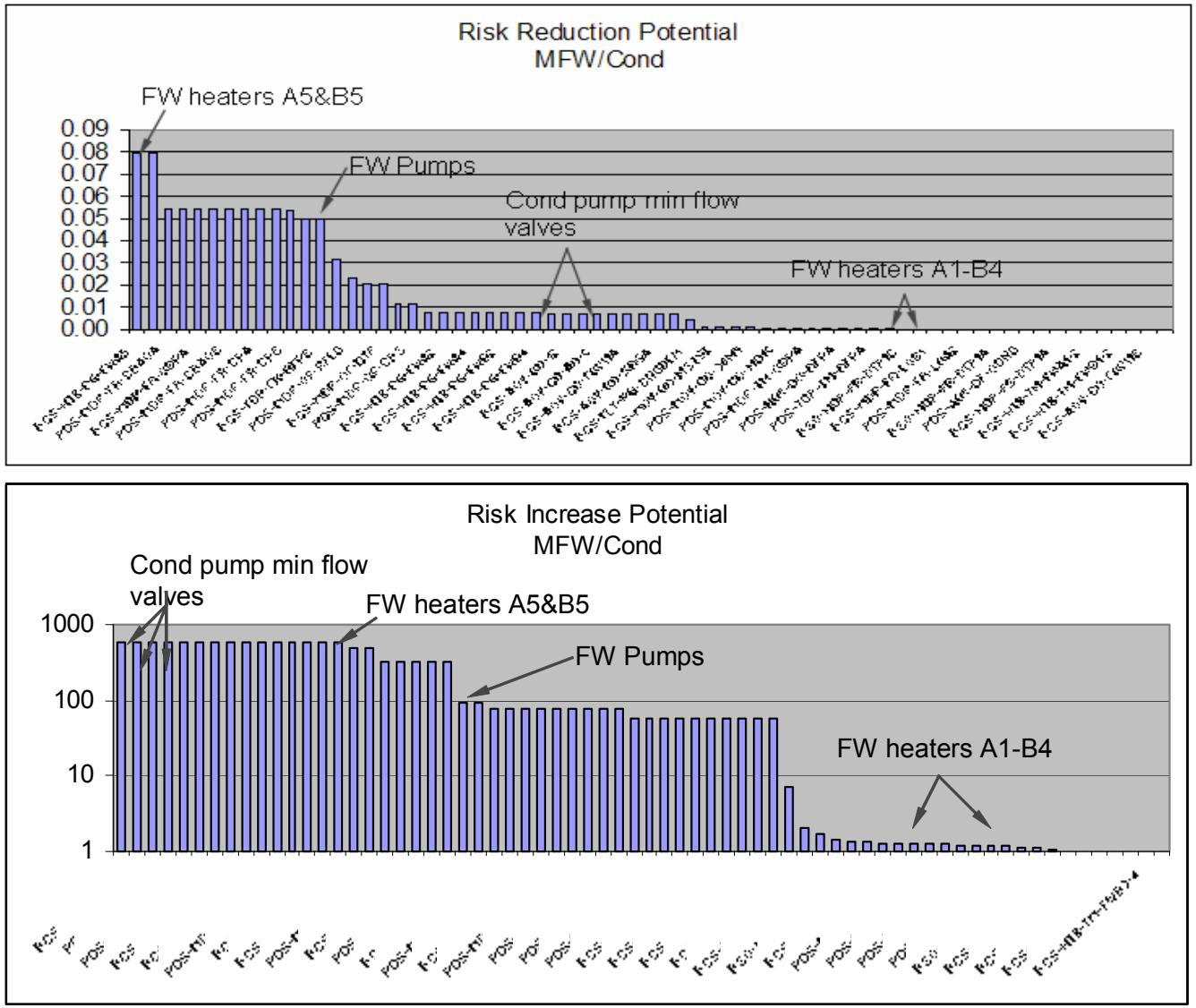


Figure 6-4
GRA Results: Two Importance Measures, MFW/Condensate System

The upper bar chart of Figure 6-4 illustrates the risk increase potential (also known as RAW) measure of importance. 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 booster and feedwater minimum flow and pressure control valves. While designed to prevent damage to condensate, condensate booster, and feedwater pumps under low flow conditions, inadvertent operation of these valves also has the potential to divert flow from the condensate/feedwater systems possibly causing a low reactor level condition. It is this flow diversion failure mode that dominates the risk increase potential importance plot, as opposed to the minimum flow function. The two feedwater heaters connected to the turbine moisture separator drain are also dominant with respect to risk increase potential.

These heat exchangers cannot be removed from service while the plant is at power as they receive flow from the turbine moisture separator drains. Therefore any significant leakage or other problems in these exchangers requires a plant shutdown to effect repairs. Feedwater pumps have a less significant risk increase potential as loss of a single pump leads only to partial derate conditions as opposed to a full plant trip.

The lower bar chart in Figure 6-4 ranks all the major components in the system from highest to lowest in risk reduction potential. It can be seen that the dominant contributors to lost generation for this system are feedwater heat exchangers A-5 and B-5. Again, these heat exchangers cannot be removed from service during operation, so significant leakage from either heat exchanger requires a plant shutdown for repair. Major rotating equipment (such as the feedwater pumps) contributes to lost generation to a lesser extent. Loss of one of these pumps (or a condensate or condensate booster pump) generally results in partial load reductions as opposed to full plant shutdown. Inadvertent operations of minimum flow valves in the feedwater/condensate system leading to plant trips do not contribute significantly to lost generation due in large part to the reliability of the valves (e.g., they are normally closed and need to remain closed to support full power operation). The remaining feedwater heaters are also low in risk reduction potential as they can be bypassed during power operation and the estimated loss in generation without a feedwater heater is estimated to be small. Feedwater pump drain tank pumps are also low in risk reduction potential, largely due to the redundancy provided by these components.

Four-Quadrant Plot

It can be seen with the few component types that have been discussed that any component can be high in risk reduction potential and risk increase potential, low in both measures of importance, or high in one and low in the other. This combination of importance 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 as input to maintenance programs and/or investment in plant capital improvements. The relationship is presented most effectively by plotting the two importance measures on a four-quadrant plot as in Figure 6-5.

The X-axis scales in Figure 6-5 are produced in a straightforward manner. The right-hand side of the axis for risk reduction potential is "pegged" at 1% of the net dependable capacity of the plant. The CNS net dependable capacity used for the GRA is 764 Mw x 8760 hours/year, or roughly 6.7E6 Mwh per year. Dividing that number by 12 (for a "per month" value), and taking 1%, results in a value of approximately 5,500 Mwh per month. This value is reflected at the right hand side of the second X-axis scale.

The third or value scale involves assumptions regarding power price ($/Mwh), economic period over which revenues and costs are discounted (years), and the discount rate (%). For the CNS GRA these have been chosen to be $20/Mwh, five years, and 10%, respectively.

The Y-axis scale of Figure 6-5 represents the sensitivity of the GRA results to changes in the reliability of components included in the model. This sensitivity measure is the slope of generation risk with respect to the failure probability of the component in question. It has units of change in capacity factor per unit change in failure probability for a given component.

A four-quadrant plot such as shown in Figure 6-5 can be used 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. These components are candidates for a corrective maintenance program. However, any strategy that simply provides for replacement or repair of components after their failure should be evaluated for its cost-effectiveness.

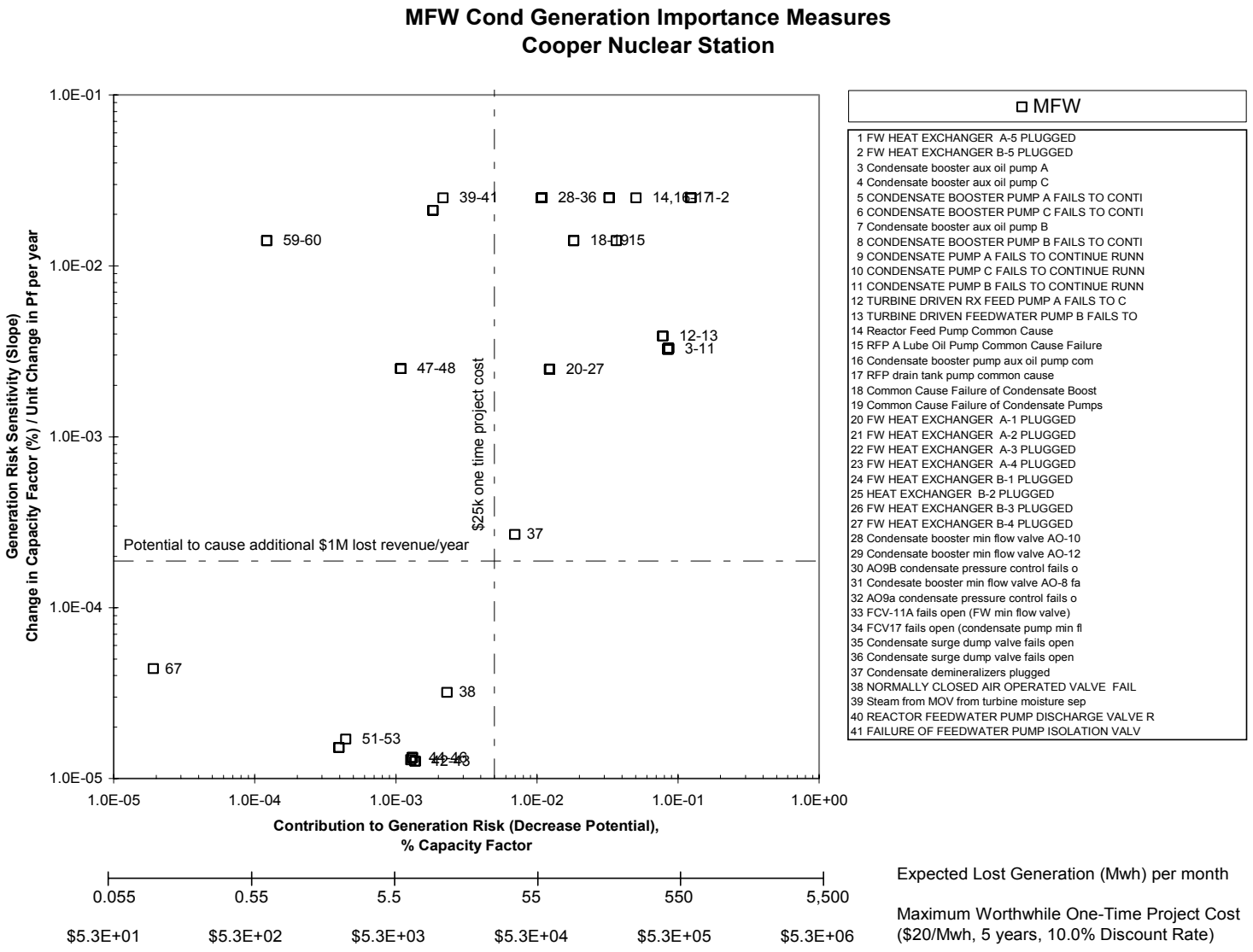


Figure 6-5
GRA Results: 4 Quadrant Plot, MFW/Condensate

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 prior to placing them in a corrective maintenance program.

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 generation 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 (predictive and preventive maintenance programs).

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 or a misapplication of the design of the component) but would not have a significant additional impact on risk if they were to 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 (it is assumed that the plant has already taken all other reasonable actions to improve the reliability of the component and/or decrease its contribution to lost generation; design changes or component replacement may be the only options left).

The discussion above used impact on lost generation as reflected by importance measures (indications of reliability and redundancy) as the parameter of interest. For financial decisions these results must be converted into units appropriate for economic analyses as discussed earlier in this section.

Basis for Thresholds on Four Quadrant Plot

The dashed lines shown in Figure 6-5 roughly divide the plot into regions of importance. They are not generic criteria to be used by all plants for categorizing the importance of generation-related components. Rather, the lines delineate boundaries that are set at the discretion of a plant to distinguish more-important from less-important components according to the viewpoint of management. In setting the boundaries, it is useful to consider both reliability levels (Mwh or capacity factor) and corresponding monetary levels.

To set the vertical divider line, we consider the cost-benefit of proposed activities directed at mitigating the risk from the component in question. For the purposes of the CNS GRA the vertical divider for risk decrease potential has been placed to represent the value of a one time cost (e.g., a capital improvement that would essentially eliminate the risk) of $25,000. In other words, any event with a risk decrease potential larger than this one time cost may warrant increased attention regarding options for improving its reliability. Of course, if the actual cost associated with this increased attention is estimated to be substantially more than that represented by the maximum one time project cost for that particular component, then the effort will not be cost-beneficial.

To set the horizontal divider line, we consider the annual revenue that would be lost from a component being out of service all the time. For the CNS study, this line in Figure 6-5 was set at an annual lost revenue of a million dollars. It would likely be worthwhile to investigate performance monitoring, predictive or preventive maintenance programs that will assure the current performance of components that have the potential to result in lost revenues greater than this.

Use of Contribution to Generation Risk as a Project Evaluation Screen.

For GRA applications, the X-axis scale can be viewed as an upper bound cost estimate for investing in projects to improve the reliability and/or redundancy of components represented on plots like that of Figure 6-5. Since the scale represents the maximum theoretical generation loss that can be eliminated by making a component perfectly reliable, (i.e. the risk associated with a given component is completely eliminated), this value can be used as a screening device when assessing candidate improvement projects. If a candidate project is estimated to cost more than the upper bound value presented on the X-axis, it is probably not a project that should be pursued. Thus, the X-axis value represents the maximum worthwhile present-value project cost for each component displayed on the four-quadrant plot. Projects estimated to cost substantially less than this remain as valid candidates for further, more detailed economic evaluation.

Application of Generation Risk Sensitivity at CNS

As indicated earlier, the Y-axis of Figure 6-5 represents the sensitivity of the GRA results to changes in the reliability of components included in the model. For a unit change in failure probability of a given component over the course of a year, the net effect on the capacity factor of the plant can be estimated from the Y-axis. If a preventive maintenance (PM) program for a

given component were being considered for deletion and the effect of deleting the PM were to be estimated (e.g., it would double the potential for the component failing over the course of a cycle), then the effect of deleting the PM could be converted directly into a change in expected Mwh generated. As an example, the valves represented by data points 47 & 48 in Figure 6-5 have a failure probability over the course of a year of 6E-3. If eliminating the PM was estimated to increase this failure probability to 1.2E-2/yr, then the effects on generation could be estimated as follows:

> Generation Sensitivity for valves (data points 47 & 48) = 0.25% CF (read off of Figure 6-5; Y-axis value for these points is 0.0025, or 0.25%)
>
> Change in failure probability of valves = 1.2E-2 - 6E-3 = 6E-3
>
> Change in capacity factor (CF) due to eliminating PM = 0.25%/yr * 6E-3 * 2 valves = 0.003% CF
>
> Change in generation loss due to eliminating PM (i.e., additional loss over and above that associated with current PM program) = 0.00003 * 764 Mw (maximum dependable capacity (MDC) for CNS) * 8760h/yr = 200Mwh/yr

The question is, of course, how does one go about estimating the effects of the change in PM on the reliability of a given component? Data sources such as LAMDA [9] have been developed to assist in such estimates; eliciting expert opinion from those who are responsible for maintaining and operating the equipment can also be used. EPRI has also developed PM templates that can be used to estimate the failure rate based on types of maintenance tasks, and calculate the expected change in failure rate associated with postponing recommended PMs for given duty cycles. [16]

It should be noted from Figure 6-5 that the same distinct levels of risk increase potential (Y-axis) into which the component results are grouped in the lower bar chart of Figure 6-4 are evident. These levels correspond to the load reduction that would occur if the various components were to fail or be removed from service. For example, the top-most row of data points (points 1, 2, 28-36, etc.) corresponds to the 100% derate (plant shutdown) category. If any one of these components fails, a plant shutdown will result. The second row (data points 15, 18, 19, 59, 60, etc.) corresponds to 67% derates – failures represented by these points will result in a load reduction to 33% full power. (For example, failures of two out of three condensate booster pumps (represented by data point 18) will result in a derate of 67%, down to 33% power.)

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

Lessons Learned from Feedwater System Four-Quadrant Plot

For any system, the most important components to current lost generation are those found in the upper right of the plot. It is these components at which reliability improvement efforts should be directed or programs that at least assure that failures of these components are avoided. The following observations are made from the CNS feedwater results in Figure 6-5.

- For the most part, main feedwater/condensate components that dominate in both risk decrease and risk increase potential are the major rotating equipment (turbine feedwater pumps, condensate pumps and condensate booster pumps). It should be noted that the most significant contributors to lost generation from the pumps are at the 33% and 50% derated levels. Individual pump failures can lead to these partial load reductions whereas full plant shutdown generally requires multiple failures to occur, making a plant shutdown lower in frequency than partial derates.
- One non-pump related component type dominates the potential for full plant shutdown. The GRA suggests that feedwater heaters A-5 and B-5 each contribute to the loss of approximately 0.12% capacity factor (700Mwh/mo). These two heat exchangers cannot be removed from service while the turbine moisture separators are in operation. As a result, the GRA assumes that plugging or leakage of either of these heat exchangers will lead to a plant shutdown.
- Valves found in the upper right include those that, if they fail to remain in position, could lead to a full plant shutdown:

  Minimum flow AOVs in the feedwater condensate system that are assumed to cause sufficient flow diversion to shut down the plant (e.g., FCV-17, FCV-11A, AO-8, AO-9A, AO-9B, etc.). It is noted that because these valves are normally in position to support power operation (e.g., closed) that they only contribute a minor amount to total lost generation; 0.01% lost capacity factor (55Mwh/mo).
- Components located in the upper left of the plot do not currently contribute significantly to lost generation, but could if their reliability were allowed to degrade significantly. Efforts at improving the reliability of these components would be expected to have little effect on generation. Maintenance of the current reliability of these components would be most effective in managing risk. Most of the components in the upper left of the plot represent passive failures of individual components required for power operation.

  Steam supply MOV from the moisture separator to the feedwater pump turbines

  Components that by themselves lead to a partial load reduction:

  - MOVs in the flow path to the reactor (e.g., MO-29, MO-30, etc.)

  - Hydraulically operated steam supply valves to the feedwater pump turbines
- The remaining components are located in the lower left of the four quadrant plot. These components may be candidates for corrective maintenance programs provided they can be shown not to contribute significantly to lost generation in combination.

  Condensate demineralizer bypass valve fails to open

Feedwater heater bypass valves fail closed

Reactor feedwater pump drain tank pumps

Findings such as the above for main feedwater/condensate are contained in the detailed system model and evaluation result descriptions for each of the modeled systems. Those descriptions are provided in Appendix A.

6.1.3 Summary of Important Components

Using the four quadrant plots produced for each system as the primary tool for identification it is possible to prepare a listing of components that dominate the generation loss risk. Table 6-3 contains those components located in the upper right quadrant of the four quadrant plots produced for each of the six modeled systems.

Table 6-3
Summary of Important Components

System	Components	Comments
MFW/Cond	Feedwater Heaters A-5 and B-5	Cannot be taken out of service for repair while plant is on-line
MFW/Cond	Feedwater, condensate booster, and condensate booster auxiliary oil pumps	Primarily single pump failures resulting in partial load reductions as opposed to plant trip
Generator	Rotor windings, voltage control, isolated phase bus duct cooling heat exchangers	Single failures of turbine components result in 100% derate; bus duct cooling heat exchanger failures result in 50% derate
Switchyard	Main Power Transformer, Auto Transformer T2, Circuit Breakers 3310 and 3312 (common cause failure)	Transformers are single failures (i.e., have no redundancy); circuit breakers establish path from main generator to switchyard
Service Water System	Individual and common cause failures of SWS pumps	Major active components in system; single failures of pumps and heat exchangers result in plant shutdown during hottest period of the year
Instrument Air System	Individual air receivers and air dryers; common cause failures of air compressors	Failure of any single dryer or receiver results in plant shutdown; single failures of air compressors not as important because of redundancy (thus the importance of common cause failures)
TEC	Individual TEC pumps, individual TEC heat exchangers, thermocouples	Single failures of pumps and heat exchangers result in plant shutdown during hottest period of the year; thermocouple failures result in control valve failure, isolating flow to the heat exchangers and requiring plant shutdown

6.1.4 Summary of Uncertainty Distribution

As described in previous sections, uncertainty parameters were assigned for events in the GRA models (in most cases, directly from the PRA database). The results of the propagation of these parameters are shown in Table 6-4. Discrete and cumulative probability distributions for the Main Feedwater/Condensate results are presented in Figures 6-6 and 6-7.

Table 6-4
Uncertainty Analysis Results

System	EFPH per year				
	Mean	5%	50%	95%	Standard Deviation
Generator – 100% derate	8.77	0.67	6.6	23.7	8.36
Generator – 50% derate	2.1	0.16	0.9	7.3	4.2
MFW/Cond	78.9	24.6	56.6	195	100
Instrument Air	10.7	3	6.4	27	14.3
Service Water	8.11	1.86	4.1	24.4	16.9
Switchyard	23.1	6.5	21	46.9	12.9
TEC	27.3	15.1	22.5	54.6	17.4

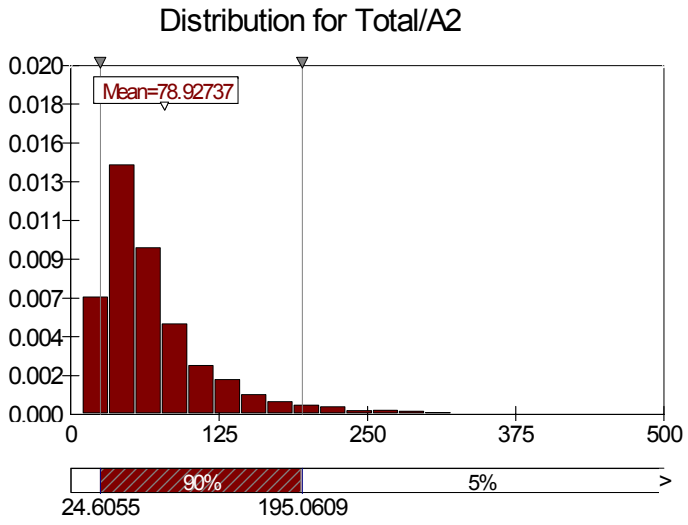


Figure 6-6
Main Feedwater Condensate Discrete probability distribution

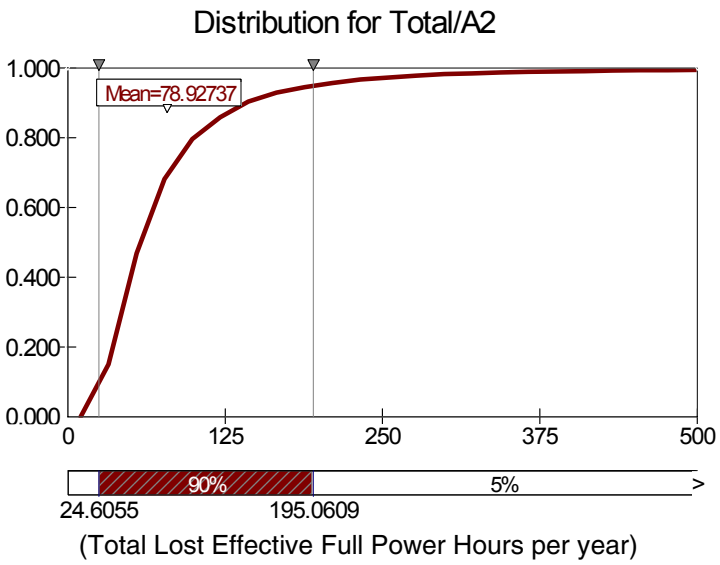


Figure 6-7
Main Feedwater Condensate Cumulative Probability Distribution

6.1.5 Comparison to Industry

As one means of assessing the reasonableness of the results produced for the CNS GRA a comparison to the U.S. commercial nuclear power industry was conducted. The NERC database was used to produce shutdown and derate frequencies for the industry, for each of the six systems evaluated in the CNS GRA. The range of data included events occurring between 1982 and 2003, inclusive. For most systems the population of interest was limited to BWRs. However, due to the small number of BWRs having similar generator designs to CNS, PWRs were included when generating information used in the comparison of generator results.

Other populations were also adjusted as appropriate to focus on specific design features. For example, BWRs with turbine driven MFW pumps were selected when comparing industry results to CNS for the MFW/Condensate system.

Table 6-1 summarizes the results of the GRA and the NERC data analysis for the six evaluated systems. As can be seen from the table, the comparison of both frequency and consequences reveals, for the most part, very good correlation. In almost every case the GRA and NERC values are within a factor of two of each other, if not actually much closer. A few exceptions can be seen: (a) the CNS generator values are lower than industry averages, (b) the CNS IAS values are higher than the industry, (c) the TEC frequency and consequences are much higher than the industry data shows; TEC results are the farthest away from industry averages among the six systems evaluated.

The following provides some insights into these observations of the results for the six systems.

The CNS generator has had only one NERC-reportable shutdown in the 22 calendar-years of plant-specific data included in the NERC-GADS database utilized for the GRA. Thus, the low frequency and consequence values for CNS may be appropriate given plant experience.

The IAS has experienced performance issues in the past, and in fact the piston-type air compressors are in the process of being replaced with screw-type compressors. Thus, although a detailed review of CNS experience versus other BWR experience has not been conducted, the higher values calculated by the CNS GRA appear to be reflective of plant experience.

The TEC system must operate with all pumps and heat exchangers in operation for the hottest period of the year. Any single pump or heat exchanger failure occurring during this time period will result in a plant shutdown. In addition, there is instrumentation whose failure will result in control valve failure, and subsequent plant shutdown, at any time of the year. These failure mechanisms may have more impact at Cooper than in industry at large, resulting in the discrepancy between the GRA values and those representing industry averages. It may be worthwhile to investigate the contributors to the industry values to determine if any are similar to those dominating the Cooper results.

6.2 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 the applications performed or envisioned at CNS using GRA tools and results as major input.

6.2.1 Preventive Maintenance Program Validation and Modification

The TEC system results were used to provide a mechanism for reviewing and validating current preventive maintenance (PM) activities for that system. Following completion of the four quadrant plot the results of the analysis were presented to the TEC system engineer for review. The outcomes of this review were:

1. No unwarranted PM was found. This was determined by ensuring that any components in the lower left quadrant of the plot did not have significant PM resources applied to them.
2. PM activities may be developed for thermocouples installed in the temperature control loops for TEC. At the time of the GRA evaluation those components had a run to failure approach for maintenance. However, the results of the GRA clearly indicate the importance of thermocouple reliability to minimizing plant trips and lost generation.
3. TEC pump reliability is important in minimizing plant trips. At the time of the evaluation a predictive maintenance program (vibration, thermography) was being used to ensure reliability. This may not minimize generation loss. Predictive maintenance is performance based and may result in the requirement for pump change-out during the summer. This change-out would be unadvisable since a plant shutdown would be required. Based on this, preventative maintenance will be considered in the future to ensure that the pumps are reliable throughout summer months.

6.2.2 Loss of Service Water Significance Determination Process Issues

The Service Water System GRA model was used to assist the station in addressing issues that were raised as a part of the Significance Determination Process (SDP) and the NRC's analysis of the Cooper Nuclear Station using the NRC's SPAR models.

Cut sets for the GRA model containing the Service Water pump discharge strainers were generated as part of the GRA evaluation reported elsewhere in this report. Those cut sets provide the frequency of the loss of Service Water initiating event, including a breakdown of the key components contributing to the loss of Service Water.

The PRA cut sets developed for a Loss of Service Water initiating event were merged with the GRA cut sets to provide an integrated set of cut sets for the loss of Service Water accident sequences. This set provided insights as to both what leads to the loss of Service Water event as well as what dominates the ability to provide adequate core cooling following a loss of Service Water.

The results were used to define where the risks lay with respect to loss of Service Water events, and as a basis for suggestions as to how loss of Service Water should be treated in the NRC's SPAR models for Cooper.

6.2.3 Power Critical List/GRA Comparison

At the time of the development of the GRA, the system engineers were in the process of performing the equipment criticality assessment of AP-913. AP-913 guidance recommends placement of power plant components into three categories; critical, non-critical and run to failure. At the Cooper Nuclear Station, the classification of components from a power critical standpoint depends on whether failure of the component can cause a reactor or turbine trip, a derate of >10% rated power or entry into an LCO of <72 hours. Components can be classified as power critical, but to a lesser extent, if they cause derates <10% rated power, redundancy is lost in the ability to prevent a trip or derate or significant economic consequences are expected as a result of a component failure.

At the time of this report, a comparison of the component importance from the GRA and the Power Critical list developed under AP-913 was in progress. Similarities and differences between the lists were being identified and investigated. This effort is expected to:

- Identify components that may be conservatively categorized as Power Critical but do not have a significant potential for affecting lost generation as supported by the GRA. These components would be candidates for reclassification of their criticality under the Cooper equipment reliability program.
- Identify trains of equipment that support power operation, but may not have been a part of the PRA models (particularly those trains which can lead to derates or shutdown due to technical specification or other procedural requirements). These trains of equipment would

be candidates for addition to the GRA models as contributors to potential shutdowns and derates.

7
RESOURCE REQUIREMENTS

This section provides general feedback concerning the labor (time) spent in completing the GRA modeling and analysis.

As is true in almost any project, the time required to complete CNS GRA tasks reduced as the analysts became more experienced with the GRA processes. Estimates of the time required to complete the CNS GRA models, using the various modeling techniques described in earlier sections, are as follows:

Fault Tree Conversion (PRA to GRA)

Converting from a PRA model to a GRA model required approximately 3 person-days of analyst time for the final systems completed in the CNS trial application. This time estimate includes reviewing and converting the PRA fault tree and its success criteria, generating results (including the four quadrant plot), reviewing the model and results with the system engineer at the station, addressing comments, and finalizing the documentation. The system engineer's effort was less than ½ of a person-day total. These models were completed entirely by CNS staff without assistance from outside contractors.

The first models converted required the most time, as both the analysts and the system engineers received training (both formal and on-the-job) about GRA in general, and the modeling tools and techniques in some detail. The initial models, therefore, required about 5 person-days of analyst time and a total of about 1 person-day of system engineer time. These time estimates include training, and therefore are not solely time spent on model conversion.

In all cases, involvement of the Risk Management Supervisor and other staff was minimal.

These estimates compare favorably with (and in fact are lower than) the estimates for labor requirements included in the GRA Implementation Guide for using the detailed fault tree approach with existing models (i.e., PRA to GRA conversion).

Detailed Fault Tree Development "From Scratch"

The switchyard model was developed for the PRA update, and then converted for use in the GRA. The total time to complete the fault tree from start to finish is counted towards the GRA effort. Because the switchyard model was developed in stages over an extended period, the benefits of continuity of effort were lost, thus increasing to some degree the total time that otherwise would have been involved.

That being said, the time required to construct the switchyard fault tree, develop data, convert to a GRA version, and produce and document the GRA results, is estimated to be approximately six person-weeks of analyst effort over the span of time between the start of the PRA fault tree and the completion of the GRA model (a span of several months). This is about a factor of two greater than the estimate in the GRA Implementation Guide. Removing the inefficiencies inherent in spreading a project over many months would remove about one person-week from the total; completing the system after already having experience with the PRA to GRA conversion process would remove another one half to one person-week.

Supercomponent Approach

For the generator system it is estimated that the completion and documentation of the GRA model and results required about four person-weeks of analyst time. Much of this time was spent generating failure rates, MTTR values, and uncertainty parameters from NERC data; construction of the fault tree itself was completed relatively quickly. This level of effort is roughly the same as the estimate provided in the GRA Implementation Guide.

In summary, the labor-hours required to complete a system were approximately:

- Fault Tree Conversion – 48 hours
- Detailed Fault Tree Development – 240 hours
- Supercomponent Approach – 160 hours

8
SUMMARY

8.1 Technical Insights

During the process of developing the GRA models and analyzing the results, some insights about system design and operation were identified. Many of these were known to the system engineers and plant operators, but the GRA results and presentation format provided a different and reinforcing perspective on the issues. Some were new. Some of the key technical insights for the six systems evaluated for the CNS GRA are:

- Generator: good performance overall compared to industry; malfunctions of generator voltage control are top contributors to lost generation
- Instrument air: Single and common cause failures of air compressors dominate. Single failures of air dryers and receivers are important contributors as well.
- Main feedwater: The most significant contributors to lost generation from the pumps are at the 67% and 50% derated levels. Individual pump failures can lead to these partial load reductions, whereas full plant shutdown generally requires multiple failures to occur. One non-pump related component type dominates the potential for full plant shutdown, namely, feedwater heaters A-5 and B-5. Plant shutdown is required to address plugging or leakage of these heaters (they cannot be removed from service while the turbine moisture separators are in operation).
- Service water: Strainer plugging issues are important contributors, as are other failures during the summer and "hottest summer" portions of the year. During the hottest periods of the year the system becomes essentially a single train (i.e., all pumps and heat exchangers are required to maintain the plant at 100% power).
- Switchyard: Main transformer failures dominate contribution to lost generation. 345kv ring bus arrangement has significant redundancy, other than the T-2 transformer.
- Turbine equipment cooling: During the hottest part of the year the system loses all redundancy and lost generation is dominated by single failures (i.e., all pumps and heat exchangers are required to maintain the plant at 100% power). Thermocouples associated with control valves are key contributors to generation risk throughout the year.

8.2 GRA Process Lessons

In piloting the GRA at Cooper Nuclear Station, the Cooper staff was looking to obtain experience in the practicality of the development of quantitative models for business decision making and to determine the types of personnel needed to not only develop the models but interpret the results. The following summarizes lessons learned in this regard.

- A reasonable amount of effort is all that is required to develop a GRA system model (person-days as opposed to weeks). This is particularly true if there is system modeling already available as a part of the PRA. Because of the existence of PRA information (particularly data), it does not take nearly the effort to produce GRA models as was the case for the plant-specific PRA.
- GRA modeling can be developed a system at a time and then immediately applied. There is sufficient information within each individual model to generate insights with respect to current system, train and component contributions to lost generation, potential contributions to lost generation if reliability were to degrade, input to cost-benefit evaluations, etc. There is no need to develop a full scope, integrated GRA before its application.
- At this time, an experienced PRA analyst is needed to develop and quantify GRA models. Tools for automated development of GRA models do not yet appear to be sufficiently developed that they can be implemented by non-PRA personnel (such as system engineers) without significant training or assistance from PRA experts. However, there are promising software tools on the market that, if converted to formats more intuitive to system experts, could be a first step to the production of GRA models by non-PRA personnel with limited assistance and review by PRA experts.
- With minimal training and indoctrination, non-PRA personnel (system engineers, managers) can interpret and apply the results of a GRA. Such applications include
  - Component importance (in terms of potential change in risk if reliability or availability changes are anticipated as well as current contribution to lost capacity factor or generation).
  - Simple cost benefit analysis for capital improvements or changes to maintenance practices.

    The format of the results is important in allowing engineers and managers to use the GRA results and must be in terms with which they are familiar in the day to day operation of the plant.

8.3 GRA Generic Lessons

Investigation of the various methods of modeling and obtaining data for components for the six Cooper GRA systems revealed the following insights:

- Plants having balance-of-plant modeling that is already a part of the plant-specific PRA have an advantage in the development of GRA models.
  - Fault tree logic for individual trains of equipment and data assignment may be largely complete for these systems. It may only be necessary to change some top logic in the fault trees to change the success criteria from a safety focus to a generation focus to produce GRA models. Review of the capacities of trains of equipment within the balance-of-plant model from the PRA also can reveal additional changes that are needed to the logic to eliminate component failure modes that are important only following a

plant trip and add events that are not a part of the PRA as they support power operation but are not needed post-trip.

- Modification of PRA cut sets to reflect
  - GRA related mission times
  - generation-related repair and recovery activities, and
  - consequences associated with trips and derates

  is a viable approach to producing GRA results.

- For the most part, existing data from the plant-specific PRA appears to produce reasonable generation-related results.
  - Adjustment of failure data may be necessary for selected components have a significant effect on the results and do not appear to have failure rates consistent with plant or industry experience.
  - The NERC-GADS database appears to be a reasonable source of GRA failure data for components that are not explicitly modeled in the PRA. Generation of failure rates from this source can be somewhat labor intensive.
- GRA model results for CNS appear to agree with industry experience.
  - Estimates of the frequency of plant shutdowns and derates and overall consequences (lost Mwh) as derived from the GRA models compare reasonably well with NERC reported experience (often within a factor of two or three)
  - Where there are significant differences between the GRA results and industry experience, it can often be explained by
    - seasonal variation in seasonal success criteria (e.g., more pumps and heat exchangers needed in summer months than during winter)
    - Plant-specific equipment performance that leads to less reliable system operation than industry averages.

8.4 Candidate Tasks for Further Development of GRA

Two distinct areas of improvement should be considered in the further development of GRA: demonstration of the applications of GRA and improvements in the efficiency of constructing GRA models.

Further Demonstration of the Application of GRA

The selection of the first few systems for the Cooper pilot study was centered on potential immediate applications of the GRA. These applications included evaluation of the effects of currently planned design changes and component replacements (switchyard transformer and instrument air compressors), system performance issues (service water system strainer performance) and implementation of ongoing industry sponsored programs directed at improvement of equipment reliability (AP-913). With the availability of models for the first six

systems, the GRA is already being used to make decisions regarding investments that are worthwhile for several of the systems.

To increase the credibility of GRA as a decision analysis tool, demonstration of its ease of use for several other applications is suggested. These applications include:

- Development of input for the performance of a cost-benefit analysis for a planned capital improvement
- Assist in the next step of AP-913 implementation by providing performance criteria for key plant equipment
- For selected generation related components
  - Estimate the effects of improving/decreasing maintenance activities for selected components using the recently completed LAMDA database
  - Support cost-benefit evaluation of these maintenance changes
- Provide quantitative input to review of operating events leading to plant trips
  - Support root cause analyses
  - Help focus corrective action

Improvements in the Efficiency of Developing GRA Models

- Automate input/output to the GRA
  - Integrate with LAMDA
  - Automated data extraction from NERC
  - Automated fault tree development (KB3/RBDA)
  - Presentation of results in a variety of business formats (graphical/tabular)
- Make applications more efficient
  - Conversion of PRA cut sets to GRA cut sets
  - CAFTA/UNCERT enhancements
- Integrate with EOOS/Safety Monitor

9
REFERENCES

1. EPRI, “Risk-Informed Asset Management (RIAM) Development Plan,” Report 1006268, June 2002.

2. EPRI, “Risk-Informed Asset Management (RIAM) – Method, Process, and Business Requirements,” Report 1009632, May 2005.

3. EPRI, “LcmVALUE Version 1.5 – LCM Planning for SSC - LCM Planning Tool,” EPRI Software 1003455, August 2002.

4. EPRI, “Generation Risk Assessment (GRA) Plant Implementation Guide,” Report 1008121, December 2004.

5. EPRI, “Pilot Application of Enterprise Project Prioritization Process at NPPD,” in progress.

6. Minner, G.L., et al, “PEPSE and PEPSE-GT Volume 1 Manual, User Input Description”, SCIENTECH, Inc., Idaho Falls, ID, 2002.

7. 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.

8. North American Electric Reliability Council (NERC), “pc-GAR for Windows,” Release 2.06 v26, 2004.

9. EPRI, “LAMDA (Long-term Asset Management Database) 1.0,” Software 1011927, December 2005.

10. U.S. Nuclear Regulatory Commission, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

11. IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Data for Nuclear-Power Generating Stations, (1984).

12. EPRI, “CAFTA”, EPRI Software, version 5.1a, 2003

13. Applied Reliability Engineering, Inc., “PRA2GRA,” 2005.

14. Palisade Corporation, “@Risk, Version 4.5”, October, 2004.

15. Nuclenor, Iberdrola, and Data Systems & Solutions, “Uncert for Windows”, Version 2.3a, 2002.

16. PM Basis Database, Version 5.1.1, EPRI Software Product 1010919, May 2004.

A
COOPER NUCLEAR STATION GRA MODELS

This appendix contains system documentation summarizing the development of the GRA models completed for the Cooper Nuclear Station GRA trail application. These system documents were prepared by the analyst primarily responsible for completing the evaluation of the system. They contain descriptions of success/failure criteria, modeling and data assumptions, results, and comparison to industry experience.

(Note: in the system write-ups that follow, references are typically grouped by category or type of reference (e.g., “Operating Procedures,” “Lesson Plans,” “Fault Trees,” etc.). Some of the references may not be explicitly cited in the documentation.)

Main Generator

Rev. 0 8/1/05

1. System Function

GRA Function: The Main Generator converts rotational energy of the Main Turbine into electrical energy to maintain the economic viability of CNS.

The Auxiliaries provides for the safe operation of the Main Generator by providing a means to remove the heat generated, and seal the generator from contaminants, and by providing a source of excitation to the generator field.

2. Success/ Failure Criteria

Plant Disconnected from Grid – 100% Derate

The success/failure criteria of the generator are dictated by the operation of the generator and its auxiliaries. For the purposes of the Generation Risk Assessment (GRA), failure of any component part of the generator, or failure of any of the auxiliaries of the generator listed below is assumed to result in either a direct failure of the generator, or the need to take the generator off-line to avoid additional damage. Either situation results in a 100% loss of generation to the grid.

Auxiliaries whose failure will result in generator failure (generator off-line) are:

- Main Generator Gas System
- Seal Oil System
- Isolated Phase Bus Duct Cooling System
- Generator Protective Devices (failure = inadvertent function)
- Radio frequency Monitor Alarm

Some of these auxiliaries in turn require the successful operation of supporting systems:

- AC power
- DC power
- Turbine Equipment Cooling

Plant Derate - 50% Derate

From Section 2.2 of CNS Operating Procedure 2.2.53 – Isolated Phase Bus Duct Cooling System, main generator output is limited to 50% load when bus duct cooling is not available. Therefore, failure of the bus duct cooling system is included as a contributor to a 50% plant derate condition.

3. Fault Tree Modeling

3.1 Development of Fault Tree

There was no "generator" fault tree existing in the PRA model, and therefore the model was developed from scratch.

1. The top event for the 100% derate situation was defined to be Loss of Transmission to the Grid or Loss of Generator. This was done to take into account switchyard faults that result in a turbine generator trip (e.g., failure of CB 3310 and 3312 to remain closed; circuit faults that cause the switchyard to isolate; etc.).
    a. Modeling of Loss of the NSST captured the majority of these faults. Gate EAC-SY-002E, No Power from NSST, was extracted from the Plant Centered LOSP fault tree and combined ("merged") with the generator fault tree.
    b. Failure of the NSST to operate while the SSST was being repaired, and failure of the SSST to operate while the NSST was being repaired, were deleted from the model, since these are appropriate for "loss of power following a transient" event, and not "loss of generation".
    c. All other SSST events were deleted.
    d. The Plant Centered LOSP fault tree was also updated to include changes suggested by the Grid Reliability Study completed in late 2004. These changes primarily were associated with additional detail for the loss of 345KV lines attached to the switchyard – ultimately these changes had no impact on the final results of this evaluation.
2. Generator and generator auxiliary faults were modeled to be consistent with cause codes in the NERC GADS database. This is essentially representative of a "supercomponent" approach to fault tree modeling.
3. However, ac power and TEC were included as supporting systems where necessary. To do this, system operating procedures were reviewed to determine the ac power sources for auxiliaries such as H2 Cooling, Lube Oil Cooling, etc. Then, the "merged.caf" fault tree was reviewed to determine if it contained modeling of the ac power bus or panel supplying power to the auxiliary. If modeling was included, the associated gates were extracted as separate fault trees, and then combined ("merged") with the generator fault tree. The following gates were extracted:
    a. Gate EAC-L-500, no power to critical MCC-L.
    b. Gate EAC-T-500, no power to critical MCC-T.
    c. Gate TEC-HTX-500, Insufficient TBCCW Flow.

i. All events associated with pump restart following a loss of offsite power (LOSP) were deleted. Pump re-starting is not a GRA related condition. Corresponding operation actions to start an idle pump that is placed in auto after a LOSP was also removed.

4. If a direct link to an existing model within the merged.caf tree could not be found, a "placeholder" transfer event was added to the generator fault tree model. This was done for the following:
   a. EAC-H2_-AC-MCCB: No ac power from MCC-B
   b. EAC-H2_-DC-250V: No dc power to EE-STR-250TURB
5. Any initiating events (events starting with "%") included in the extracted fault trees combined with the generator fault tree were set to False to eliminate them from the fault tree. These events were used in PRA model as house events for the purpose of accident sequence quantification.

<u>50% Derate</u>

1. A search of the NERC database revealed no events, generic or plant-specific, related directly to the Isolated Phase Bus Duct Cooling components. Therefore, the system was modeled as a single heat exchanger with two redundant blowers (fans).
   a. The fans each receive ac power from a separate MCC, now modeled as an undeveloped transfer event (these MCCs are not included in the "merge.caf" fault tree).
      i. Train A was modeled with event EAC-H2_-AC-MCCB (same event as included for the 100% derate situation)
      ii. Train B was modeled with event EAC-TG_-AC-MCCG (no power to MCC-G)
   b. Cooling of the heat exchanger is modeled via a transfer to gate TEC-HTX-500 (the same gate used for the 100% derate situation).

3.2 Modeling Assumptions and Comments

1. For the GRA, the exposure time of interest for all components is one year. For the base model, operating times of 24 hours were assigned to the data, which were then updated to a one year exposure time using the PRA2GRA conversion code.
2. Any failure of a generator or generator auxiliary component modeled at the level of a NERC Cause Code was assumed to result in failure of the generator. In other words, all NERC cause codes represent "single" failures within the fault tree – failures that by themselves fail the generator.
3. It is assumed that any event that results in a full plant derate (100% power) leading to cold shutdown causes the plant to implement the 3 day outage plan. This means that all cold shutdown events have minimum outage times of 72 hours before the plant begins to heat up to return to power. Thus, even if a component has a mean time to repair of less than 72 hours, the plant remains shutdown for 72 hours to complete other repairs.
4. See Section 4 for assumptions specific to data.

50% Derate

1. Train A is assumed to be operating, with Train B in standby.
    a. Therefore, Train B has a "failure to start" event.
2. Common cause failures to run of the blowers are included.
    a. A 10% beta factor is used to represent common cause failures of the redundant trains.
3. A placeholder event is included to capture unspecified, undeveloped bus duct cooling failures that could contribute to a 50% derate.
4. Failure of the heat exchanger is modeled by combining "heat exchanger plugged" and "heat exchanger ruptured" failures, using failure rates included in the PRA database for these two events.
5. According to plant staff, one train of the blowers has experienced significant repair and maintenance in recent history, such that the system is essentially operating as a 1 train system (note, however, that this is not reflected in NERC records). Thus, a sensitivity analysis was conducted in which one train of the blowers was "turned off" in the fault tree model. The results are reported later in this document.

4. System Reliability Data

The PC-GAR software program (v2.06) was used to develop failure rates (failure per hour) for all components represented by cause codes within the fault tree. For other components, i.e., those included in fault tree logic "merged" into the generator fault tree from other existing fault trees, the failure rates (per demand and per hour) included in the PRA database was used.

Failure rates from NERC data were developed by dividing the number of "forced outages" by "service hours", for each specific cause code. Subsequently, these rates were updated using a Bayesian update technique – see "Bayesian Update Approach" discussion below.

For the baseline data:

1. Generator data within PC-GAR was filtered to include as closely as possible industry-wide data only for US nuclear units having generators similar in design to that of the Cooper generator.
2. "Forced outages" included any event classified as U1, U2, or U3 within PC-GAR, for each specific cause code.
3. "Service hours" were calculated by taking the average annual service hour value, provided by PC-GAR for the set of plants specified, and multiplying by the total number of "unit-years" given by PC-GAR for that set of plants.
4. Cooper-specific data from PC-GAR were used if available. For the generator system, only one cause code exists within the PC-GAR database for Cooper, namely, cause code 4700, Generator Voltage Control. For this single cause code the number of forced outage event occurrences and the total number of service hours are limited to Cooper values.

"Mean time to repair" values were also extracted from NERC by taking the "hours per occurrence" as representative of the repair/recovery time. When multiple forced outage categories (i.e., U1, U2, U3) exist for a specific cause code, a weighted average of the hours per occurrence was used to derive a MTTR for the cause code.

It is important to note that NERC (PC-GAR) defines the hours per occurrence as the amount of time between when the plant becomes desynchronized from the grid (this is the event start time) until the plant is resynchronized to the grid (this is the end time). Thus, the NERC "hours per occurrence" includes not only time to repair the fault, but also may include ramp up time from shutdown power level (e.g., 0%) to the power level at which the plant synchronizes to the grid. Cooper synchronizes to the grid at approximately 20% full power – it is assumed that this value is similar for other plants.

In addition, it must be pointed out that an outage, in the NERC database, is a disconnection from the grid. It is not necessarily a "plant trip" or "plant shutdown" or "plant scram", as may typically be thought of at a nuclear unit when the word "outage" is mentioned. Thus, all plant scrams/trips/shutdowns are NERC outages, but not all NERC outages are plant scrams/trips/shutdowns.

Thus, short "hours per occurrence" are possible in the NERC database because the plant may have disconnected from the grid but may not have proceeded to cold shutdown following a component fault. Following repair of the equipment the plant was quickly brought back up to the power level where synchronization occurred.

To begin the GRA evaluation, each system cause code is reviewed and an assessment is made as to if a plant shutdown to cold shutdown would normally take place in order to repair the component fault. The "hours per occurrence" in the NERC database may provide a clue, i.e., if the hours are short (for example, less than 50) this may indicate that the plant stayed in hot standby during component repair. Conversely, if the hours are long (for example, greater than 100 or so), it may mean that cold shutdown occurred. System engineers and other cognizant analysts should be consulted to determine the appropriate plant response. If the majority of component repairs would require cold shutdown, then it is assumed that ALL would require cold shutdown (and vice versa). This assumption impacts the subsequent treatment of "heat up time"(see next section).

When cold shutdown is assumed for all cause codes, the Cooper-specific heat up time from 0 to 20% (approximately 34 hours) was deleted from the NERC-derived "hours per occurrence" for any value greater than 100. The resulting value was used as the "mean time to repair the equipment". NERC-derived values of less than 100 hours were used as-is.

For the generator system a cold shutdown is assumed to be necessary to complete any repair of a component whose outage leads to a 100% derate.

When MTTR values could not be derived from NERC (e.g., if no NERC data existed for specific cause codes), other sources – such as WASH-1400 – may have been used in place of the default value utilized by the PRA2GRA code.

Bayesian Update Approach

The baseline rates for events utilizing NERC data were updated using a Bayes update technique. This was completed for two purposes: (a) to account for Cooper-specific experience, which in most cases appears to be better than industry experience (i.e., Cooper has reported fewer events than the industry average); (b) to develop information used in an uncertainty evaluation (see Section 6.3).

To perform the update, the following steps were completed:

1. Produce NERC cause code data for the generator system for each year 1982-2002 – each year generated within its own file. Produce this data for the appropriate population of US nuclear power plants, WITHOUT Cooper data included
    a. Also generate the annual service hours for each year for this population of plants
2. Maintaining the break down by year of event, combine all D1, D2, D3, U1, U2, and U3 events for a given cause code to determine the total number of events, by year.
3. Produce NERC cause code data for the generator system for the Cooper Nuclear Station only, for the period 1982-2002. This does not have to be done on a year by year basis.
4. Using the formulae for producing Bayesian update, generate "prior" and "posterior" results for each cause code by entering the distribution of industry (non-CNS) events by year, and updating with the number of CNS-specific events over the entire period.
5. For uncertainty analysis purposes, a gamma distribution is assumed for the NERC data. Using the information developed by the Bayesian update process a variance can be calculated. The variance and the mean are then entered into the CAFTA database for the basic event or its type code (the event itself if it is a "demand" type of event; the type code if its failure probability is calculated using mission time).

The Bayes-Gamma spreadsheet listed in the References section (under Uncertainty Analysis) contains the results of the Bayesian update, along with the parameters calculated for the gamma distribution.

<u>50% Derate</u>

Because no NERC events for the Isolated Phase Bus Duct Cooling system were found in the database, quantification of the 50% derate case relied predominantly on data included in the PRA for like-components. Mean time to repair values were set using the default value set by the user in the PRA2GRA code, or values included in the PRA database for similar component types.

Uncertainty distributions generally followed those assigned in the PRA database.

5. Cutset Post Processing

The following was performed on the generator system cutsets to obtain the final system top event frequency.

1. The PRA2GRA code was used to convert mission times from 24 hours to 1 year.
2. The PRA2GRA code also assigned "mean time to repair" values, based on assigned values.
   a. A default value of 168 hours was used for any event not specifically assigned.
3. PRA2GRA was then used to assign consequences, i.e., the number of equivalent lost full power hour hours associated with the component outage. This is calculated as a function of the derate and the amount of time required to restore the plant to 100% power. The time is in turn a function of the "mean time to repair the equipment", plus the "heat up time" (to restore the plant to 20% power, when the plant is synchronized to the grid), plus the time required to go from 20% to 100% power.
4. A code called SetEventStates (developed by AREI – see References) was used to help produce cutsets containing only non-generator system basic events. These cutsets were then deleted from the results of the PRA2GRA evaluation, using CAFTA's "Delete Term" tool, to arrive at the final set of cutsets, namely, those containing at least one generator system basic event.
5. The result is the amount of "equivalent full time hours" lost as a result of component failures associated with the generator system.
6. For the 50% derate case, the "3 day outage" assumption (see Section 3.2, #3) was not employed. "Heat up time" (see #3, above) was also set to 0 hours.

Eliminating cutsets containing only non-generator system basic events had a significant impact. For the 100% derate evaluation the top contributors to the results were associated with transformer failures (Main and NSST) that result in load rejection and generator trip. Removing those contributors substantially lowered the lost MWh estimate. A similar impact was noted for the 50% derate situation.

6. Results

The yearly frequency for generator system failure resulting in a 100% derate, as modeled for the GRA, is 0.0681. This failure rate is approximately one failure every 14 to 15 years. The rate reflects the low incidence of reported generator-specific issues at the Cooper Nuclear Station, and in fact is consistent with the fact that only one Cooper event (cause code 4700, generator voltage control) is recorded in the NERC database over the 16.3 operating-years of data represented in the NERC-GADS database used for this evaluation (an operating-year is equal to a calendar-year x average service hours (hours plant was available and on-line) divided by 8760 hours/calendar year; for the 22 calendar-years included in the NERC-GADS database for CNS, the average service hours per year was approximately 6490: (22 x 6940/8760 = 16.3)). Bayesian

updating for other cause codes using industry data accounts for the increase from 1 in 16 years to 1 in 14 years.

For the 50% derate situation, the yearly frequency for failures in the Isolated Phase Bus Duct Cooling system resulting in the derate is approximately 8.4E-2, or roughly once every 12 years. No Cooper-specific duct cooling events are recorded in NERC, so this frequency is derived using industry data.

When factoring in consequences (in other words, the amount of full power equivalent hours lost as a result of system unavailability), there are a total of 8.96 effective full power hours lost per year, on average, due to generator system component failures resulting in 100% derates, and another 1.99 hours lost due to 50% derates – for a total of 10.95 hours per year from all causes. If full power is equal to 764 MWe, this means that there is an average of 8366 MWh lost per year due to generator related issues.

It must be noted that failures in support systems, such as Service Water, TBCCW/TEC, etc., significantly increase the frequency of generator unavailability. For example, loss of cooling to the duct bus cooling heat exchanger results in the loss of that component and then a 50% derate. However, those support systems are or may be treated separately within the GRA, and their impacts should be addressed within the context of those evaluations. The results and discussions here and in subsequent sections focus solely on components explicitly identified as being part of the generator and its sub-systems.

6.1 Top Contributors

100% Derate

The top contributor to system failure resulting in a 100% derate is a failure of generator voltage control (NERC cause code 4700). This event is recorded in NERC as a Cooper-specific event – in fact, the only Cooper event in the NERC database for 1982-2003. Thus, the system failure frequency is dominated by a plant-specific event occurrence, at 0.068 per year.

All other event contributors to 100% derate utilize industry wide (non-Cooper) data updated to reflect zero Cooper-specific events. The next highest contributor to system failure is “other exciter problems” (cause code 4609), at 0.0015 per year, followed by failure of the H2 Cooling System piping and valves, cause code 4610 (less than 1E-3 per year).

When considering mean time to repair and restore power to 100% full power, the generator voltage control event remains the top contributor; its “equivalent full power hours lost” of 123 hours, multiplied by its yearly frequency, results in an average annual loss of 7.5 full power hours.

All other contributors add much less than 1 hour annually to the total of 8.96 hours lost due to 100% derates.

50% Derate

The top contributor to system failure is a failure of the bus duct cooling heat exchanger (rupture or plugging), at 0.076 per year. The failure rate for this event is based upon generic data for heat exchanger plugging plus heat exchanger rupture. Because there is a single heat exchanger, failure results in total system unavailability.

The next contributor is an event representing common cause failure of the two blower trains. This event is based on a generic value for "fan fail to run".

The next cutsets are associated with Train A failing to run and Train B failing to start, followed by Train A failing to run and Train B failing to run.

When considering mean time to repair and restore power to 100%, the average annual loss of effective full-power hours is estimated to be 1.99 hours, with most of these (1.8) coming from failure and subsequent repair of the bus duct cooling heat exchanger.

Sensitivity Study – 1 Blower Train in Operation

If it is assumed that only one blower train is actually in operation, the likelihood of failures resulting in 50% derate increases. The frequency of a 50% derate increases by roughly 100%, to 0.16 per year, while the MWh lost due to these derates also goes up by about 100%, from 1.99 to 4.1 hours per year.

This increase in both frequency and economic impact should be considered if the plant continues to operate in a mode that is more like a "one blower" than "two blower" system.

6.2 Comparison to Industry

Using the PC-GAR code, a comparison was completed for average MWh lost for plants with generators similar to Cooper's to the value derived from the GRA model. For all outages (disconnections from the grid, not derates) due to all generator causes (cause codes 4500-4899, without 4830, 4831, 4840 – major and minor overhaul, and inspection, respectively), the average number of MWh lost for this set of plants was roughly 16500 per year; Cooper's 100% derate loss is about 6850 Mwh (8.96 hours * 764 MW at full power). Thus, the industry average is a bit more than a factor of 2 higher than Cooper's. This difference, although not dramatic, may be from factors such as Cooper design, estimated heat up time, etc.

The frequency of shutdowns caused by generator failures for the industry population selected for the GRA evaluation is 0.26 per operating year. This is not quite a factor of four higher than calculated using the GRA model with CNS-specific data.

To develop the generic values from NERC, the following assumptions were used:

1. The column "MWh lost per Unit Year" in the PC-GAR output represents all MWh from when the plant first experiences the event and drops from 100% load, until the plant is reestablished at 100% load.

2. Effective Full Power Hours per unit year can be calculated by dividing the total MWh lost per unit year (from all generator causes) by the median Net Dependable Capacity (in MW) for the set of plants contained in the database. Net Dependable Capacity is included on the report "Annual Unit Performance" in PC-GAR. For this evaluation and the set of plants chosen to represent generator cause codes, this value is 794.5 MW.
3. To calculate on a "per operating year" basis, the "per unit year" values are multiplied by 8760 (the number of hours in a calendar year) and divided by the average Unit Service Hours for the population included in the database. From PC-GAR for all U.S. BWRs, 1982-2003, this value is 6407 hours.

Employing these assumptions, the effective full power hours per operating year estimated by using information in PC-GAR for the set of plants with generator designs similar to Cooper's is 31.6 hours. This is a bit more than a factor of 3 higher than the full power hours calculated using the GRA fault tree and the PRA2GRA code.

The differences between "generic" NERC values and CNS-specific values may be explained by the excellent performance of the generator during the CNS operating lifetime. As noted earlier, CNS has reported only one generator-related shutdown in the 16+ "operating-years" of operation represented by the NERC-GADS data used in the evaluation (an operating-year is equal to a calendar-year x average service hours per calendar-year (hours plant was available and on-line) divided by 8760 hours/calendar year; for the 22 calendar-years included in the NERC-GADS database for CNS, the average service hours per year was approximately 6490: (22 x 6940/8760 = 16.3)). Industry experience for plants other than Cooper that have similar generator types shows a higher outage rate.

Appendix A contains additional information, namely, comparisons of the GRA results to another source of industry information. EPRI report "Life Cycle Management Planning Sourcebook, Volume 5: Main Generator" (1007423, July 2003) summarizes main generator performance based upon NPRDS/EPIX data, as well as NERC/GADS data. These summaries were used as other comparison points to check the reasonableness of the Cooper GRA model.

The EPRI report does not distinguish between derate conditions – it is assumed therefore that all discussion in the EPRI report is valid for 100% derate cases.

Table A-1 that follows contains a comparison of Sourcebook reported performance data and that of the Cooper GRA model. The first part of the table compares NPRDS/EPIX to the GRA (mostly NERC, Bayesian updated) data. The second part of the table compares the EPRI report's NERC-derived values to those derived independently for this GRA (and then updated using Bayesian updating methods) for the GRA.

From the table it can be seen that although there is wide variation in the failure rates assigned to individual components, there is very good correlation between the EPRI Sourcebook values and those of the Cooper GRA model at the "system" level. The system failure frequency is 0.095 (NPRDS/EPIX) vs. 0.068 (Cooper GRA), with an average of 21.5 forced outage hours (the

terminology used in the Sourcebook, derived from NPRDS/EPIX) vs. 8.96 "full power hours" for Cooper GRA. The forced outage frequency (defined in the Sourcebook as forced outage hours/period hours) is .002 (NPRDS/EPIX) vs. .00095 (Cooper) – within a factor of 3. (It is assumed that a "forced outage hour" as used in the Sourcebook is equivalent to an "effective full power hour" as defined for the GRA.)

Using NERC data, the EPRI Sourcebook calculates a forced outage rate, defined as forced outage hours /(forced outage hours + service hours), of .0053 for all BWRs, and .0073 for BWRs of 800-1000 MW. Using the definition for forced outage rate, the Cooper GRA model calculates a forced outage rate of .00138 – within a factor of 4 and 6, respectively.

Finally, note that the Sourcebook's estimate for "forced outage hours" of 21.5 compares very favorably to the "effective full power hours lost" estimated by using information in PC-GAR for the set of plants with generator designs similar to Cooper's (20.8 hours – see discussion earlier in this section).

50% Derate

As mentioned previously, no NERC events have been recorded for failures of the bus duct cooling system. In addition, the generator sourcebook does not contain discussion of this system. Therefore, no direct (explicit) comparison can be made using those two sources. However, the fact that no events are included in the NERC database can be used to imply that the failure rate and/or the hours lost per occurrence or per unit-year should be low (e.g., a failure rate of essentially zero). Because the GRA model employed here derives a value of approximately 0.1 per year for system unavailability, it may be reasonable to conclude that the use of generic data for heat exchanger rupture and plugging is conservative and not necessarily representative of industry experience specific to the bus duct cooling systems. A lower failure rate for the heat exchanger, and for the system in general, would result in a correspondingly lower annual contribution to lost Mwh.

Changing (reducing) the failure rate of the heat exchanger by a factor of ten reduces the hours lost from 1.99 to less than 0.5, illustrating the sensitivity of the results to the failure rate chosen.

For the purposes of this evaluation, the baseline heat exchanger failure rate remains at the generic failure rate.

Using PC-GAR for plants with generators similar in type to Cooper's, and employing the approach discussed above for the 100% derate case, the "industry" value for Mwh lost per year due to generator-related derates is 914. This translates into about 1.1 effective full power hours. This is about 55% of the value estimated for Cooper, supporting the statement that the failure rates used in the GRA model for the heat exchanger may be somewhat (but not excessively) higher than industry data would support for the bus duct cooling system. However, it may also be the case that Cooper's design and/or operating procedures are different from other plants.

6.3 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the generator fault tree. The figure represents components in both the 100% and 50% derate cases.

> The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the system to lost generation given the current reliability of components as assumed in the GRA.
>
> The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur if the reliability of the individual components was allowed to degrade significantly.

The most important contributions to current lost generation are the components represented by the events found in the upper right of the plot. Data point 1 is the generator voltage control; data point 2 represents the isolated phase bus duct cooling heat exchanger. Data point 3 is also located in the upper right quadrant; this data point represents common cause failure of trains A and B of the isolated phase bus duct cooling system; data point 4 is the generator rotor windings; data point 5 is "other generator problems."

Other components that impact the lost generation potential of the system, but to a lesser degree, are those in the upper left quadrant. Those include the H2 Cooling System components, the exciter, and many generator components.

Points 25, 26, and 27 are in the lower left quadrant. These components represent the Train A blower and Train B blower of the isolated phase bus duct cooling system. These components (and those truncated from the analysis) may be candidates for corrective maintenance programs provided they can be shown not to contribute significantly to lost generation in combination – and in fact data point 3, representing common cause failures of both trains, is located in the upper right quadrant, indicating that the combined failures of Train A and Train B blowers do in fact contribute to lost generation.

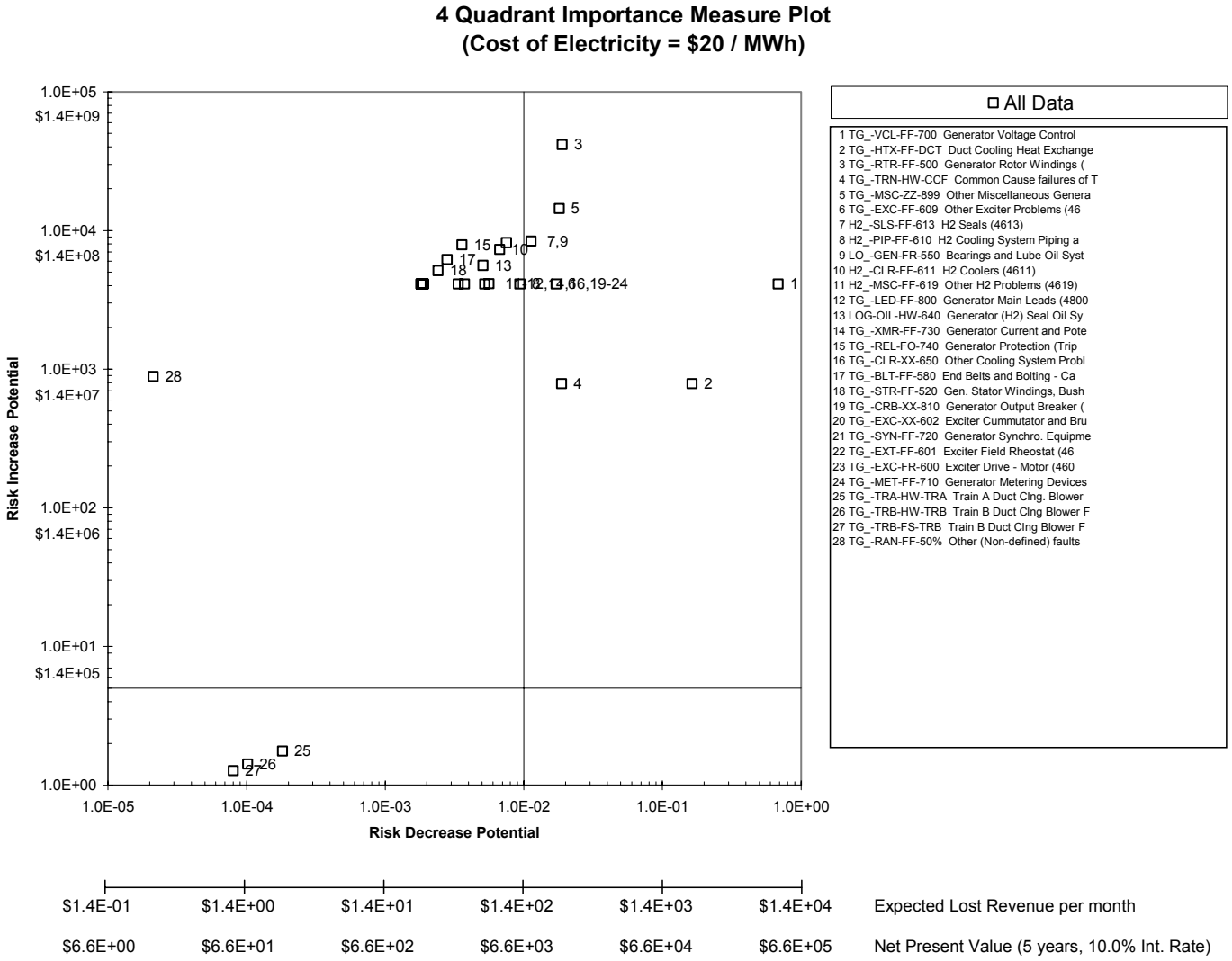


Figure 1
Four Quadrant Plot for Generator System

6.4 Uncertainty Analysis

A generator uncertainty analysis was performed using UNCERT, a CAFTA add-in program. In the analysis, UNCERT assigns a correlation factor of 1 for all basic events with the same component type and failure mode.

The results of the analysis are shown in Figures 2, 3, and 4, following the References section (multiply values in Figure 2 by 1E+06).

Figure 2 represents the 100% derate case:

#Iterations = 10000
Mean lost generation = 8.77 effective full power hours (EFPH) lost per year
Std Deviation = 8.36 full power hours lost per year

Cumulative Probability	Lost Generation (EFPH)
5%	0.67
50%	6.6
95%	23.7

Figure 3 represents the 50% derate case:

#Iterations = 10000
Mean lost generation = 2.1 full power hours lost per year
Std Deviation = 4.2 full power hours lost per year

Cumulative Probability	Lost Generation (EFPH)
5%	0.16
50%	0.90
95%	7.3

Figure 4 represents the sensitivity study in which only one train of operation is assumed available for the isolated phase bus duct cooling system:

#Iterations = 10000
Mean lost generation = 4.0 full power hours lost per year
Std Deviation = 6.4 full power hours lost per year

Cumulative Probability	Lost Generation (EFPH)
5%	0.53
50%	2.3
95%	12.9

7. References

Cooper Operating Procedures

1. 2.1.10 - station power changes
2. 2.1.4.3 - power reduction to less than 25%
3. 2.2.14 - 22KV electrical system
4. 2.2.51 - Hydrogen gas system
5. 2.2.51A - Hydrogen gas component checklist
6. 2.2.52 - Hydrogen seal
7. 2.2.52A - Hydrogen seal oil component checklist
8. 2.2.52B - Hydrogen seal oil instrument valve checklist
9. 2.2.53 - Isolated phase bus duct cooling
10. 2.2.53A – Isolated phase bus duct cooling component checklist
11. 2.2.77 Main Turbine
12. 2.2.77A – Turbine generator checklist
13. 2.4 GEN-H2 Generator or Hydrogen Abnormal

Cooper Operator Training – Lesson Plan

1. COR0011301R13-L-OPS Main Generator and Auxiliaries
2. COR0011301R13-S-OPS Main Generator and Auxiliaries
3. COR0011302R12-L-OPS Main Generator and Auxiliaries
4. COR0011303R05-L-Main Generator

Fault Trees, Results, and Database

1. CNSGRASwyrdGenSWS8-1-05.rr
   8/1/2005 10:59 PM
2. Compare NERC to EPIX for generator components 4-7-05.xls
   4/7/2005 01:47:50 PM

3. Cooper Main Generator 100% Derate GRA Model Basic Events 4-7-05.txt
   3/28/2005 01:09:12 PM
4. Cooper Main Generator 100% Derate GRA Model basic Events 4-7-05.xls
   3/28/2005 12:59:04 PM
5. Cooper Main Generator 50% Derate 1 Train Blowers GRA Model 4-7-05.cut
   3/28/2005 01:53:12 PM
6. Cooper Main Generator 50% Derate 1 Train Blowers GRA Model FINAL WITH GENERATOR EVENTS ONLY - CO... 8/2/2005 12:11 AM
7. Cooper Main Generator 50% Derate 1 Train Blowers GRA Model MTTR 8-1-05.cut
   8/2/2005 12:10 AM
8. Cooper Main Generator 50% Derate 1 Train Blowers GRA Model.caf
   1/26/2005 02:23:46 PM
9. Cooper Main Generator 50% Derate GRA Model 4-7-05.cut
   3/28/2005 01:02:36 PM
10. Cooper Main Generator 50% Derate GRA Model basic events.txt
    4/6/2005 11:25:52 PM
11. Cooper Main Generator 50% Derate GRA Model basic events.xls
    3/28/2005 01:09:54 PM
12. Cooper Main Generator 50% Derate GRA Model FINAL WITH GENERATOR EVENTS ONLY - CONVERTED 8-1-05.cut 8/1/2005 11:52 PM
13. Cooper Main Generator 50% Derate GRA Model MTTR 8-1-05.cut
    8/2/2005 12:54 AM
14. Cooper Main Generator 50% Derate GRA Model.caf
    3/28/2005 06:12:00 PM
15. Cooper Main Generator ALL DERATES GRA Model FINAL WITH GENERATOR EVENTS ONLY - CONVERTED 8-1-05.cut 8/2/2005 12:16 AM
16. Cooper Main Generator100% Derate Plant Trip GRA Model.caf
    3/16/2005 12:02:30 PM
17. Cooper Main Generator100% Derate Plant Trip GRA Model.cut
    3/16/2005 11:58:02 AM
18. Cooper Main Generator100% Derate Plant Trip GRA Model - MTTR 8-1-05.cut
    8/1/2005 11:44 PM
19. Cooper Main Generator100% Derate Plant Trip GRA Model FINAL WITH GENERATOR EVENTS ONLY - CONVERT... 8/1/2005 11:46 PM
20. Four Quadrant Plot Generator 8-1-05.xls
    8/2/2005 12:38 AM
21. Non-generator 100% derate cutsets for use in Delete Term 4-7-05 100% derate case.cut
    3/17/2005 02:22:32 PM
22. Non-generator 50% derate cutsets for use in Delete Term 4-7-05 50% derate case.cut
    4/6/2005 11:28:26 PM

PC-GAR (NERC) Spreadsheets

1. 10-AnnualUnitPerformance all w_o CNS 1982 Gen specific.xls
   2/18/2005 12:02:16 PM
2. 10-AnnualUnitPerformance all w_o CNS 1983 Gen specific.xls
   2/18/2005 12:03:30 PM
3. 10-AnnualUnitPerformance all w_o CNS 1984 Gen specific.xls
   2/18/2005 12:04:44 PM
4. 10-AnnualUnitPerformance all w_o CNS 1985 Gen specific.xls
   2/18/2005 12:05:42 PM
5. 10-AnnualUnitPerformance all w_o CNS 1986 Gen specific.xls
   2/18/2005 12:06:40 PM
6. 10-AnnualUnitPerformance all w_o CNS 1987 Gen specific.xls
   2/18/2005 12:07:40 PM
7. 10-AnnualUnitPerformance all w_o CNS 1988 Gen specific.xls
   2/18/2005 12:08:40 PM
8. 10-AnnualUnitPerformance all w_o CNS 1989 Gen specific.xls
   2/18/2005 12:09:50 PM
9. 10-AnnualUnitPerformance all w_o CNS 1990 Gen specific.xls
   2/18/2005 12:11:00 PM
10. 10-AnnualUnitPerformance all w_o CNS 1991 Gen specific.xls
    2/18/2005 12:12:16 PM
11. 10-AnnualUnitPerformance all w_o CNS 2003 Gen specific.xls
    2/18/2005 12:13:30 PM
12. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1982 2-18-05.xls
    2/18/2005 12:31:20 PM
13. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1983 2-18-05.xls
    2/18/2005 12:32:44 PM
14. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1984 2-18-05.xls
    2/18/2005 12:33:40 PM
15. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1985 2-18-05.xls
    2/18/2005 12:39:44 PM
16. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1986 2-18-05.xls
    2/18/2005 12:34:46 PM
17. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1987 2-18-05.xls
    2/18/2005 12:40:38 PM
18. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1988 2-18-05.xls
19. 2/18/2005 12:47:20 PM
20. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1989 2-18-05.xls
    2/18/2005 12:48:22 PM
21. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1990 2-18-05.xls
    2/18/2005 12:49:14 PM
22. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 1991 2-18-05.xls
    2/18/2005 01:06:50 PM
23. 10-IndCauseCodeTotals ALL w_o CNS w_generator specific Follow Events 2003 2-18-05.xls
    2/18/2005 01:06:44 PM
24. 1-AnnualUnitPerformance ALL US 1-4-05.xls
    1/6/2005 10:17:22 AM

25. 1-CompCauseCodeLosses ALL US ALL GENERATORS 1-4-05.xls
    1/4/2005 05:21:52 PM
26. 1-IndCauseCodeTotals ALL US ALL GENERATORS 1-4-05.xls
27. 1/4/2005 05:58:16 PM
28. 2-Cooper EventsbyDate 1982-2003.xls
    1/27/2005 06:41:24 AM
29. 2-IndCauseCodeTotals - GENERATOR ONLY, COOPER ONLY.xls
30. 2/18/2005 01:50:22 PM
31. 6-AnnualUnitPerformance ALL US w_generator specific Follow Events 1-4-05.xls
    1/6/2005 03:15:56 PM
32. 6-CompCauseCodeLosses ALL US w_generator specific Follow Events 1-4-05.xls
33. 1/6/2005 10:18:32 AM
34. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1-4-05.xls
    3/9/2005 04:54:34 PM
35. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1992 1-27-05.xls
    1/27/2005 07:06:56 AM
36. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1992-2002 1-27-05.xls
    2/18/2005 12:02:52 PM
37. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1993 1-27-05.xls
    1/27/2005 07:06:18 AM
38. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1994 1-27-05.xls
    1/27/2005 07:06:02 AM
39. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1995 1-27-05.xls
    1/27/2005 07:08:04 AM
40. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1996 1-27-05.xls
    1/27/2005 07:08:42 AM
41. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1997 1-27-05.xls
    1/27/2005 07:13:12 AM
42. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1998 1-27-05.xls
    1/27/2005 07:13:40 AM
43. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 1999 1-27-05.xls
    1/27/2005 07:14:54 AM
44. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 2000 1-27-05.xls
    1/27/2005 07:15:12 AM
45. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 2001 1-27-05.xls
    1/27/2005 07:16:32 AM
46. 6-IndCauseCodeTotals ALL US w_generator specific Follow Events 2002 1-27-05.xls
    1/27/2005 07:17:08 AM
47. IndCauseCodeTotals ALL US w_o CNS w_generator specific Follow Events 1982-2003 2-18-05.xls
    2/18/2005 03:20:58 PM

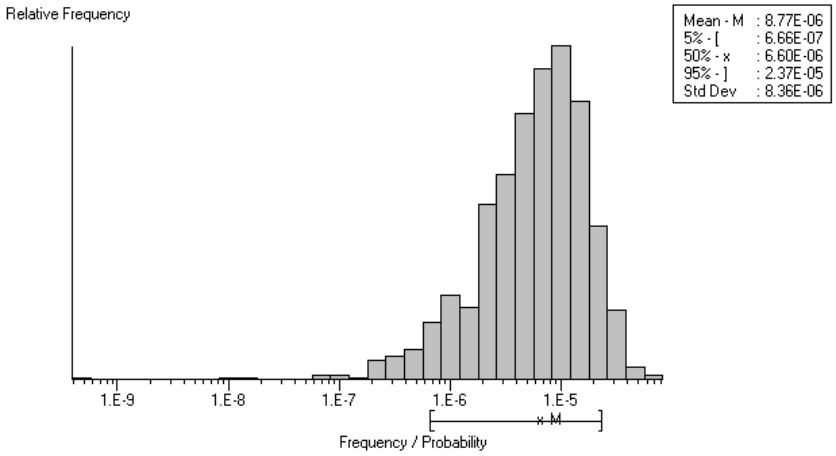
Uncertainty Analysis Spreadsheet

1. CNS Generator NERC bayes-gamma March 2005.xls
   3/30/2005 03:13:28 PM

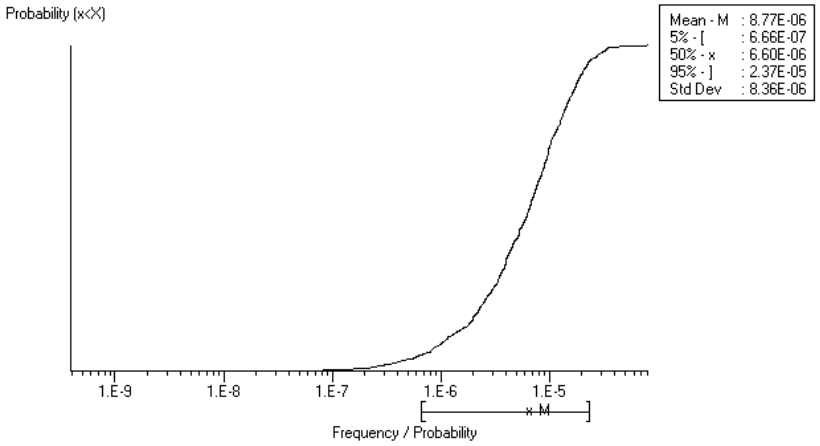
Other

1. EPRI, "Life Cycle Management Planning Sourcebook, Volume 5: Main Generator" (1007423, July 2003)
2. North American Electric Reliability Council (NERC), "pc-GAR for Windows", release 2.06 v26, 2004
3. Applied Reliability Engineering, Inc., "PRA2GRA", August 1, 2005.
4. Electric Power Research Institute (EPRI), "CAFTA", version 5.1a, 2003
5. Applied Reliability Engineering, Inc. (AREI), "SetEventStates.exe", March 2005.
6. Nuclenor, Iberdrola, and Data Systems and Solutions, "Uncert for Windows", Version 2.3a, 2002.

Density Function



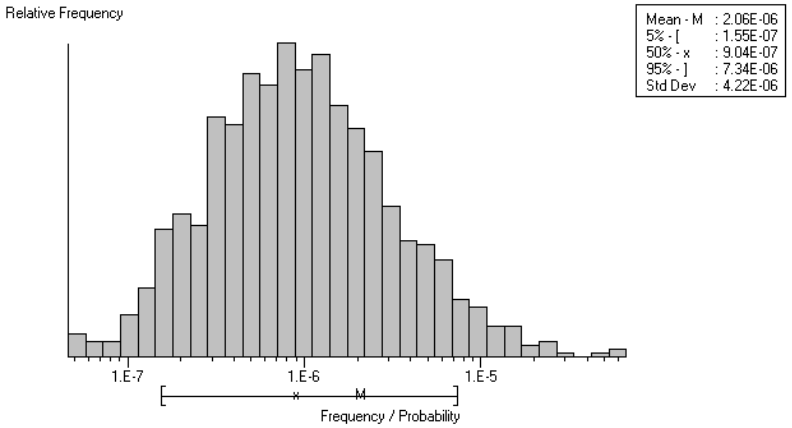
Cumulative Function



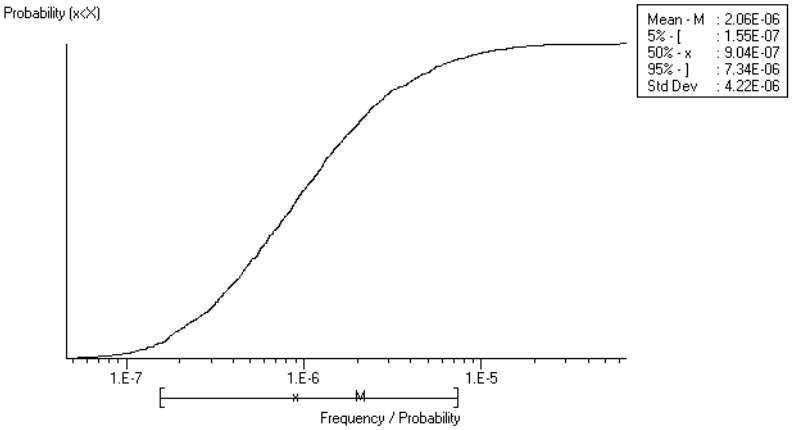
(NOTE: Multiply all values by 1E+06 to obtain actual results.)

Figure 2
Uncertainty Analysis Results – Generator, 100% Derate

Density Function



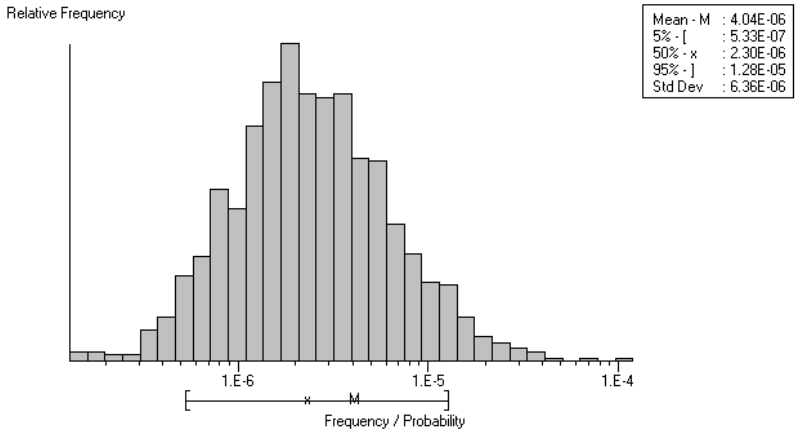
Cumulative Function



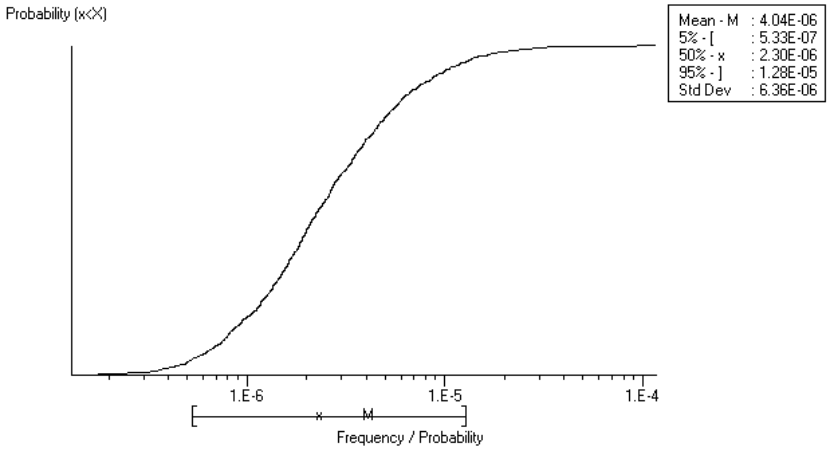
(NOTE: Multiply all values by 1E+06 to obtain actual results.)

Figure 3
Uncertainty Analysis Results – Generator, 50% Derate

Density Function



Cumulative Function



(NOTE: Multiply all values by 1E+06 to obtain actual results.)

Figure 4
Uncertainty Analysis Results – Generator, 50% Derate, 1 Train Blowers in Operation

APPENDIX A – ADDITIONAL COMPARISONS TO INDUSTRY DATA

Table 1
Comparison of Results, EPRI Generator Sourcebook and Cooper GRA Model

EPRI SOURCEBOOK		COOPER GRA MODEL			RATIO	
Component(s)	**Failure per year (NPRDS/EPIX)**	**Component(s)**	**Failure per year (based on NERC)** "Prior"	"Posterior" (Bayes update)	**EPRI/"prior"**	**EPRI/"posterior"**
Stator Winding (.016) + terminals, bushings (.0032)	1.92E-02	stator windings, bushings, and terminals (code 4520)	1.05E-02	1.71E-04	1.83	112.28
Rotor winding	5.60E-03	(code 4500)	3.66E-03	1.67E-04	1.53	33.53
Rotor forging, fans, RR	4.00E-03	end belts, bolting (code 4580)	3.11E-03	1.65E-04	1.29	24.24
H2 coolers	2.40E-03	(code 4611)	8.26E-03	3.35E-04	0.29	7.16
H2 seals	4.00E-03	(code 4613)	1.13E-02	4.95E-04	0.35	8.08
Bearings	7.20E-03	bearings and lube oil (code 4550)	8.31E-03	3.36E-04	0.87	21.43
Exciter	2.64E-02	motor, rheostat (4601), commutator (4602), "other" (4609)	7.22E-02	1.85E-03	0.37	14.25
Voltage regulator	9.60E-03	voltage control (code 4700)	5.25E-02	6.10E-02	0.18	0.16
Terminals, bushings	3.20E-03	included above, code 4520	-	-		
Brush gear	5.60E-03	(code 4540)	4.16E-03	1.67E-04	1.35	33.53

EPRI SOURCEBOOK			COOPER GRA MODEL			RATIO	
Component(s)		**Failure per year (NPRDS/EPIX)**	**Component(s)**	**Failure per year (based on NERC)** "Prior"	"Posterior" (Bayes update)	**EPRI/"prior"**	**EPRI/"posterior"**
Current and potential transformers		8.00E-03	(code 4730)	6.75E-03	3.33E-04	1.19	24.02
			other contributors		3.00E-03		
TOTALS		**9.52E-02**		**1.81E-01**	**6.80E-02**	**0.53**	**1.40**
Forced Outage Frequency (FOF) = forced outage hours/period hours; period hours = 8760	21.5 hours (EPRI SOURCEBOOK)	2.45E-03	8.955 (100% derate hours)		9.47E-04	-	2.59
USING NERC DATA Forced Outage Rate (FOR) = forced outage hours /(forced outage hours + service hours) (service hours = 7000 in EPRI report)	BWRs only	5.30E-03	(service hours = 6496 for CNS)		1.38E-03	-	3.85
	800 MW BWRs only	7.30E-03			1.38E-03	-	5.30

Instrument Air

Rev. 0 8/1/05

1. System Function

GRA Function: Instrument air provides clean, dry air throughout the plant at pressures required to actuate valves or pneumatically control processes needed to support various plant functions.

2. Success/ Failure Criteria

Plant Disconnected from Grid – 100% Derate

The success criterion of the instrument air function is to ensure that pneumatic motive force is available for plant equipment operation. This criterion is met by providing compressed air to the various air distribution headers at a rate that is adequate to make up for expected air header leakage. Main header pressure is maintained at approximately 100 psig. Failures that result in a pressure drop in the main air header to less than 77 psig will result in a 100% derate condition.

For the purposes of the Generation Risk Assessment (GRA), failure of any component that results in the inability to provide compressed air at a rate that is adequate to make up for expected air header leakage results in a plant trip and a 100% derate condition. This condition results in a loss of instrument air support to key plant equipment. Specifically, loss of instrument air directly results in inability to control reactor feed water flow rates which corresponding results in a plant trip.

Instrument air requires the successful operation of the following support systems:

- AC power
- DC power
- Turbine Equipment Cooling
- Reactor Equipment Cooling
- Service Water

Plant Derate - Derates Less Than 100%

Plant derates less than 100% are not considered in this assessment. This is based on the fact that power reductions are not effective in mitigation of the consequences caused by the loss of the instrument air function. Thus partial derates do not prevent plant trips.

3. Fault Tree Modeling

3.1 Development of Fault Tree

Fault trees were developed using existing instrument air system fault trees contained in the Cooper Nuclear Station (CNS) probabilistic safety assessment (PSA) model.

Instrument air system fault trees contained in the CNS 2005 average test and maintenance PSA model were extracted and converted to generation risk assessment fault trees.

Conversion of PSA fault trees to allow quantification of generation risk was done using PRA2GRA cutset conversion software. Overall, this conversion results in the quantification of the expected number of full power hours lost per year as a result of instrument air system failures. PRA2GRA was utilized to perform the following tasks:

1. Generation of PSA instrument air system cutsets that exclusively contain at least one basic event that would result in a loss of electrical generation. Generally, this involves elimination of all cutsets that contain only demand type failures. PSA instrument air system cutsets that credited use of standby AC power systems were also eliminated since these cutsets are associated with plant trip conditions and not applicable for loss of generation quantification.
2. Conversion of the PSA, instrument air, loss of generation cutsets from 24 hour mission times to 365 day mission times.
3. Identification of cutsets where repair could be credited and assigning repair time to recovery factors for those cutsets. This involved identification of cutsets that had two (2) or more run time failures and multiplying those cutset by a mean time to repair value.
4. Quantification of the expected number of full power hours lost as a result of instrument air failures. This is quantified by multiplying each PSA, instrument air, loss of generation cutsets by the resulting time required to recover from a derated condition (100% derate for instrument air).

Section 5 of this report details the cutset processing steps used to quantify instrument air system cutsets.

3.2 Modeling Assumptions and Comments

1. For the GRA, the exposure time of interest for all components is one year. For the base model, operating times of 24 hours were assigned to the data, which were then updated to a one year exposure time using the PRA2GRA conversion code.
2. It is assumed that any event that results in a full plant derate (100% power) leading to cold shutdown causes the plant to implement the 3 day outage plan. This means that all cold shutdown events have minimum outage times of 72 hours before the plant begins to heat up to return to power. Thus, even if a component has a mean time to repair of less than 72 hours, the plant remains shutdown for 72 hours to complete other repairs.
3. See Section 4 for assumptions specific to data.

4. System Reliability Data

Failure rates (failure per hour) for all components included in the CNS PSA database were used.

PSA failure rates were also reviewed to ensure that failure data for dominant instrument air components reflect current industry/CNS reliability values. Specifically, probabilities for rupture of air dryers and run failures of air compressors were changed to 6.0E-7/hour (Reference, "Other, 6") and 5.0E-5/hour (Reference, "Other, 7") respectively. These values were validated using CNS failure data gathered between the years of March 2000 through March, 2005.

"Mean time to repair" values were extracted from the data provided by the North America Electrical Reliability Council (NERC). Specifically, the NERC "hours per occurrence" were used to represent repair/recovery times. When multiple forced outage categories (i.e., U1, U2, U3) existed for a specific cause code, a weighted average of the hours per occurrence was used to derive a MTTR for the cause code.

It is important to note that NERC (PC-GAR software) defines the hours per occurrence as the amount of time between when the plant becomes desynchronized from the grid (this is the event start time) until the plant is resynchronized to the grid (this is the end time). Thus, the NERC "hours per occurrence" includes not only time to repair the fault, but also may include ramp up time from shutdown power level (e.g., 0%) to the power level at which the plant synchronizes to the grid. Cooper synchronizes to the grid at approximately 20% full power – it is assumed that this value is similar for other plants.

In addition, it must be pointed out that an outage, in the NERC database, is a disconnection from the grid. It is not necessarily a "plant trip" or "plant shutdown" or "plant scram", as may typically be thought of at a nuclear unit when the word "outage" is mentioned. Thus, all plant scrams/trips/shutdowns are NERC outages, but not all NERC outages are plant scrams/trips/shutdowns.

Thus, short "hours per occurrence" are possible in the NERC database because the plant may have disconnected from the grid but may not have proceeded to cold shutdown following a component fault. Following repair of the equipment the plant was quickly brought back up to the power level where synchronization occurred.

To begin the GRA evaluation, each system cause code is reviewed and an assessment is made as to if a plant shutdown to cold shutdown would normally take place in order to repair the component fault. The "hours per occurrence" in the NERC database may provide a clue, i.e., if the hours are short (for example, less than 50) this may indicate that the plant stayed in hot standby during component repair. Conversely, if the hours are long (for example, greater than 100 or so), it may mean that cold shutdown occurred. System engineers and other cognizant analysts should be consulted to determine the appropriate plant response. If the majority of component repairs would require cold shutdown, then it is assumed that ALL would require cold shutdown (and vice versa). This assumption impacts the subsequent treatment of "heat up time" (see next section).

When cold shutdown is assumed for all cause codes, the Cooper-specific heat up time from 0 to 20% (approximately 34 hours) was deleted from the NERC-derived "hours per occurrence" for any value greater than 100. The resulting value was used as the "mean time to repair the equipment". NERC-derived values of less than 100 hours were used as-is.

5. Cutset Post Processing

The following was performed on the CNS PSA instrument air system cutsets to obtain the final system top event frequency.

1. The PRA2GRA code was used to convert mission times from 24 hours to 1 year.
2. Note that the following basic events PSA mission times were changed to 24 hours to allow proper conversion to one year:
   a. TEC_HTX_PG_THX1A (TEC heat exchanger plugging)
   b. EDC-FUS-OP-BPNLB (Supply fuse for DC panel "B")
   c. EDC-FUS-OP-APNLA (Supply fuse for DC panel "A")
   d. EDC-FUS-OP-BB3 (Supply fuse for DC panel "BB3")
   e. EDC-FUS-OP-AA3 (Supply fuse for DC panel "AA3")

3. The PRA2GRA code also assigned "mean time to repair" values, based on assigned values.
4. PRA2GRA was then used to assign consequences, i.e., the number of equivalent lost full power hour hours associated with the component outage. This is calculated as a function of the derate and the amount of time required to restore the plant to 100% power. The time is in turn a function of the "mean time to repair the equipment", plus the "heat up time" (to restore the plant to 20% power, when the plant is synchronized to the grid), plus the time required to go from 20% to 100% power.
5. A code called SetEventStates (developed by AREI – see References) was used to help produce cutsets containing only non-instrument air system basic events. These cutsets were then deleted from the results of the PRA2GRA evaluation, using CAFTA's "Delete Term" tool, to arrive at the final set of cutsets, namely, those containing at least one instrument air system basic event.
6. The result is the amount of "equivalent full time hours" lost as a result of component failures associated with the instrument air system.

6. Results

The yearly frequency for instrument air system unavailability resulting in a 100% derate, as modeled for the GRA, is 8.59e-02. This failure rate is approximately one failure every 11 to 12 years. The rate reflects the low incidence of reported instrument air-specific issues at the Cooper Nuclear Station, and in fact is consistent with the fact that only one Cooper event is recorded in the NERC database over the 16.3 operating-years of Cooper experience represented in the 22 calendar years worth of NERC-GADS data used for the evaluation (an operating-year is equal to a calendar-year x average service hours per calendar-year (hours plant was available and on-line) divided by 8760 hours/calendar year; for the 22 calendar-years included in the NERC-GADS

database for CNS, the average service hours per year was approximately 6490: (22 x 6940/8760 = 16.3)).

When factoring in consequences (in other words, the amount of full power equivalent hours lost as a result of system unavailability), there are a total of 10.78 efph (equivalent full power hours) per year lost, on average, due to instrument air system component failures resulting in 100% derates. If full power is equal to 809 MWe, this means that there are an average of 8721 MWh lost per year due to instrument air system related issues; with a power level of 764 Mwe this is an average of 8236 Mwh per year.

NERC data gathered between the years of 1982 and 2003 details that CNS had one lost generation event resulting from instrument air system failures. This event resulted in a loss of 138 efph. This represents a 6.27 efph per year loss on average and provides a single point comparison to the quantification results of 10.78 efph per year.

It must be noted that failures in support systems, such as turbine equipment cooling (TEC), AC/DC power, etc., increase the frequency of instrument air system unavailability. However, those support systems are or may be treated separately within the GRA, and their impacts should be addressed within the context of those evaluations. The results and discussions here and in subsequent sections focus solely on components explicitly identified as being part of the instrument air system.

6.1 Top Contributors

100% Derate

The top contributor to system unavailability resulting in a 100% derate is run failures of instrument air compressors (NERC cause code 3840, 3850). All cutsets that contain compressor run failure events represent a probability of 5.1e-02 (6.273 efph/yr). This represents a Fussell-Vesely value of 0.47.

Air receiver and dryer ruptures are the next major contributors to instrument air system failures. These rupture events result in a system failure probability of 2.1E-02 (2.58 efph/yr).

All other contributors add much less than 1 hour annually to the total of 10.78 efph/yr loss quantified by this assessment.

6.2 Comparison to Industry

NERC data provided during the years of 1982 to 2003 provides the following results for 100% derates of boiling water reactor (BWR) nuclear generating units:

	Cause	Hours Lost per Unit Year (NERC data)	Hours Lost per Unit Year (CNS GRA quantification)
1	Compressor failures (excluding CNS)	0.073	6.27
2	Other air problems (excluding CNS)	0.5256	4.51
3	All air failures (excluding CNS)	2.06	10.78
4	All air failures (CNS only)	6.27	10.78

For the population of BWRs including CNS, the results are as follows:

Frequency of 100% derate (shutdown) per operation year = 0.032 (compared to CNS-specific value of .0859)

Mwh lost per operating year = 2459 (compared to CNS value of 8236)
EFPH per operating year = 2.76 (compared to CNS value of 10.78)

Conclusions and analysis that can be surmised by this data are as follows:

1. Correlation between GRA quantification and "CNS only", NERC data (Row #4) is more apparent than the correlation between GRA quantification and NERC data that excludes CNS failures (Row #3). This could be indicative of differences in plant design and/or operation.

2. GRA quantification currently predicts greater losses of generation than the historical performance data provided by NERC. Historical judgment concludes that plant trips in the industry have been avoided by the ability of plant operators to take immediate corrective actions for instrument air system failures. Because these actions are not readily quantifiable for GRA modeling, differences (as detailed in the table above) may result when comparing GRA results to historical data.

6.3 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the instrument air fault tree.

The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the system to lost generation given the current reliability of components as assumed in the GRA.

The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur if the reliability of the individual components was allowed to degrade significantly.

In general, air compressor failures (data points 1, 6, 7-9 and 16-18) have higher importance measures. Compressor redundancy results in lower risk increase potential (y-axis). However, because of their importance to the overall function, reliability on the compressor is high (x-axis). Common cause failures of the compressors have the highest risk importance amongst all GRA events.

The ruptures of air receivers and dryers (data points 2-5) have some of the highest importance. This is based on the fact that rupture is a single event that results in system unavailability and 100% plant derate. Preservation of receiver/dryer integrity is critical in ensuring instrument air reliability.

6.4 Uncertainty Analysis

A instrument air uncertainty analysis was performed using @RISK, a software tool provided by Palisades Corporation. Common cause events were correlated with their associated random failure events.

The results of the analysis are shown in Figure 2 and tabulated below.

#Iterations = 10000
Mean lost generation = 10.727 MWh lost per year
Std Deviation = 14.34 Mwh lost per year

Cumulative Probability	*Lost Generation (Mwh)*
5%	2.997
95%	27.04

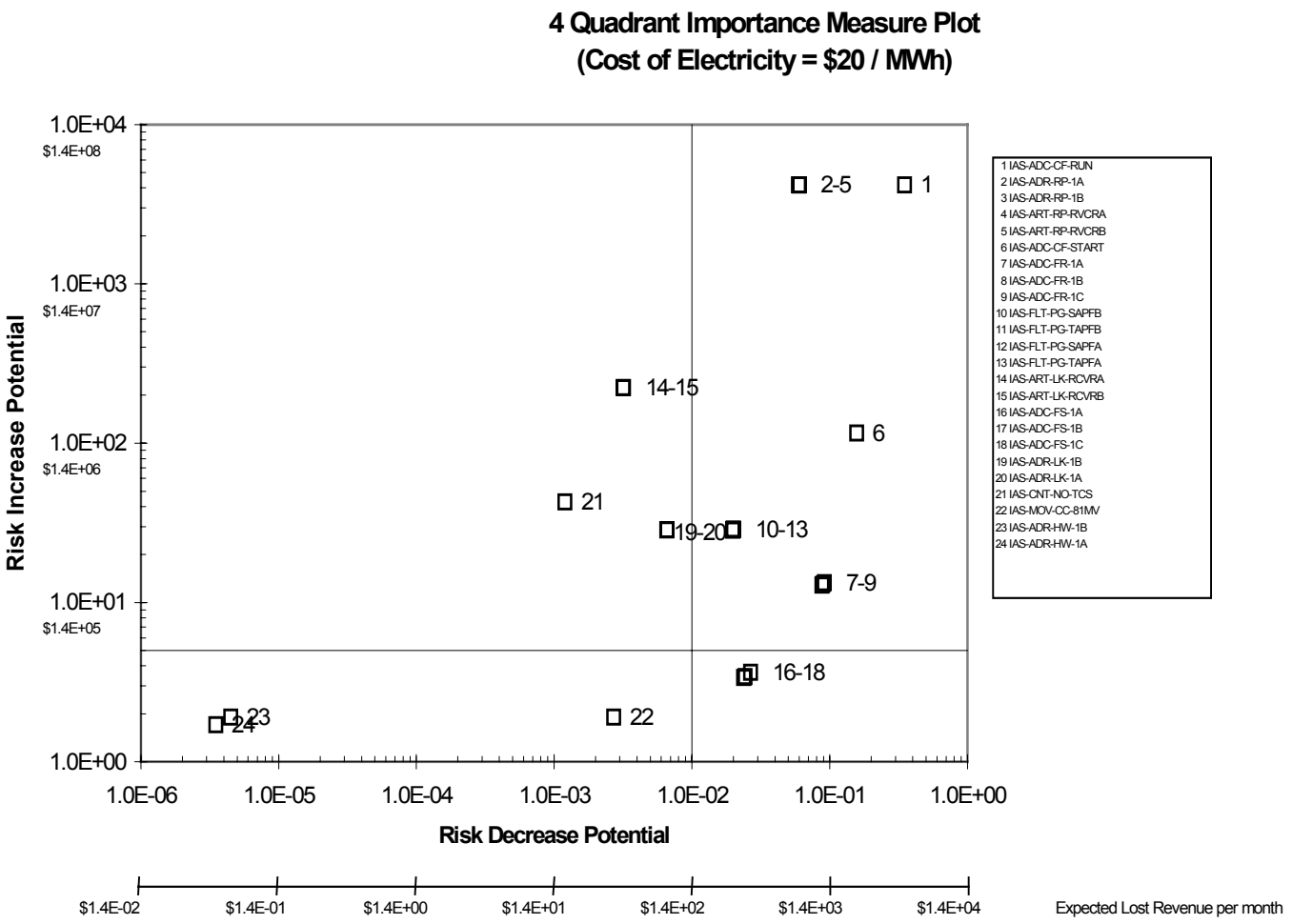


Figure 1
Four Quadrant Plot for Instrument Air System

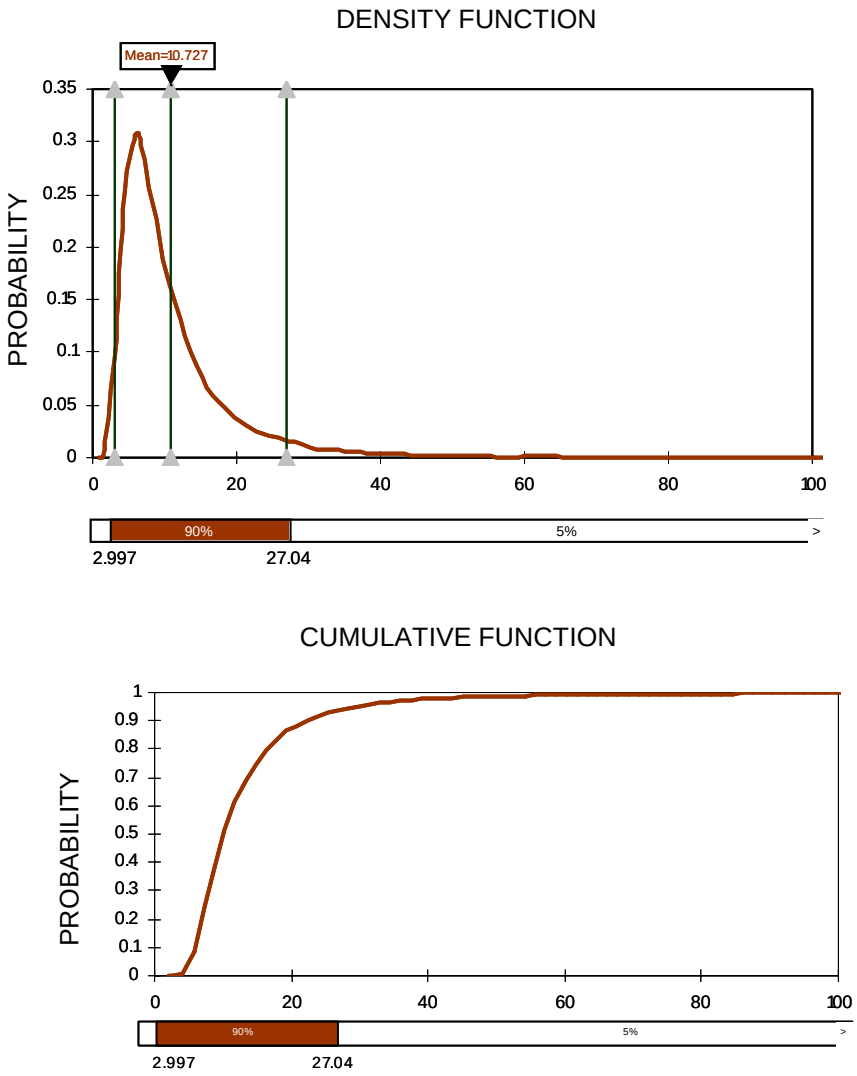


Figure 2
Uncertainty Analysis Results – Instrument Air, 100% Derate

7. References

Cooper Operating Procedures

14. 2.1.10 - Station Power Changes
15. 2.1.4.3 - Power Reduction to Less Than 25%
16. 2.2.59 – Plant Air System
17. 2.2.59a – Plant Air System Component Checklist
18. 5.2.AIR – Loss of Instrument Air

Cooper Operator Training – Lesson Plan

5. COR001701R17-L-OPS Plant Air
6. COR001701R17-S-OPS Plant Air

Fault Trees, Results, and Database

48. GRA_IAS_CUT_041505.cut, Cutsets from Conversion of IAS PSA Fault Trees to Generation Risk Assessment (GRA) Cutsets, Top Event: Plant Trip Probability
49. IAS.caf, CNS PSA, Instrument Air System Fault Tree, Average Test and Maintenance Model, 2005
50. IAS.cut, CNS PSA, Instrument Air System Cutsets, Average Test and Maintenance Model, 2005
51. pra2001a.BE, CNS PSA Model Database, Average Test and Maintenance Model, 2005
52. pra2001a-gra_ias.rr, GRA Model Database, April 2005
53. pra2gra.exe, Executable - Conversion of PSA Fault Trees to GRA Cutsets
54. IAS_GRA_BE_Review.xls, GRA Cutset Review Results
55. SetEventStates.exe, Executable – Basic Event True/False Setting
56. gra_ias_lost gen_no_ias_BEs_Apr_15_2005.cut, IAS GRA Cutsets Containing No Instrument Air Basic Events
57. gra_ias_lost gen_Apr_15_2005.cut, IAS GRA Cutsets Quantifying Loss of Full Power Hours
58. GRA_IAS_CAF_REPORTS.xls, IAS GRA Cutset Reports, Importance Measures and 4 Quadrant Plot

PC-GAR (NERC) Spreadsheets

1. 11-AnnualUnitPerformance All US Nucl no CNS, serv and inst air.xls, Annual Unit Performance of All US Nuclear Generating Units, Excluding CNS, April 19, 2005
2. 11-IndCauseCodeTotals All US Nucl no CNS, serv and inst air.xls, Instrument and Service Air Failures of All US Nuclear Generating Units, Excluding CNS, April 19, 2005
3. 12-AnnualUnitPerformance BWRs no CNS, serv and inst air.xls, Annual Unit Performance of All US Nuclear BWR Generating Units, Excluding CNS, April 19, 2005

4. 12-IndCauseCodeTotals BWRs no CNS, serv and inst air.xls, Instrument and Service Air Failures of All US Nuclear BWR Generating Units, Excluding CNS, April 19, 2005
5. 2-AnnualUnitPerformance COOPER.xls, Annual Unit Performance of CNS, April 19, 2005
6. 2-EventsbyDate COOPER.xls, Plant Derate Events for CNS, April 19, 2005
7. 2-IndCauseCodeTotals COOPER, serv and inst air.xls, Instrument and Service Air Failures for CNS, April 19, 2005

Uncertainty Analysis Spreadsheet

1. GRA_IAS_SENSVTY_041505.xls, Sensitivity Study for Lognormal Failure Distributions of GRA IAS Cutsets, April 15, 2005

Other

1. EPRI, "Life Cycle Management Planning Sourcebook, Volume 2: Instrument Air System" (1006609, December 2001)
2. North American Electric Reliability Council (NERC), "pc-GAR for Windows", release 2.06 v26, 2004
3. Applied Reliability Engineering, Inc., "PRA2GRA", December 16, 2004
4. Electric Power Research Institute (EPRI), "CAFTA", version 5.1a, 2003
5. Applied Reliability Engineering, Inc. (AREI), "SetEventStates.exe", March 2005.
6. IEEE 500-1984, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations (Reaffirmed May 6, 1992)
7. WSRC-TR-93-262, Savannah River Site Generic Data Base Development, June 30, 1993

Main Feedwater/Condensate

Rev. 0 7/29/05

1. System Function

GRA Function: The Condensate and Feedwater system provides a dependable, high quality supply of makeup water to the reactor, at a rate equivalent to the steam generation rate. Condensate/feedwater heaters preheat makeup to the reactor for efficiency purposes

2. Success/ Failure Criteria

The success/failure criteria of feedwater are dictated by the demands for makeup water set by the steam generation rate in the reactor. Various levels of plant derate may occur depending upon the status of the feedwater and condensate pumps and other components of the system. A mismatch between the steam generation rate and the ability of the main feedwater/condensate (MFW/CND) system to provide makeup will lead to power reductions, up to and including a reactor trip.

Normal power operation at 100% requires:

- All three condensate pumps
- All three condensate booster pumps
- Both reactor feed pumps
  (includes one of two lube oil pumps and one of three drain tank pumps)
- Two of two feedwater heater trains or a feedwater heater train and feedwater heater bypass
- The gland seal condenser
- One of two steam jet air ejectors (SJAE)
- Five of seven condensate demineralizers or the condensate demin bypass
- Reactor feedpump turbine speed control

It is assumed that reductions in power can occur due to flow diversion should the minimum flow valves fail open on the discharge of the condensate, condensate booster or reactor feed pumps.

Summary of Failure Criteria

Failure Condition (derate)	Failure Criteria (Equipment Failures)*
Failure to maintain power >0%	o Loss of 2 of 2 FW trains (50% each) [i.e., loss of both FW trains will result in a 100% derate] o Loss of 3 of 3 Condensate trains (33% each) o Loss of 3 of 3 Condensate booster trains (33% each) o Loss of 3 of 3 heater trains and bypass (50% each) o Loss of Either feedwater heater (A-5 or B-5) from the turbine moisture separator o Loss of 1 of 1 gland seal condenser** (100%) o Loss of 2 of 2 air ejectors** (100% each) o Loss of 2 of 2 Augmented Offgas Condenser trains** (100% each) o Loss of Condensate demineralizers and demineralizer bypass (100% each) o Substantial flow diversion -Any condensate pump, condensate booster pump or FW pump minimum flow valve spuriously opening and causing pressure drop to suction of pump - Failure of FW pump discharge check valve with the affected FW pump tripped o MFW/CND reactor level control failures***
Failure to maintain power >33%	o Loss of 2 of 3 condensate trains o Loss of 2 of 3 condensate booster trains
Failure to maintain power >50%	o Loss of 1 of 2 FW trains o Loss of 2 of 3 FW heater paths
Failure to maintain power >67%	o Failure of 1 of 3 condensate trains o Failure of 1 of 3 condensate booster trains
Failure to maintain power >10%	Loss of any 1 of 8 feedwater heaters A1, 2, 3, 4; B1, 2, 3, 4 (loss of a feedwater heater is assumed to result in a minor derate <10% rated power)

*Any single bulleted criterion will produce its associated failure condition.

** While included as a part of the main feedwater/condensate fault tree, the gland seal condenser, SJAEs and augmented offgas condensers are considered to be a part of the main condenser system.
*** Reactor level control is considered to be a part of the primary coolant system

3. Fault Tree Modeling

The MFW/CND system was evaluated for the GRA by using a detailed fault tree model.

3.1 Conversion of PRA Fault Tree

The main feedwater fault tree was extracted from the PRA model (merged.caf 1/21/02 gate TOP-U0). All initiating events were set to False and the configuration events set to True or False. The following modifications to the MFW/CND PRA fault tree were then made to obtain the GRA version of the 100% derate model:

1. Failure of 3 of 3 Feedwater pumps – use existing gate PCS-CMDP-001
2. Failure of 3 of 3 condensate booster pumps – use existing gate PCS-CBP-001
3. Failure of 2 of 2 RF pumps – use existing gates PCS-RFPB-004 & PCS-RFPB-004, adding a single normally open motor operated (MO) valve to both pumps from the turbine moisture separator
4. 3 of 3 feedwater heater trains and bypass - Added logic (gate PCS-GRA-001) representing leakage/plugging of appropriate combinations of heaters A-1 through A-4 & B-1 through B-4 and of MO-17 & MO-18.
5. Either 1 of 2 feedwater heaters connected to turbine moisture separator drain - Added logic (gate PCS-GRA-001) representing leakage/plugging of either heater A-5 or B-5
6. Both feedwater pumps receive steam from turbine moisture separator – Added event (PCS-MOV-OC-MSTSE) representing single MOV from moisture separator to both RF pumps
7. 1 of 1 gland seal condenser - Added logic (PCS-HTX-PG-GSCOND) representing leakage/plugging of gland seal condenser
8. 2 of 2 SJAEs - Added logic (gate PCS-GRA-020) representing plugging/degradation of SJAE 1-A and 1-B
9. 2 of 2 Augmented Offgas condensers - Added logic (gate PCS-GRA-024) representing loss of function of AOGs and AOG condenser booster pumps
10. All condensate demineralizers or condensate demineralizer bypass – Added logic (gate PCS-GRA-030) representing flow path through condensate demineralizers and AO-B1 (it is assumed that if several demineralizers plug that all of them will be subject to similar plugging).
11. Flow diversion - Add logic (gate PCS-GRA-040) for failing to remain closed:
    a. Condensate pumps - FCV-17 (min flow to CSTs); AO-9A&B (cond pressure control); 2 dump valves to CSTs
    b. Condensate booster pumps - FCV-8, 10 & 12 (min flow to CSTs)

c. Feedwater pumps – air operated ((AO) valve on discharge of each pump (min flow to main condenser). Also added as a means of flow diversion of opposite pump when discharge check valve on affected pump fails to close.

12. Dependencies between condensate booster pumps - Added condensate booster aux oil pumps and power dependencies (PCS-GRA-050, PCS-GRA-052, PCS-GRA-054).
13. Dependencies of RFP on RFP drain tank pumps - RFP drain tank pump logic and power dependencies added (gate PCS-GRA-060)
14. FW control dependencies - Added logic "OR-ing" RFP trains with feedwater level control and RFP discharge valve isolation (gates PCS-GRA-071 & PCS-GRA-072). Deleted startup valve logic PCS-RFW-002

Other derates (failure to maintain power >33%, >50%, >67%, and >90%) were added by creating top gates reflecting the failure criteria defined in Section 2.0.

3.2 Modeling Assumption and Comments

The baseline exposure time for all running components in the fault tree model is 24 hours. However, this exposure time is subsequently changed to a one year (8760 hour) mission time through the use of a computer code (PRA2GRA – see References) that converts PRA cutsets into GRA cutsets.

4. System Reliability Data

The database of failure rates employed for the PRA quantification was used initially to provide the rates utilized in the MFW/CND GRA model. However, subsequent to the initial quantification of the GRA models and a review of the results it was concluded that the PRA failure data for the reactor feed pumps may be overly optimistic based on plant specific and industry experience. Thus, the North American Electric Reliability Council (NERC) database was used as a source for the development of failure rates (failure per hour) for the reactor feedwater pumps.

<u>Feedwater pump fail to run</u>

Investigating the source of the data for the feedwater pumps in the Cooper PRA reveals that the feedwater pump fail to run probability is a fixed value (4E-4) not dependent on a 24 hour mission time. On the surface, the probability appears to be low for a turbine driven pump. The PRA2GRA code assumes this is a mission time event with a 24 hour mission time.

Examining the HPCI pumps in the Cooper PRA database yields a turbine driven pump FTR rate of 5E-3/hr, similar to NUREG/CR-4550. Assuming this value for a feedwater pump would yield a loss of a single feedwater pump on the order of 50 times per year, unrealistically high for a train of equipment needed to keep the plant at full power.

A review of NERC data was undertaken to derive a failure rate for use in the Cooper GRA as an alternative to Cooper or generic PRA data. To screen out those plants that have motor driven pumps, only BWRs with turbine feedwater systems were selected. This results in 21 units with 390 unit years of reports. The mean operating hours per year for these 21 units is 6048 hrs.

A report for all individual cause codes for the feedwater system was generated from pc-GAR. It was assumed that all derates (D1-D4) and forced outages (U1-U3) associated with cause codes 3408-3419 (with the exception of 3415) could be assigned to the feedwater pumps.

When employed, failure rates from NERC data were developed by dividing the number of "forced outages" by "service hours", for each specific cause code.

1. MFW/CND data within pc-GAR was filtered to include as closely as possible industry-wide data only for US nuclear units having pump designs similar to those of the Cooper (e.g., turbine driven).
2. "Forced outages" included any event classified as U1, U2, or U3 within pc-GAR and derates included any event classified as D1, D2, D3 or D4 for each specific cause code.
3. "Service hours" were calculated by taking the average annual service hour value, provided by pc-GAR for the set of plants specified, and multiplying by the total number of "unit-years" given by PC-GAR for that set of plants.

A total of 33 forced outages and 467 derates were identified for the 390 BWR unit years reported by NERC. The plants in the report averaged 6048 service hours per year during the period 1982 through 2001. This resulted in an average 2 feed pump failures per unit operating year. Assuming two feedwater pumps per unit results in a generic hourly failure rate of roughly 1E-4/hr.

NERC data was also investigated for the Cooper plant specifically. Cooper has experienced 5 feedwater pump failures in 22 years of operation (16 operating years - an operating-year is equal to a calendar-year x average service hours (hours plant was available and on-line) divided by 8760 hours/calendar year; for the 22 calendar-years included in the NERC-GADS database for CNS, the average service hours per year was approximately 6490: (22 x 6940/8760 = 16.3)). Performing a Bayesian update of generic information with this plant specific data yields an hourly pump fail to run failure rate of 2.3E-5/hr (see CNS FW Pump NERC Bayes-gamma January 2005.xls).

5. Cutset Post Processing

The following was performed on the MFW/CND system cutsets to obtain the final system top event frequencies:

1. As the definition of each top event is failure to maintain power above a specific power level, the cut sets for each level of derate may contain combinations of failures that lead to that specific power level or lower. To assure that there are not

duplicate cut sets in multiple derate bins, the cut sets for each level of derate were deleted from all higher power levels. That is:

Cut sets for failure to maintain >0% power were deleted from >33%, >50%, >67% & >90%

Cut sets for failure to maintain >33% power deleted from >50%, >67% & >90%

Cut sets for failure to maintain >50% power were deleted from >67% & >90%

Cut sets for failure to maintain >67% power were deleted from >90%.

2. Cut sets for the five levels of derate were processed through PRA2GRA to
   Increase mission time to one year.
   Calculate the consequences of each combination of failures

3. Cut sets having no events associated with the main feedwater/condensate system were deleted leaving only combinations of failure to which feedwater/condensate component failures contributed. (Note: Initially all basic events beginning with a system code PCS were included in the final results. Following comparison with NERC, PCS events associated with the gland seal condenser, the SJAEs, the augmented offgas condenser and reactor level control were eliminated from the analysis as they are considered to be part of other systems).

6. Results

Main feedwater/condensate components only

	Frequency of Load Reduction (per operating year)		Lost Generation (EFPH/operating year)	
Magnitude	NERC (BWRs 1982-2003)	GRA	NERC (BWRs 1982-2003)	GRA
100% (Shutdown)	0.34	0.24	25.9	30.4
Derate				
67%		0.016		0.59
50%		0.42		10.1
33%		2.4		36.3
10%		0.40		1.2
Total	4.8	3.2	28.5	48.2

It can be seen from the preceding table that the overall frequencies of trips and derates for the main feedwater/condensate system agree relatively well with NERC industry averages and the

Cooper GRA model. From a total lost generation perspective, the GRA estimates for shutdown are very close and for derates are within a factor of 2.
The following discusses the contributors to trips and derates from the GRA model and compares these results to NERC industry cause codes.

6.1 Top Contributors

Each feedwater/condensate basic event in the GRA (those beginning with the system designator PCS) was assigned a NERC cause code. Importance measures were then generated for each basic event (Birnbaum's measure x probability of failure was used to estimate a frequency and total lost effective full power hours for each basic event) and aggregated for each cause code.

The following compares the frequency for each cause code from NERC and the GRA:

Plant Shutdown (100% load reduction)

Cause code	Desc	NERC sd/ operating yr	GRA sd/ operating yr	GRA/NERC %	Cooper-NERC sd/ unit yr
3408-3419	Feedwater Pump	0.111	0.036	32.9%	0.22
3431	Other Feedwater Valves	0.052	0.005	10.2%	0.046
3499	Other Feedwater System Problems	0.042		0.0%	
3310-3311	Condensate/hotwell Pumps	0.020	0.013	67.4%	
3320	Condensate Piping	0.016		0.0%	
3330	Condensate Valves	0.013	0.036	274.4%	
3350	Condensate Polishing And Filtering Systems	0.013	0.002	17.6%	
3439-3441	Other High Pressure Heater Problems	0.013	0.100	768.0%	0.046
3312-3313	Condensate Booster Pump	0.013	0.026	202.3%	
3339-3341	Low Pressure Heater - Other	0.010		0.0%	
3415	Feedwater Pump/drive Lube Oil System	0.016	0.026	161.5%	
3420	Feedwater Piping	0.010		0.0%	
3430	Feedwater Regulating (boiler Level Control) Valve	0.010		0.0%	
3399	Other Miscellaneous Condensate System Problems	0.003		0.0%	
	Total	0.342	0.246	71.8%	0.311

* excluding cause code 3415

Derate (All load reductions < full shutdown)

Cause Code	Desc	NERC derate/ operating yr	GRA derate/ operating yr	GRA/NERC %
3408-3419	Feedwater Pump	1.60	0.42	25.91%
3439-3441	Other High Pressure Heater Problems	0.60	0.40	66.78%
3339-3341	Low Pressure Heater Head Leaks	0.52	0.00	0.00%
3310-3311	Condensate/hotwell Pumps	0.44	1.31	298.95%
3499	Other Feedwater System Problems	0.33	0.00	0.00%
3350-3352	Condensate Polishing And Filtering Systems	0.43	0.00	0.00%
3342	Intermediate Pressure Heater Tube Leaks	0.17	0.00	0.00%
3312-3313	Condensate Booster Pump	0.19	1.07	567.66%
3431	Other Feedwater Valves	0.08	0.01	14.08%
3415	Feedwater Pump/drive Lube Oil System	0.11	0.00	1.68%
3399	Other Misc Condensate Problems	0.05	0.00	0.00%
3430	Feedwater Regulating (boiler Level Control) Valve	0.05	0.00	0.00%
3420	Feedwater Piping	0.03	0.00	0.00%
3320	Condensate Piping	0.02	0.00	0.00%
3330	Condensate Valves	0.04	0.00	0.00%
3370	Condensate System I&C	0.02	0.00	0.00%
3344	Deareator	0.00	0.00	0.00%
3360	Condensate Makeup & Return (incl CST)	0.00	0.00	0.00%
		4.70	3.22	68.49%

*excluding cause code 3415

There is reasonably good agreement between the GRA results and industry NERC data for the frequency of trips (within 30%) and derates (roughly a factor of 2 difference) associated with main feedwater/condensate components. From the preceding tables, it is seen that

- The results for motor driven pumps (condensate, condensate booster) are very similar.
- Feedwater/condensate valves are in reasonable agreement if the valves from the two systems are combined (0.64 shutdowns/yr for NERC as compared to 0.41/yr from the GRA).
- Contributions to trips from the feedwater lube oil system are also reasonably close for plant trips (although plant derates show little contribution from this part of the system in the GRA as compared to NERC).

The major differences between NERC and GRA are for

- Feedwater pumps (derived from Cooper NERC reports, the Cooper feedwater pumps appear to have a significantly lower failure rate than industry average).
- Feedwater/condensate piping (the GRA does not model passive piping failures).
- Feedwater regulating valves (Cooper feedwater flow control is performed with turbine speed and does not have regulating valves other than for startup).
- "Other feedwater system problems" (which are explicitly modeled among specific components in the GRA).

The GRA also underestimates feedwater heater contributions and condensate demineralizer contributions to derates as compared to NERC.

The following compares total lost generation for the feedwater/condensate system in terms of lost effective full power hours between industry NERC data and the Cooper GRA.

Plant Shutdown (100% Load Reduction)

Cause code	Desc	NERC EFPH/ operating yr	GRA EFPH/ operating year	GRA/NERC %
3408-3419	Feedwater Pump	7.902	4.550	57.6%
3431	Other Feedwater Valves	5.330	0.741	13.9%
3499	Other Feedwater System Problems	3.332		0.0%
3312-3313	Condensate Booster Pump	0.586	3.242	553.6%
3310-3311	Condensate/hotwell Pumps	1.377	1.619	117.6%
3320	Condensate Piping	1.915		0.0%
3330	Condensate Valves	0.486	4.536	932.8%
3350-3352	Condensate Polishing And Filtering Systems	1.131	0.617	54.5%
3439-3441	Other High Pressure Heater Problems	1.003	12.303	1226.2%
3399	Other Miscellaneous Condensate System Problems	0.154		0.0%
3415	Feedwater Pump/drive Lube Oil System	1.266	3.234	255.5%
3420	Feedwater Piping	0.575		0.0%
3430	Feedwater Regulating (boiler Level Control) Valve	0.280		0.0%
3339-3341	Low Pressure Heater - Other	0.598		0.0%
		25.9	30.8	118.9%

*excluding cause code 3415

Derates (All load reductions < full shutdown)

Cause Code		NERC EFPH/ operating year	GRA EFPH/ operating year	GRA/NERC %
3408-3419	Feedwater Pump	11.26	9.56	85%
3339-3341	Low Pressure Heater Head Leaks	6.69	0.00	0%
3350-3352	Condensate Polishing And Filtering Systems	1.99	0.00	0%
3439-3441	Other High Pressure Heater Problems	2.03	1.39	68%
3310-3311	Condensate/hotwell Pumps	2.13	20.47	959%
3499	Other Feedwater System Problems	1.31	0.00	0%
3431	Other Feedwater Valves	0.62	0.46	73%
3415	Feedwater Pump/drive Lube Oil System	0.58	0.07	11%
3342	Intermediate Pressure Heater Tube Leaks	0.47	0.00	0%
3330	Condensate Valves	0.38	0.00	0%
3312-3313	Condensate Booster Pump	0.37	16.85	4544%
3420	Feedwater Piping	0.21	0.00	0%
3399	Other Misc Condensate Problems	0.17	0.00	0%
3430	Feedwater Regulating (boiler Level Control) Valve	0.10	0.00	0%
3320	Condensate Piping	0.08	0.00	0%
3370	Condensate System I&C	0.05	0.00	0%
3344	Deareator	0.02	0.00	0%
3360	Condensate Makeup & Return (incl CST)	0.00	0.00	0%
		28.5	48.8	171%

*excluding cause code 3415

The GRA estimates for total lost generation are mixed between being higher or lower for most cause codes as compared to NERC. The most significant differences between the GRA and NERC are for the condensate and condensate booster pumps, condensate valves and high pressure heater problems.

It is noted that the GRA currently approximates the total down time by adding the MTTR for all components in a cut set leading to trips or derates, which may be conservative (i.e., multiple repair activities may occur in parallel during a plant shutdown). Also, most MTTR are estimated from generic data sources (e.g., pump MTTR = 19h, valve MTTR = 7h, electrical equipment MTTR = 6h). When no estimates are provided, a default MTTR of 168h is assumed. It may be that actual MTTRs for the condensate and condensate booster pumps may be better than generic estimates.

That the high pressure heaters contribute significantly more than NERC experience is due to the assumption that leakage or plugging of heaters A5 and B5 require a plant shutdown to repair. As they are connected to the turbine moisture separator drains, they cannot be isolated during plant operation.

6.2 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the feedwater/condensate system fault tree.

> The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the main feedwater/condensate system to lost generation given the current reliability of feedwater/condensate components as assumed in the GRA.
>
> The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur were the reliability of the individual components to be allowed to degrade significantly.

The importance of components in the main feedwater/condensate system are grouped in layers along the risk increase potential axis. The top layer represents those component failures that lead to a plant shutdown. Layers are found that represent derates to 67% and 50% power.

The most important components to current lost generation are those found in the upper right of the plot.

> For the most part, main feedwater/condensate components that dominate in both risk decrease and risk increase potential are the major rotating equipment (turbine feedwater pumps, condensate pumps and condensate booster pumps). It should be noted that the most significant contributors to lost generation from the pumps are at the 67% and 50% derated levels. Individual pump failures can lead to these partial load reductions whereas full plant shutdown generally requires multiple failures to occur, making a plant shutdown lower in frequency than partial derates. Data points 3-13, representing failure of individual pumps (feedwater, condensate, condensate booster, lube oil, etc), contribute to lost generation roughly 7.5 EPFH/yr (5,700 MWh/yr) [which translates to a monthly lost revenue on the order of $9,500/mo at $20/MWh].
>
> One non-pump related component type dominates the potential for full plant shutdown. The GRA suggests that feedwater heaters A-5 and B-5 each contribute to the loss of approximately 11 EFPH/yr (8,300 MWh/yr) [or $14,000/mo lost revenue]. Per, COR002-02-02 (Condensate and Feedwater Training Lesson Plan), these two heat exchangers cannot be removed from service while the turbine moisture separators are in operation. As a result the GRA assumes that plugging or leakage of either of these heat exchangers will lead to a plant shutdown. The GRA assumes heat exchanger plugging to occur at a rate of 5.7E-6/hr which results in the potential for one of these heat exchangers needing to be removed from service once every 10 years.

Components located in the upper left of the plot do not currently contribute significantly to lost generation, but could if their reliability were allowed to degrade significantly. Most of the components in the upper left of the plot represent passive failures of individual components required for power operation.

The upper row is made up of valves that, if they fail to remain in position, could lead to a full plant shutdown:

Minimum flow AOVs in the feedwater condensate system that are assumed to cause sufficient flow diversion to shut down the plant (e.g., FCV-17, FCV-11A, AO-8, AO-9A, AO-9B, etc.)

Steam supply MOV from the moisture separator to the feedwater pump turbines

Components that by themselves lead to a partial load reduction;

MOVs in the flow path to the reactor (e.g., MO-29, MO-30, etc.)

Hydraulically operated steam supply valves to the feedwater pump turbines

Individual feedwater heaters

Plugging of the condensate demineralizers also can lead to load reductions in combination with failure of the demineralizer bypass valve.

The remaining components are located in the lower left of the four quadrant plot. These components (and those truncated from the analysis) may be candidates for corrective maintenance programs provided they can be shown not to contribute significantly to lost generation in combination.

Condensate demineralizer bypass valve fails to open

Feedwater heater bypass valves fail closed

Reactor feedwater pump drain tank pumps

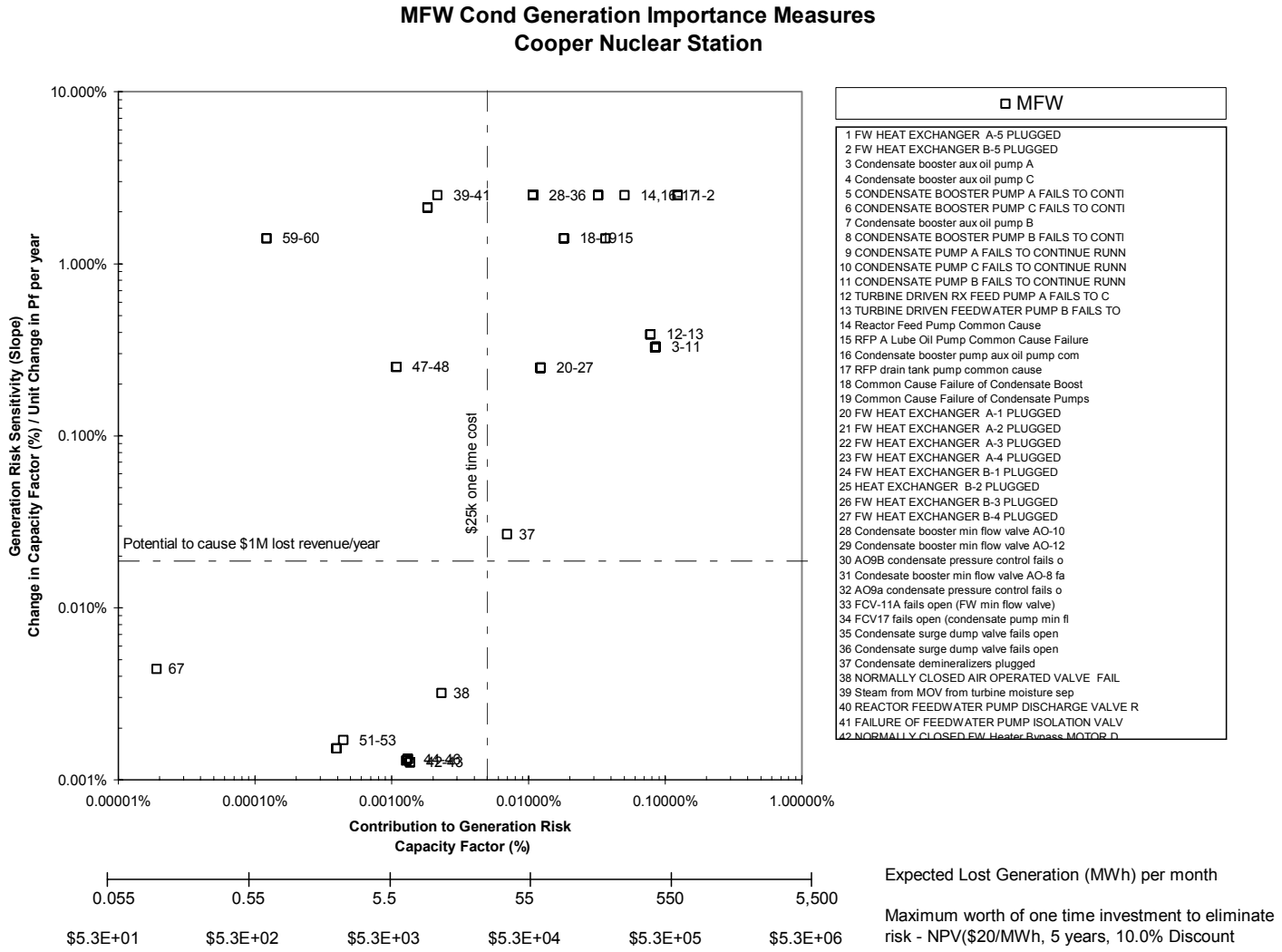


Figure 1
Four Quadrant Plot for MFW/CND System

6.3 Uncertainty Analysis

A main feedwater/Condensate System uncertainty analysis was performed using @Risk. With the exception of motor driven pumps, 100% correlation was assumed between all components having the same component type and failure mode (e.g., AOV CC, normally closed air operated valve fails closed, or FTO). Common cause events were correlated with their associated random failure events. The motor driven pumps in the main feedwater/condensate system were 100% correlated in the following groups:

Turbine driven feedwater pumps
Feedwater pump lube oil pumps
Feedwater pump drain tank pumps
Condensate pumps and condensate booster pumps
Condensate pump aux oil pumps

The results of the analysis are as follows:

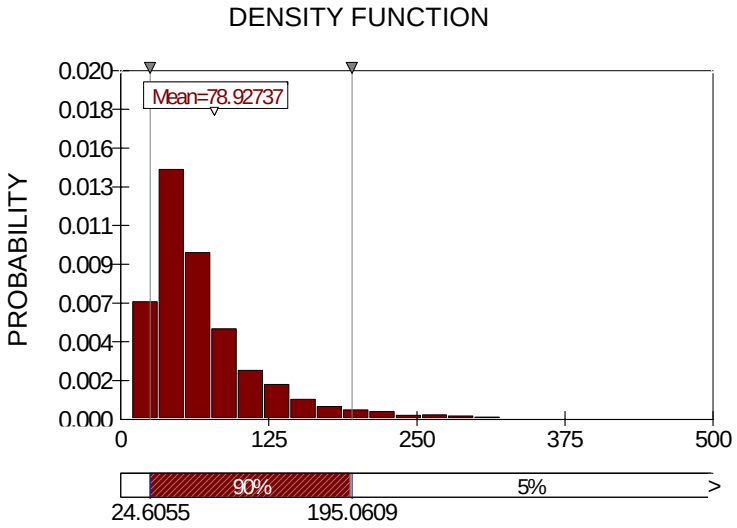
#Iterations = 10000
Mean lost generation = 78.9 EFPH/operating yr
Std Deviation = 100.0 EFPH/operating yr

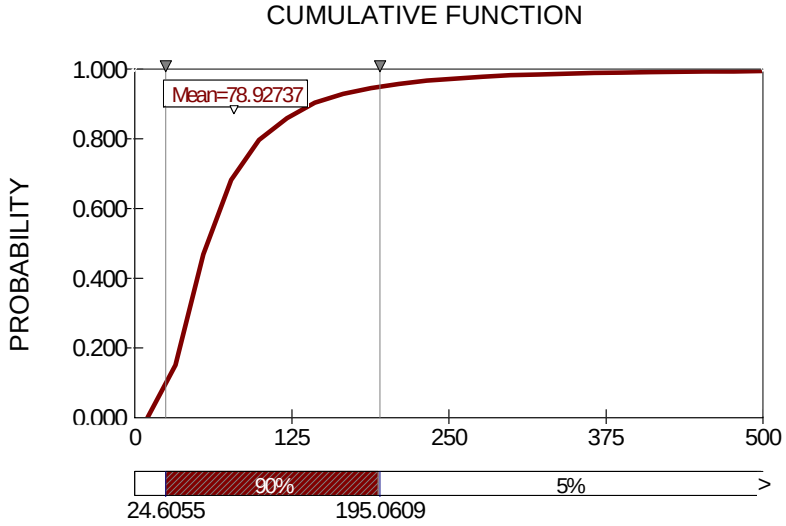
Cumulative Probability	Lost Generation (EFPH/yr)
5%	24.6
10%	28.7
15%	32.2
20%	35.5
25%	38.6
30%	42.2
35%	45.6
40%	49.1
45%	53.0
50%	56.7
55%	61.3
60%	66.4
65%	72.2
70%	79.6
75%	88.2
80%	99.8
85%	116.2
90%	141.3
95%	195.1

From the preceding table, there is a 10% chance of losing 140EFPH/yr or greater. Drilling down into the upper tail of the curve, dominant contributors to this 10% are:

Condensate Booster Pumps (individual pump fail to run and common cause fail to run)
Condensate Pumps (individual pump fail to run and common cause fail to run)

Discrete and cumulative probability distributions for Total lost EFPH/yr for the Feedwater/Condensate system:





7. References

Cooper Operator Training – Lesson Plan

1. COR002-02-02 OPS Condensate and Feed, Revision 16

Drawings

1. COR002-02-02 Figure 1, Simplified Diagram of Condensate and Feed System

Fault Trees, Database and Results

1. mfw-gra-mxfr-alltops.caf 1/10/2005 02:26 PM
2. pra2001a-gra24.rr 3/18/2005 05:45 PM
3. cut files
    a. u0-all-pcs-con-xpcs2.cut 3/19/2005 04:01 PM
    (all MFW consequence cut sets)
    b. u0-00-pcs.cut 03/16/2005 06:21 PM
    (MFW plant trip frequency & consequence cut sets)
    c. u0-33-pcs.cut 03/16/2005 06:27 PM
    (MFW 33% power frequency & consequence cut sets)
    d. u0-50-pcs.cut 03/16/2005 06:28 PM
    (MFW 50% power frequency & consequence cut sets)
    e. u0-67-pcs.cut 03/16/2005 06:29 PM
    (MFW 67% power frequency & consequence cut sets)
    f. u0-90-pcs.cut 03/16/2005 06:30 PM
    (MFW 90% power frequency & consequence cut sets)
4. Importance measures
    g. MFW GRA NERC Comparison.xls 03/16/2005 08:00 PM
    (frequency and consequence comparison)
    h. MFW 4qp 050319.xls 03/20/2005 08:28 AM
    (consequences only)
5. Uncertainty analysis
    i. MFW uncert 050318.xls 03/20/2005 07:04 PM
    (consequences only)

PC-GAR (NERC) Spreadsheets

1. NERC MFW 040107.xls 1/11/2005 11:10 AM
(BWRs 1982-2001, Steam driven feedwater pumps, MFW/Cond cause codes)
2. CNS FW Pump NERC bayes-gamma January 2005.xls 03/18/2005 06:36 PM
(Bayesian analysis of main feedwater pump fail to run)
3. NERC results supporting Bayesian update (main feedwater pump fail to run)
    a. 1-CompCauseCodeLosses 1982.xls 03/15/2005 05:10 PM
    b. 1-CompCauseCodeLosses 1983.xls 03/15/2005 05:16 PM
    c. 1-CompCauseCodeLosses 1984.xls 03/15/2005 05:18 PM

d. 1-CompCauseCodeLosses 1985.xls 03/15/2005 05:21 PM
e. 1-CompCauseCodeLosses 1986.xls 03/15/2005 06:19 PM
f. 1-CompCauseCodeLosses 1987.xls 03/15/2005 06:21 PM
g. 1-CompCauseCodeLosses 1988.xls 03/15/2005 06:24 PM
h. 1-CompCauseCodeLosses 1989.xls 03/15/2005 06:26 PM
i. 1-CompCauseCodeLosses 1990.xls 03/15/2005 06:27 PM
j. 1-CompCauseCodeLosses 1991.xls 03/15/2005 06:29 PM
k. 1-CompCauseCodeLosses 1992.xls 03/15/2005 06:31 PM
l. 1-CompCauseCodeLosses 1993.xls 03/15/2005 06:32 PM
m. 1-CompCauseCodeLosses 1994.xls 03/15/2005 06:34 PM
n. 1-CompCauseCodeLosses 1995.xls 03/15/2005 06:35 PM
o. 1-CompCauseCodeLosses 1996.xls 03/15/2005 06:38 PM
p. 1-CompCauseCodeLosses 1997.xls 03/15/2005 06:39 PM
q. 1-CompCauseCodeLosses 1998.xls 03/15/2005 06:41 PM
r. 1-CompCauseCodeLosses 1999.xls 03/15/2005 06:43 PM
s. 1-CompCauseCodeLosses 2000.xls 03/15/2005 06:45 PM
t. 1-CompCauseCodeLosses 2001.xls 03/15/2005 06:46 PM

4. 2-IndCauseCodeTotals COOPER ONLY MFW_COND.xls 12/23/2004 10:43 PM (Cooper specific cause codes for Feedwater/Condensate 1982-2003)

Other

1. North American Electric Reliability Council (NERC), “pc-GAR for Windows”, release 2.06 v26, 2004
2. Applied Reliability Engineering, Inc., “PRA2GRA”, December 16, 2004
3. Electric Power Research Institute (EPRI), “CAFTA”, version 5.1a, 2003

Service Water System

Rev. 09/30/05

1.0 System Function

GRA Function: The Service Water (SW) system provides cooling to balance of plant systems through the Reactor and Turbine Equipment Cooling Systems (REC and TEC) during normal power operation:

Normal Operating REC Loads:

- RWCU
- IA compressor
- CRD pumps
- DW Coolers

Normal Operating TEC Loads:

- Main Generator Hydrogen Coolers
- Main Lube Oil Coolers
- Exciter Air Coolers
- Bus Duct Heat Exchangers
- Circulating water pumps
- Condensate/Feedwater Pumps

2.0 Success/ Failure Criteria

Plant Shutdown – 100% Derate

The success/failure criteria of service water is dictated by the biggest normal operating heat loads; main generator hydrogen coolers, main lube oil coolers, exciter air coolers and bus duct heat exchangers. Cooling of these components is supplied by the turbine building equipment cooling system which in turn is supplied by the service water system. The service water system success criterion is dictated by the TEC heat exchanger outlet temperature of 95^{o} F. When this temperature is exceeded, the operators are instructed to trip the reactor to avoid failure of the equipment supplied by TEC. Historical operation has shown that the TEC heat exchanger outlet temperature limit is reached before the REC heat exchanger temperature limits when service water becomes unavailable.

From system experience, three pumps are necessary to meet the TEC heat loads in the hot summer months (1/3 of the year) and two for the rest of the year to maintain TEC outlet temperature below 95 deg. F. During the hottest summer period, typically lasting for 14 days, four pumps are necessary to meet this temperature limitation. One TEC heat exchanger (of the 2

at the plant) is capable of removing the entire TEC heat load so, during plant operation, only one is normally in service. The idle TEC heat exchanger can be placed in service in situations where flow to the operating heat exchanger fails.

Loss of service water to both REC heat exchangers (there are 2 total) would also require shutdown of the plant per Emergency Procedure 5.2. Loss of service water to a REC heat exchanger does not require shutdown of the reactor since one REC heat exchanger is adequate to remove heat from operating REC loads.

Plant Derate : < 100% Derate

None.

Success/Failure Criteria Summary

Plant Derate	Limiting Condition	Equipment Success Criteria
Manual Shutdown (100% plant derate)	*TEC Hx outlet temperature*	2 of 4 pumps – Non Summer Months 3 of 4 pumps – Summer Months 4 of 4 pumps – hottest Summer period (average 14 days per year) 1 of 2 TEC heat exchangers – Non Summer Months 2 of 2 TEC heat exchangers – hottest Summer (see TEC system evaluation)
	SW to both REC Hx	Same as SW to TEC*
< 100% Plant Derate		None

* service water pump criterion is dictated by TEC outlet temperature as discussed in the above text.

3.0 Fault Tree Modeling

3.1 Conversion of PRA Fault Tree

The following modifications were made to the PSA service water fault tree to obtain the GRA fault tree:

1. Fault tree gate “SWS-NC-000” in the Cooper PSA merged fault tree model “merged.caf” was extracted to a separate fault tree with top event “SWS-NC-000”. The SWS-NC-000 logic is the starting point for converting the SW PSA to GRA model. This gate is input to the new top fault tree logic developed for the GRA model (100% derate). The new top gate is “SWS-NC-LOAD”.

2. All initiating events, basic events beginning with the designator "%" were set to ***False*** to eliminate them from the "SWS-NC-000" fault tree. These events were used in the PRA model as house events for the purpose of accident sequence quantification and are not applicable to the GRA analysis.
3. A new fault tree top logic was generated (top event "SWS-NC-LOAD") to model the three failure pump success/failure criteria defined for the Summer, Summer hottest period and Winter months described in Section 2.0. Corresponding basic events, SUMMER, SUMMER-H and WINTER represent the fraction of the year the service water system is in these configurations. The service water top gate (SWS-NC-000) extracted from the PSA (see note #1) is directly input under the gate representing the Winter condition (gate "SWS-NC-W) with the following modifications:

   - Pump configuration house events were modified to represent the default configuration.
   - Service water pump A configuration: Gates SWS-FLG-LF-AOFA, SWS-FLG-LF-AOPS and SWS-FLG-LF-AOFS were set to False.
   - SW pump B configuration: Gates SWS-FLG-LF-BOFA SWS-FLG-LF-BOPS and SWS-FLG-LF-BOFS, were set to False.
   - SW pump C configuration: Gates SWS-FLG-LF-COFA, SWS-FLG-LF-COFS and SWS-FLG-LF-COFS were set to False
   - SW pump D configuration; Gates SWS-FLG-LF-DOPA, SWS-FLG-LF-DOFA and SWS-FLG-LF-DOPS were set to False.
   - Gate "LOSP" is set to False to remove pump start logic after restoration of power following a loss of offsite power event. Pump re-starting in this condition is not credited as a failure in the GRA model because the plant has already tripped as a result of the loss of offsite power (LOSP) event. Corresponding events for failure to start an idle pump that is placed in auto after a LOSP event were also removed by setting basic event SWS-XHE-FS-SWPS to False.
   - The basic event "EAC-TRN-LP-SU" under gate SWS-NC-000", representing failure of the plant startup transformer, was removed. Dependency of the emergency diesel generators on the startup transformer for its cooling support was also removed.
   - The event representing common cause failures of different combinations of 3 pumps, "SWS-MDP-CF-3MDPS", was moved one level higher in the logic to the level of its parent gates because the pump independent failure logic is used in the Summer, Winter and Summer Hot conditions where the success criteria are different. This is to eliminate the generation of non-minimal cut sets associated with common cause pump failures.
   - The event representing common cause failures of different combinations of 2 pumps, "SWS-MDP-CF-2MDPS", was added under gate "SWS-NC-100" for the Summer conditions. This is the minimum number of pumps failures resulting in manual shutdown. Gate SWS-NC-100 is a new gate included in the GRA tree.

4. New logic was added to represent plant shutdown due to closure of MV36 and MV37, the critical loads loop isolation valves. Per Assumption 3.2.7 below, failure of an operating pump may result in pressure drop that is significant enough to cause closure of these valves, thereby isolating flow to the TEC heat exchangers (per plant staff). The operator must reopen the valves to restore flow to the heat exchangers to avoid plant shutdown. The logic is represented under gate SWS-TEC-HX. Only logic associated with pump operating status is included under its child gates. Operator failure to reopen either isolation valve is modeled by basic event "SWS-XHE-FO-M367".

5. Logic associated with pump start after loss of offsite power and subsequent power restoration to the pump buses was eliminated. The logic was AND-ed with gate "LOSP" representing pump start after loss of offsite power. Loss of offsite already leads to reactor trip and post trip service water operation is not credited in the GRA model. See note 3.

3.2 Additional Modeling Assumptions and Comments

1. Passive failures such as pipe leakage or rupture were not included in the SW GRA model.

2. The exposure (mission) time for all running SW components is 24 hours. All operating components are assigned this 24-hour mission time. The mission time for these components is adjusted during cut sets post processing to the desired mission time (i.e., 365 days).

3. Based on conversation with plant staff, the average Winter duration is two-thirds of the year and Summer duration is one-third of a year. There is a brief period (~ 14 days) in the Summer (the hottest part) where cooling of the TEC loads requires all four service water pumps. The fractions of the year for Winter, Summer and hottest Summer are .67, .29 and .04, respectively. These fractions are applied to basic events WINTER, SUMMER, and SUMMER-HOT, respectively.

4. The boundary of the GRA SW system model is limited to all equipment in flow paths to the non-critical load header and to the service water discharge canal. Failures of operating equipment normally supplied by service water are included in their respective GRA system models. Service Water flow paths to the diesel generator and to the RHRSW systems are not included because they are standby components and are only required for safety purposes (i.e., accident mitigation). Other flow paths are also not included in this GRA model (specifically, screen wash pumps, condenser backwash, backup to circulating water pump seals, and circulating water fill) as loss of service water to these loads would not impact plant operability.

5. The plant operating philosophy is to have one pump in each service water train operating if a total of two pumps are required. The pumps are periodically rotated to distribute the service equally among the four pumps. In the Summer time when three pumps are

required, both pumps in a loop plus one pump in the other loop would be operating. Flag events are included for each train to enable selection of the initial desired configuration.

6. During normal system operation, the service water train crosstie valves MV-36 and MV-37 are open to supply water to the non-critical and normally operating loads. Failure of a single SW pump could lead to pressure perturbations that could result in their closure. This would automatically isolate SW flow to the TEC heat exchangers. The valves close automatically on low pressure in the SW headers (20 psig) and an alarm will be initiated in the control room alerting the operators of the loss of TEC cooling supply. If the operators do not respond by reopening the valve and restarting a standby pump, the plant would eventually be shutdown when the TEC exchanger exit temperature limit is exceeded. The plant staff indicates that it would take about 15 minutes to exceed the temperature limits of the TEC Hx outlet temperature with no SW flow. Therefore, the operator must reopen MV-36 and 37 within this time frame to avoid having to shutdown the plant. This logic is included in the SW GRA model.

7. Diversion of flow from the main flow path through the recirculation line (MO-2138 and MO-2139) would not significantly impact the flow to the SW loads as the recirculation line is only 1 ½ inches in diameter versus the 24 inches SW train flow path.

8. The SW pumps require seal cooling. The normal supply is from the service water pumps themselves. The Riverwell System is available as a backup source of gland seal cooling. If gland water pressure is not recovered in 20 seconds a SOV opens to supply gland water via the fire protection system. Failures of gland seal cooling components were not explicitly modeled. Instead, two undeveloped events representing failure of LOOP A (SWS-MDP-FR-LOOPA) and B (SWS-MDP-FR-LOOPB) SW pumps due to loss of seal cooling were included in the model. They were assigned a failure rate of 9.36E-6 per hour, based on generic failure rates.

9. Severe plugging of the pump discharge strainers (S191 and S192) is considered in the model due to experience with increased silt intake from the river through the intake structure. At the time of this analysis each strainer was being manually isolated once per week (one strainer at a time) to manually clean the strainers. Thus, plugging of the strainer and failure of the isolation path are included in the model to represent the potential to lose flow to the SWS headers. Specific assumptions associated with strainer plugging events are included below:

    a. Performing the PM activity does not contribute to loss of SW flow: the operators won't initiate the PM unless they can establish flow through the bypass line.

    b. Failing to reposition valves, or failure of those valves to reposition, after PM is not a Loss of Flow (or loss of SW) problem. But, it does have an impact on "Manual Shutdown" frequency, since the plant needs to declare DG inoperable when doing the PM, and if flow can't be reestablished through the strainer they need to shut down the plant after a few days. So, even though unlikely, each time

they do PM is an opportunity for them to have an LCO-induced manual shutdown.

c. The backwash system is in automatic mode to begin. If the alarm set point of 6 PSID is reached, operators will switch backwash into manual mode.

d. Although automatic backwash starts at 4 PSID it may not be rapid enough to prevent delta-p from continuing to increase to the 6 PSID alarm set point. However, the backwash will continue to operate and may clear the strainer before 15 PSID is reached.

    i. For situations in which "large debris" is assumed, the backwash is capable of clearing the debris prior to reaching 15 PSID 50% of the time.

    ii. For situations with "small to normal sized" debris, the backwash is capable of clearing the debris prior to reaching 15 PSID 100% of the time.

e. 15 PSID is assumed to be "failure" – at which point flow from the associated service water path downstream of the affected strainer ceases. (Note that strainer "bursting" like a diaphragm is not considered.)

    i. Loss of flow from one strainer is the same as loss of two service water pumps. Thus, depending on the time of year loss of one strainer may be sufficient to result in a plant shutdown.

        1. Plant derates to "keep up with" the reduction in flow are not considered, i.e., the plant is either at 100% power or a shutdown is initiated upon loss of flow required to maintain cooling associated with 100% power.

f. Following receipt of the 6 PSID alarm operators will switch the backwash to manual (continuous) operation and will monitor the situation. If the delta-p continues to rise, operators will initiate actions to bypass the strainer(s) and manually clean them.

    i. For small to normal sized debris the operators have a substantial amount of time before 15 PSID is reached.

        1. A Human Error Probability (HEP) of 1E-3/demand is used to represent failure of the operators to recognize the need for and to take action.

    ii. For large sized debris it is assumed that the operators have considerably less time.

1. A HEP of 0.5/demand is used to represent failure of the operators in these situations. (Source: expert opinion, plant staff)

iii. These HEPs are used for loss of flow evaluations. Different HEPs can be used in post-trip evaluation if recovery of service water is an issue.

g. A separate event probability is used to represent plugging due to small/normal sized debris, and plugging due to larger sized debris

i. Plugging is defined as sufficient debris in the strainer to cause the delta-p to reach 6 PSID.

ii. 16 alarm events were recorded over a 3 year period (source: Randall Noon). Although this data is from a time in which the weir walls were in their original configuration (as opposed to the current configuration with a different weir wall design and with turning vanes) it is assumed to be representative (data associated with the current configuration is sparse or non-existent).

1. 1 of these 16 is assumed to be representative of the frequency of large sized debris (such as the November 2004 event).

2. 15 of these 16 are assumed to be due to normal sized debris.

3. A time-based (hourly) plugging rate is assumed

a. Plugging, Large Debris = 1 event/(3 years x 8760 hours/year) = 3.8E-5 events/hour

b. Plugging, Small to Normal Debris = 15 events/(3 years x 8760 hours/year) = 5.7 E-4 events/year

4. A 10% beta factor is assumed for common cause for both small/normal and large debris

a. Plugging of both strainers, Large Debris = 3.8E-5 x 0.1 =-3.8E-6

b. Plugging of both strainers, Normal Debris = 5.7E-4 x 0.1 = 5.7E-5

h. Common cause failure is assumed to be valid for simultaneous failure of the backwash systems for both strainers, as well as between the manual valves in the bypass paths for the strainer paths

i. A beta factor of 0.1 is used for both of these situations

i. No changes are required for the failure rates in the REC, TEC, or elsewhere for the 24 hour post-trip evaluation.

j. For purposes of modeling and failure probability the strainer backwash system is treated as a "supercomponent" encompassing the drain valve, MOV, motor, and wiper.

   i. The backwash system must start upon manual initiation from the operators when the 6 PSID alarm set point is reached.

   ii. The system must continue to run for 1 hour (assumed) in order to clear the debris (in those cases where the system is assumed to be functionally capable of clearing debris)

   iii. The Fail to Run failure probability assigned is that for Motors (30-60 HP,) from IEEE-500 Section 4.1.1.a "All Modes", namely, 5.7E-6/hour (page 225)

      1. Note that traveling screens as found in the Savannah River database are assigned a failure rate of 5.2E-7/hour with a lognormal EF of 10

   iv. The Fail to Start failure probability is taken to be a combination of motor failure and valve failure

      1. Motor failure is also from IEEE-500, Section 4.1.1.1, "All Modes", 2.47E-5/demand (page 227)

      2. Valve failure (MOV Fail to Open) is from the PRA database, at 3E-3/demand (source: NUREG/CR-4550)

      3. Total = ~3E-3/demand (i.e., dominated by valve fail to open)

   v. The FTS and FTR values are combined to derive a pseudo "Fail to Operate" value of ~3.1E-3/demand

3.3 Assumptions from the PRA SW Model

The following PRA SW modeling assumption was reviewed for applicability to for GRA.

1. Service Water Pumps 1A, 1B, and 1C are normally operating. Pump 1D is idle.

GRA: Pump configuration house events are included for the SW pumps for manipulation.

2. The SW Pumps have mode selector switches for setting in automatic-manual-standby positions. A pump can be running and still in the standby position. Pumps in standby will start automatically following a LOSP event. Annunciation is arranged so that at least one selector switch in each loop must be set to standby position to avoid an immediate alarm. This assures automatic startup of at least one SW Pump per loop in an emergency.

GRA: Pump start after a LOSP event has been eliminated because a LOSP event would have resulted in a reactor trip. Pump configuration house events are included for all SW pumps.

3. Service Water Pumps 1A and 1D are in standby mode and will automatically start after LOSP is restored.

GRA: Modeling for four pump status configurations is included in the GRA model.

4. RBCCW Heat Exchanger 1B is operating. SW to RBCCW Heat Exchanger 1A is isolated by Valve MOV-651MV.

GRA: Same for GRA model.

5. Gland Water Supply to the SW pumps has a normal supply and two backup supplies and is modeled superficially in the fault tree, but has a low probability of failure.

GRA: Same for the GRA model

6. Failure to restore an RHR heat exchanger or a service water pump or a service water booster pump following maintenance is not considered because the heat exchangers and the pumps are put back into service immediately following maintenance and an improper configuration would be identified immediately and corrected.

GRA: Flow to the RHRSW system is not included in the GRA SW system. The RHRSW system which provides flow to the RHR heat exchangers is only credited to mitigate a plant transient in which the reactor has already tripped.

7. There are no failure to restore after maintenance events for Service Water Valves SW-V-417, 419, 421, and 423 - SW supply to Emergency RBCCW Loops. Monthly surveillances are performed and any failure to properly restore would be discovered and corrected. Failure to restore is included in plant specific data.

GRA: SW flow directly into the REC system is only performed during emergency conditions when the plant has tripped and flow to the REC heat exchanger is not available. Therefore, this flow path is not credited in the GRA SW model.

8. RBCCW heat exchanger unavailable due to maintenance is addressed in the RBCCW system model.

GRA: RBCCW heat exchanger unavailable due to maintenance is not included in the SWS GRA model..

9. Service water hardware failures in the DG cooling system for lube oil coolers, jacket water coolers, air intake coolers, and associated temperature control valves will be treated as one event.

GRA: Service water flow to the DG cooling system is only credited to mitigate a LOSP power event, when the DGs are required. Since the reactor has already tripped as a result of the LOSP event, this flow path is not credited for power operation.

10. Failure to restore service water to DG after maintenance is not considered because the DG is operated after maintenance and a failure to restore would be identified immediately. Failure to restore is included in plant specific data.

GRA: See #9.

11. Failure to restore SW to DG fan coil circuits after maintenance is not considered because the FCU is operated immediately after maintenance and any failure to restore would be identified immediately.

GRA: See #9.

12. Backflow through check valves SW-CV-28CV and SW-CV-27CV supply to RBCCW heat exchangers is not modeled because at least two passive failures would be required to allow flow back through SW pump discharge check valves.

GRA: Same for the GRA model.

13. Non-detectable passive plugging failures, including internal valve failures such as disc detachments, and failures to restore equipment are added to fault trees only where they are reasonable and can be a significant contributor considering the normal operation of this system.

GRA: Same for the GRA model.

14. Failure of the SW System due to biofouling, ice frazzle, trash rake plugging or Asiatic clams was considered negligible. Cooper has never experienced these events (ice blockage is prevented during the winter by a de-icing gate which routes discharge of the main condenser to the inlet of the SW pump intake structure). Trash rake plugging is a gradual occurrence, usually following heavy rains, and is alarmed in the Control Room. Adequate time is available to increase the traveling screen speed, increase sparging, or if necessary bypass the service water inlet to an alternate bay.

GRA: Same for the GRA model.

15. Low water at the intake structure is a gradual process, Tech Specs require plant shutdown at a safe level to assure adequate water.

GRA: Low water level (<865') in the E Bay is dependent on the River level and rise of fall of the river level is a natural phenomenon that can be modeled by reviewing historical data associated with rivers level. Therefore, it is not included in the GRA model. However, service water strainer plugging, possibly as a result of low or falling water level, is modeled.

16. The single passive failure of a pipe rupture in the service water header is of a low enough frequency that it is not considered.

GRA: Forced outage due to pipe failures in the SW system has occurred in the industry (Cause Code 3811 according NERC-GADS). However, forced outages due to pipe failures have not occurred at Cooper and thus are not included in the GRA model.

4.0 System Reliability Data

The following SW reliability data was used to quantify the GRA SW top event(s) defined in Section 2.

4.1 Basic Event Failure Rates

All of the component failure rates used in the SW GRA model are from the Cooper PRA project except the following events.

- SWS-XHE-FO-M367 1.00E-2 Operator fails to re-open MV-36 or MV-37

  Per assumption 3.1.4, this action is to reopen MV-36 or MV-37 to restore service water to either one TEC heat exchanger after auto closure on low header pressure. Low pressure can occur when an operating pump trips.

- SWS-MDP-CF-2MDPS and SWS-MDP-3MDPS 8.53E-06 Common Cause Failure of 2 of 4 and 3 of 4 SW pumps to Run

A common cause factor of 0.1 was used for common cause failure of 2 and 3 SW pumps.

o SWS-XVM-FO-SHORT	5.00E-02	Bypass 20" butterfly valve not opened by maintenance staff - Limited Time
o SWS-FLG-PG-CLEAR	5.00E-01	Backwash can clear
o SWS-FLG-PG-NOCLR	5.00E-01	Backwash cannot clear
o SWS-MOV-PG-651MV	2.40E-06	Motor Operated Valve 651MV Plugs
o SWS-STL-CF-SWA_B	9.12E-05	Large Debris Plugging, both strainers (common cause)
o SWS-STL-PG-191BIG	9.12E-04	Large debris plugging, this strainer only
o SWS-STL-PG-192BIG	9.12E-04	Large Debris Plugging, this strainer only
o SWS-STR-CF-SWA_B	1.37E-03	Small Debris Plugging, both strainers (common cause)
o SWS-STR-PG-192	1.37E-02	Strainer S-192 plugged
o SWS-STR-PG-S191	1.37E-02	Small debris plugging, this strainer only
o SWS-STR-PG-S192	1.37E-02	Small debris plugging, this strainer only
o SWS-XVM-CC-193	1.00E-04	20" butterfly valve 193 FTO
o SWS-XVM-CC-194	1.00E-04	20" butterfly valve 194 FTO
o SWS-XVM-CF-193_4	1.00E-05	20" butterfly valve 193, 194 FTO, common cause
o SWS-XVM-FO-194	1.00E-02	20" butterfly valve 194 not opened by maintenance staff
o SWS-XVM-FO-LONG	1.00E-04	Bypass 20" butterfly valve not opened by maintenance staff - adequate time
o SWS-XVM-FO-SHORT	5.00E-01	Bypass 20" butterfly valve not opened by maintenance staff - Limited Time
o SWS-XVM-OC-16	2.40E-06	24" butterfly valve 16 FTRO
o SWS-XVM-OC-17	2.40E-06	24" butterfly valve 17 FTRO
o SWS-XVM-OC-191	2.40E-06	24" butterfly valve 191 FTRO
o SWS-XVM-OC-192	2.40E-06	24" butterfly valve 192 FTRO
o SWS-XVM-OC-193	2.40E-06	20" butterfly valve 193 FTRO
o SWS-XVM-OC-194	2.40E-06	20" butterfly valve 194 FTRO

See Strainer Assumptions in Section 3.2 for basis.

4.2 Component Mean Time to Repair (MTTR)

The service water pump MTTR (287 hours per occurrence, Cause Code 3810) is obtained from NERC-GADS. It is the average hours per occurrence for forced outages U1 and U2. This NERC-GADS value is much higher than what was reported in WASH-1400 for motor-driven pumps but it is reasonable given that the SW pumps are large and complex pumps and are likely to require a relatively long time to repair when they fail. The remaining components in the SW systems are assigned MTTRs from WASH -1400.

All Plants (1982 - 2003, 1743 UnitYear) Cause Code 3810 - SW Pumps and Motors			
Force Outage	# of Occurrence	Hours Loss per Occurrence	Total Hours
U1	2	134	268
U2	2	440	880
Total	4		1148
Average	1148 hours / 4 occ = 287 per occ		

These MTTR can be found in Reference FT-4.

5.0 Cut set Post Processing

The following was performed on the service water system cutsets to obtain the final system top event frequency.

1. The PRA2GRA code was used to convert mission times from 24 hours to 1 year.

2. The PRA2GRA code also assigned "mean time to repair" values, based on assigned values.

3. A default value of 168 hours was used for any event not specifically assigned. The mean time to repair values can be found in table "MTTR" of Reference FT-4.

4. PRA2GRA was then used to assign consequences, i.e., the number of equivalent lost full power hour hours associated with the component outage. This is calculated as a function of the derate and the amount of time required to restore the plant to 100% power. The time is in turn a function of the "mean time to repair the equipment", plus the "heat up time" (to restore the plant to 20% power, when the plant is synchronized to the grid), plus the time required to go from 20% to 100% power.

5. All cutsets containing at least one service water basic event are retained. Cutsets containing no service water events are deleted from the service water top event cutsets.

6. The result is the amount of "equivalent full time hours" lost as a result of component failures associated with the generator system.

6.0 Results

The yearly frequency for service water system unavailability resulting in a 100% derate, as modeled for the GRA, is 0.05. This failure rate is approximately equal to one failure for every 20 years of plant operation. The rate is higher than service water failures that result in plant trip in the industry (6.9E-3 per year, sum of failure rates for NERC cause codes 3810, 3812, 3813 & 3819). The total failure rate does not include piping failures that led to a forced outage (cause code 3811), which is consistent with the SW model. There are no reported service water failures that resulted in full plant trip in the 16.3 operating-years of Cooper experience represented in the 22 calendar-years of data in NERC-GADS (an operating-year is equal to a calendar-year x average service hours (hours plant was available and on-line) divided by 8760 hours/calendar year; for the 22 calendar-years included in the NERC-GADS database for CNS, the average service hours per year was approximately 6490: (22 x 6940/8760 = 16.3)). However, recent

experiences with falling or fluctuating river water level have shown that there is a possibility of strainer plugging resulting in loss of service water flow. That issue is being addressed through strainer backwash procedures in the short term; a longer term solution is being implemented involving changes to the intake structure.

When factoring in consequences (in other words, the amount of full power equivalent hours lost as a result of system unavailability), there are a total of 8.22 full power hours per year lost, on average; due to SW system component failures resulting in 100% derates. Full power at Cooper is 764 MWe, which translates to 6280 MWh per year due to SWS failures.

6.1 Top Contributors

The top contributor to the 100% plant trip and subsequent economic consequence is plugging of a SW pump strainer during the summer months. Plugging of the strainer, failure of the operators to establish flow through the bypass line, and the resultant assumed loss of flow due to the plugging eliminates flow from 2 service water pumps – sufficient to lead to a plant shutdown. This scenario contributes 2.98 of the 8.2 EFPH lost. Other strainer plugging scenarios contribute an additional 1.5 EFPH. These are followed by loss of gland seal cooling to Loop A or Loop B of the SW pumps (.33 EFPH each) and common cause failures of 2 of 4 pumps (.31 EFPH) – all in the Summer time period. Close behind these three contributors are single failures of any of the four SW pumps during the hottest summer period (.30 EFPH each).

The contribution of the gland seal cooling loss may be overstated as gland seal cooling is backed up by more than one independent cooling source if the primary system fails (see Assumption 3.2.8). These systems were not included in the SW model, but rather a point value was included to represent failure of the pumps due to loss of gland seal cooling.

6.2 Comparison to Industry

A review of Cooper specific NERC data from 1982- 2003 shows no forced outage due to SWS failures. For the industry in this period, which includes both PWR and BWR units, the MWh loss per year (NERC Cause Codes 3810, 3812, 3813, 3814 & 3819) is 1,326 MWh per unit year or 1.9 equivalent full power hours per operating year (Ref. NERC-1). Segregating only BWRs for this period, the total MWh loss per year is higher, at 2,419 MWh per unit year or 3.7 equivalent full power hours per operating year (Ref. NERC-3). The frequency of a plant shutdown for the “BWRs only” situation is 0.015 per operating year. Compared to the industry, the Cooper SW system is higher in frequency of events leading to full plant shutdown, with a corresponding higher MWh loss on average per year.

6.3 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the generator fault tree. The figure represents components in 100% derate or plant trip case.

The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the system to lost generation given the current reliability of components as assumed in the GRA.

The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur if the reliability of the individual components was allowed to degrade significantly.

Points in the upper-right quadrant are components having both high risk decrease and increase potential and therefore, merit some attentions with regards to reliability. There are many components located in the upper-right quadrant. These include events associated with plugging of the strainers, and failures of the SW pumps (they are the major active components in the system and that they historically have shown to have the longest repair time if they were to fail).

On the threshold between the upper left and upper right quadrants are failures of gland seal cooling to Loop A and Loop B of the SWS, as well as common cause failures of 2 out of 4 SWS pumps. Gland seal cooling is important year around. Plugging of one strainer with large debris has the highest risk decrease potential (i.e., is located farthest to the right on the plot) – this plugging, if not addressed quickly by the operators though actions to implement strainer bypass, will cause one loop of SWS to fail. This in turn results in loss of flow from two SWS pumps, which is similar in impact to loss of gland seal cooling. Also located far to the right on the plot is common cause (simultaneous) plugging of both strainers, which causes both loops of SWS to fail if the strainers are not bypassed. This has impact on risk reduction because it has a lower probability of occurrence than plugging of a single strainer.

Other components located in the upper right quadrant or at the threshold between upper right and upper left are each of the individual SWS pumps. SW pump D is located very slightly lower on the plot than the other three SWS pumps; this is a result of a modeling assumption in which SW pumps A, B and C are initially operating and pump D is in standby.

Components in the upper left quadrant include common cause failure of three SWS pumps, and butterfly valves in the normal or bypass lines of the strainers (the failure mode of interest is “fail to remain open”).

The bottom right quadrant contains two points clearly within the quadrant. Point 1 is the failure of the operator to complete timely strainer bypass following plugging of a strainer (or both strainers) with large debris. The failure rate assigned to this action is quite high for operator actions, namely, 0.5. A high failure rate such as this, assigned to an event which has extreme ramifications if failed, produces the importance measures that place this event in the lower right. Typically, there are no points in the lower right since plants tend not to tolerate components or events with high importance coupled with high unreliability. In this case, the human error probability may be quite conservative – additional analyses may be warranted for this action to determine if either its failure rate can be lowered or its importance can be reduced.

Point 2 represents scenarios in which large debris is plugging the strainers, and the automatic backwash action cannot clear the debris. A conservative value of 0.5 has also been assigned to

this event. Since failure to clear large debris results in the requirement for rapid operator initiation of bypass, this event is also quite important. Again, this value may be conservative, and additional data collection and analysis for plugging events may enable the value to be reduced.

Other points are in the lower left quadrant or near the threshold of that quadrant.

6.4 Uncertainty Analysis

An uncertainty analysis was performed using UNCERT (Ref. O-5), a R&R Workstation program, for the SW 100% top event. Uncertainty distributions were assigned only to components and human error events and were not assigned to the mean time to repair events or maintenance, or the events representing the startup durations. In the analysis, complete correlation is assumed for similar type components that are represented by the same basic event type code.

The results of the analysis are shown in Figure 2.

#Iterations = 10000
Mean lost generation = 8.11 EFPH
Std Deviation =16.9

Cumulative Probability	Lost Generation (EFPH)
5%	1.86
50%	4.1
95%	24.4

7.0 References

Cooper Procedures and Lesson Plans (CPP)

1. Emergency Procedure 5.2REC – Loss of REC, 10/28/04
2. Abnormal Procedure 2.4TEC – TEC Abnormal, 7/7/04
3. Emergency Procedure 5.2SW – Service Water Casualties, 9/20/04
4. CNS USAR Section B 3.7.2 Service Water SW System and Ultimate Heat Sink (UHS)
5. OPS Service Water/COR002-27-02, Revision. 25, CNS Service Water Lesson Plan.
6. COR002-27-03, Revision 5, Service Water Lesson Plan.

Cooper Drawings (CD)

1. 3.7.2 Service Water (SW) System and Ultimate Heat Sink (UHS) [6] 2006 Sh. 1 "CNS
2. Flow Diagram – Circulating, Screen Wash & Service Water Systems", Revision N48
3. 2006 Sh. 2 "CNS Flow Diagram – Circulating, Screen Wash & Service Water Systems", Revision N25
4. 2006 Sh. 3 "CNS Flow Diagram – Circulating, Screen Wash & Service Water Systems", Revision N48
5. 2006 Sh. 4 "CNS Flow Diagram – Circulating, Screen Wash & Service Water Systems", Revision N43.
6. 2036, Sh 1, "CNS Flow Diagram – Reactor Building Service Water System" Revision N88.

PRA Sources (PRA)

1. PSA-SA019, "PRA System Notebook - Service Water and RHR Service Water Booster System"
2. PSA-SA020, "PRA System Notebook - Service Water Cross-tie System"

Fault Trees, Results, and Database (FT)

1. CNS PSA CAFTA Merged Fault Tree Model, Merge.caf - Date 1/21/2002 File Size 180kb
2. CNS PSA CAFTA Basic Event and Gate Databases:
    - pra2001a.BE, 8/21/2002, 591kb
    - pra2001a.GT, 1/18/2002, 999kb
    - pra2001a.TC, 1/18/2002, 33kb

3. Service Water GRA Fault Tree, SWS GRA 10-13-05.caf, 10/14/05, 51kb
4. Service Water GRA Basic Event and Gate Databases:
    - CNSGRASwyrdGenSWS10-13-05.rr, 10/25/2005, 3,798 kb
5. Service Water cut sets: SWS-GRA Converted 101705.cut, 10/25/05, 36 kb
6. Four quadrant plot, SWS 4 quad plot 051023.xls, 10/25/2005, 58 kb

PC-GAR Spreadsheets (NERC)

1. NERC-GADS Cause Codes Report for Industry (1982-2003)
    1-IndCauseCodeTotals PWRs and BWRs for SWS 1982-2003.xls, 20kb, 8/3/2005
2. NERC-GADS Cause Codes Report for Cooper Nuclear Plant (1982-2003)
    CNS-CompCauseCodeLosses.csv, 50kb, 12/17/2004
    CNS-IndCauseCodeTotals.xls, 40kb, 4/14/2005
3. NERC-GADS Cause Codes Report for BWRs Only (1982-2003)
    4-IndCauseCodeTotals BWRs only for SWS 1982-2003.xls, 18KB, 8/3/2005

Other (O)

1. North American Electric Reliability Council (NERC), "pc-GAR for Windows", release 2.06 v26, 2004
2. Applied Reliability Engineering, Inc., "PRA2GRA", December 16, 2004
3. Electric Power Research Institute (EPRI), "CAFTA", version 5.1a, 2003
4. Applied Reliability Engineering, Inc. (AREI), "SetEventStates.exe", March 2005.
5. Nuclenor, Iberdrola, and Data Systems and Solutions, "Uncert for Windows", Version 2.3a, 2002.

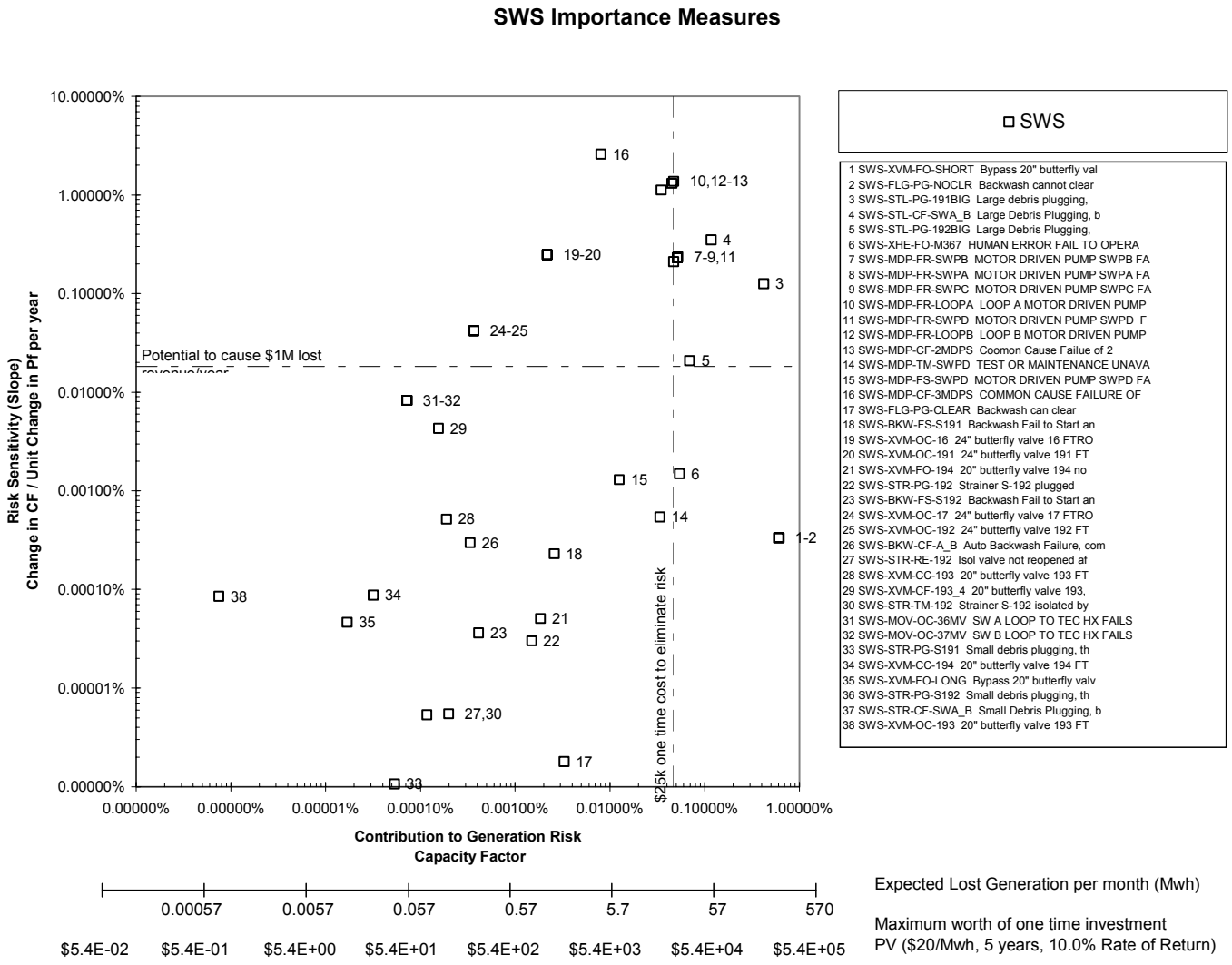
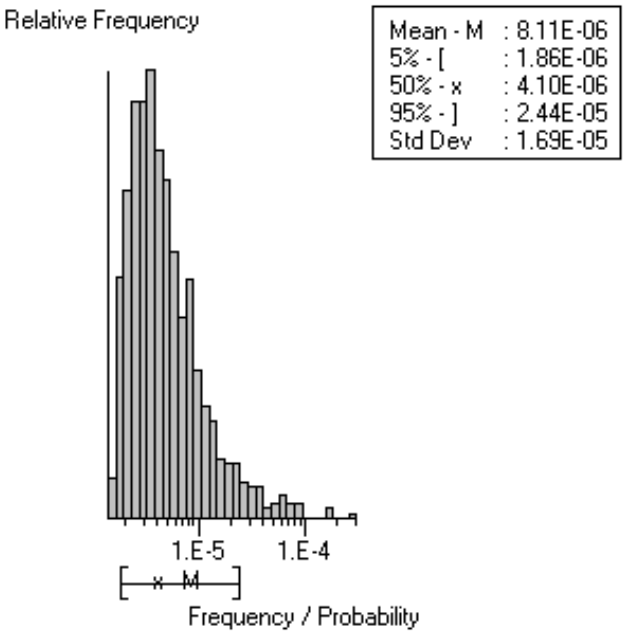


Figure 1
Service Water Four Quadrant Plot

Density Function



Cumulative Function

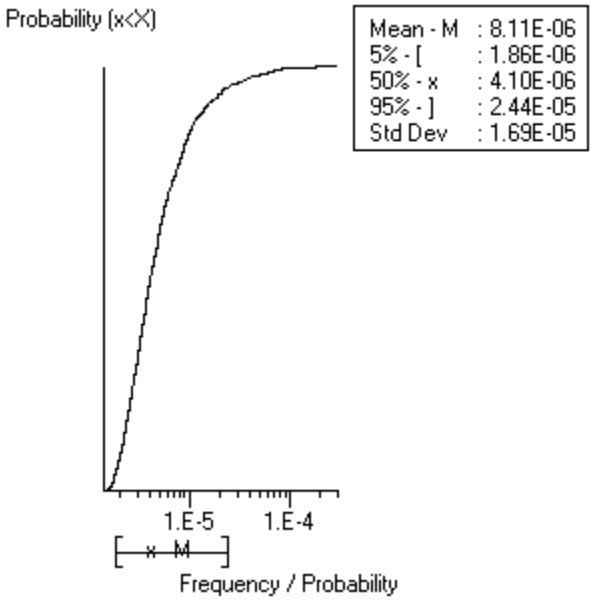


Figure 2
Uncertainty Analysis Results – Service Water, 100% Derate (Equivalent Full Power Hours (EFPH))

Note: Multiply all results by 1E+06

Switchyard

Rev. 0 8/1/2005

1. System Function

GRA Function: For GRA purposes, the function of the switchyard is to distribute power from the main generator and main transformer to the transmission system. Only transmission to the 345kv lines is considered in this model; the 161kv Auburn line and 69kv line are not included.

2. Success/ Failure Criteria

Plant Disconnected from Grid – 100% Loss of Generation

The success/failure criteria of the generator are dictated by the ability of the 345kv switchyard to transmit electrical power to the five 345kv lines (the "ring bus"). A 100% loss of generation to the transmission system occurs when the switchyard becomes unavailable to the entire 345kv grid. Thus, for the GRA, a 100% derate failure is defined as:

Failure of the switchyard to provide electrical power from the main generator and transformer to any of the five 345kv lines.

Note that the definition is not strictly associated with or reliant upon the status of the plant. In other words, theoretically speaking, the plant may be tripped or it may still be generating steam (although a loss of the 345kv switchyard should result in a plant shutdown). The main concern for the GRA is the ability of the switchyard to provide "input" to the 345kv transmission lines. If it was possible for the plant to remain at 100% "rods out" while the switchyard was completely unavailable, this would be a valid situation as far as evaluation of the switchyard is concerned. Thus, although a 100% loss of generation is most likely also a 100% plant derate (full plant shutdown), it theoretically does not have to be.

Plant Disconnected from the Grid - Less than 100% Loss of Generation

Situations in which less than 100% (but more than 0%) full power is flowing from the generator to the switchyard are addressed by "partial derate" evaluations for the plant's frontline and support systems. The switchyard GRA evaluation is focused on cases in which full power is reaching the switchyard, but not flowing to the transmission system.

For the GRA it is assumed that as long as any of the five 345kv lines is available full power generation to the transmission system is possible. In other words, the unavailability of a single or up to four 345kv lines is possible without affecting the ability to provide full generation capability to the transmission system – all power would flow through the remaining line(s). Thus, loss of any 345kv line is not included as a "partial" loss of generation situation.

Similarly, failures of flow paths within the switchyard that eliminate flow to one or more (up to four) 345kv lines are also not considered to be "partial" loss of generation situations. As long as power can still reach at least one 345kv line, regardless of the path taken to get there, full generation is assumed.

Finally, no degradation of lines or hardware (specifically, transformers) that would result in a reduction, but not a total loss of transmission, was included in the evaluation. Thus, all failures are "all or nothing" failures. For example, the evaluation includes no transformer degradation events in which some problem in the transformer does not completely disable the transformer but allows a reduced (less than 100%) of power to go to the grid.

As a result of these assumptions, there are no "Less than 100% Loss of Generation" to the grid cases included in this assessment.

3. Fault Tree Modeling

3.1 Development of Fault Tree

A previous project produced two versions of a switchyard fault tree. One version can be used to determine the frequency of a loss of power FROM the switchyards to the plant during otherwise normal operations, and is an integral part of the models used to estimate the frequency of plant-centered loss of offsite power – an initiating event in the Cooper PRA. The other version, very similar in basic content to the first, is used to calculate the probability of a loss of ac power to the vital buses from the switchyards during the first 24 hours following a postulated initiating event (an event modeled in the PRA as requiring successful system and operator response to avoid the onset of damage to the fuel). These models include the NSST, the 345kv switchyard, the 161kv switchyard, the SSST, and the 161kv Auburn line. Their focus is on the flow of electrical power from the grid into the plant, as opposed to from the plant to the grid.

Subsequent to the completion of those models a separate study was completed to assess the impact of grid stability (or instability) upon the plant. That study used as a starting point the switchyard fault tree developed for use in evaluating post-initiating event mitigation (the "24 hour" fault tree). Additions to the fault tree were made to include detailed development of 345kv line faults (such as losses due to wind, fire, tornado, etc.). Other modeling additions were included as part of an effort to develop a "grid stability monitor". Discussions with the study's author verified that those changes had no impact or bearing on the GRA, and could be dropped from the model for the GRA.
The resulting grid stability model includes events associated with the ESST and the 69kv line that are important when considering loss of power TO the station, but are not relevant when considering loss of power FROM the station to the 345kv lines through the 345kv ring bus.

Thus, the GRA fault tree used as its foundation the fault tree developed to determine the frequency of plant-centered loss of offsite power, modified to include some of the changes made to the accident mitigation model (the 24 hour fault tree) in the grid stability study. Most

important among these is the addition of the detail (events and their probabilities) for individual line faults.

Changes to the fault tree were then made to adjust for the different top event definition. Whereas the "loss of offsite power (LOSP) switchyard model" has as its top event "plant-centered loss of offsite power" (no power from the switchyards to the plant), the GRA model's top event is "No 345KV Switchyard – 100% Loss of Transmission to Grid from Switchyard." As a result, the following changes were made:

1. The top gate was changed from an AND gate to an OR gate. Previously, the gate represented failure to receive power at Bus 1C and/or1D from the switchyards AND from the NSST, i.e., both sources had to be disabled before there would be a need for the ESST or the diesel generators. For the GRA a failure of the NSST prevents power from flowing to the switchyards from the main generator, and then on to the transmission lines. In addition, even if the NSST is in operation, specific failures within the 345kv switchyard prevent power from reaching the 345kv lines. Thus, the top event is failure of NSST path OR failure in switchyard.
2. The LOSP model includes power coming from the SSST and the 161kv switchyard. The GRA model does not credit transmission through this path to the 161kv Auburn line as a valid 100% generation path. Thus, the 161kv switchyard and the SSST events were deleted from the fault tree, with the exception of events dealing with isolation of line faults in the Auburn line – if not isolated successfully, those faults could potentially propagate to the 345kv switchyard and possibly fail that switchyard as well.
3. All "mission time" events (events whose probability of failure is a function of the length of time required of its operation) were set to use a 24 hour mission time. This allows the PRA2GRA code to be used to calculate various system failure frequencies based on different mission times, ranging from 24 hours to one year or more. (For the GRA evaluation, frequencies based on a one year time frame are used as the baseline.)
4. As mentioned previously, detail for line faults was added, using the grid stability model and the grid stability report to include appropriate failure probabilities (the line fault probabilities have units of "per hour per 100 miles of line").
5. Events associated with successful continued operation of the NSST during repair of the SSST, and operation of the SSST during repair of the NSST, were deleted. If plant systems are operating off of the SSST the NSST is off-line, meaning that the plant is not providing power to the grid; thus, the initial loss of the NSST is sufficient for the GRA model. Similarly, although it is possible to do on-line maintenance and repair of the SSST while the NSST is operating, the maintenance/repair time is assumed to be much shorter than the one year mission time used in the GRA evaluation for "normal" NSST operation. Thus, the shorter mission time event is subsumed by the longer one, and can be deleted from the model without loss of information.
6. Failure of the generator to run during normal operation is represented by a transfer event to the generator 100% derate fault tree (developed separately). The transfer is to the potion of the generator fault tree dealing with generator-specific failures, i.e., those associated with NERC cause codes 4500 through 4580 (this is gate TG_-002). This transfer replaces the event "EAC-MGN-FR-MNGEN" (main generator fails to run during normal operation) that was in the original LOSP switchyard model.

3.2 Modeling Assumptions and Comments

1. For the GRA, the exposure time of interest for all components is one year. For the base model, operating times of 24 hours were assigned to the data, which were then updated to a one year exposure time using the PRA2GRA conversion code.
2. Any failure of a transformer was assumed to be a complete failure (see previous discussion about "less than 100% Loss of Generation").
3. It is assumed that any event that results in a full plant derate (100% power) leading to cold shutdown causes the plant to implement the 3 day outage plan. This means that all cold shutdown events have minimum outage times of 72 hours before the plant begins to heat up to return to power. Thus, even if a component has a mean time to repair of less than 72 hours, the plant remains shutdown for 72 hours to complete other repairs.
4. See Section 4 for assumptions specific to data.

4. System Reliability Data

The PC-GAR software program (v2.06) was used to develop failure rates (failure per hour) for the main transformer, the NSST, and the AutoTransformer (T2). For other components, the failure rates (per demand and per hour) included in the database developed for the "plant-centered LOSP" model.

Failure rates from NERC data were developed by dividing the number of "forced outages" by "service hours", for each specific cause code. All US nuclear plants were included in the data.

1. "Forced outages" included any event classified as U1, U2, or U3 within PC-GAR, for each specific cause code.
2. "Service hours" were calculated by taking the average annual service hour value, provided by PC-GAR for the set of plants specified, and multiplying by the total number of "unit-years" given by PC-GAR for that set of plants.
3. Cooper-specific data from PC-GAR were used if available. For the switchyard, only one cause code exists within the PC-GAR database for Cooper, namely, cause code 3620, Main Transformer. For this single cause code the number of forced outage event occurrences and the total number of service hours are limited to Cooper values.

"Mean time to repair" values were also extracted from NERC by taking the "hours per occurrence" as representative of the repair/recovery time. When multiple forced outage categories (i.e., U1, U2, U3) exist for a specific cause code, a weighted average of the hours per occurrence was used to derive a MTTR for the cause code.

See the Generator GRA documentation (CNS-GRA-GENERATOR.doc) for other discussions about the use of PC-GAR data, such as the interpretation of "hours per occurrence".

In determining the time to recover the plant to full power conditions, a cold shutdown is assumed to be necessary to complete any repair of a switchyard component whose outage leads to a 100% derate.

In addition to the above applications of data, Bayesian updating was performed for data derived from NERC information. The Generator GRA documentation contains a discussion of the Bayesian updating approach used.

5. Cutset Post Processing

The following was performed on the generator system cutsets to obtain the final system top event frequency.

1. The PRA2GRA code was used to convert mission times from 24 hours to 1 year.
2. The PRA2GRA code also assigned "mean time to repair" values, based on assigned values.
3. A default value of 168 hours was used for any event not specifically assigned.
4. PRA2GRA was then used to assign consequences, i.e., the number of equivalent lost full power hour hours associated with the component outage. This is calculated as a function of the derate and the amount of time required to restore the plant to 100% power. The time is in turn a function of the "mean time to repair the equipment", plus the "heat up time" (to restore the plant to 20% power, when the plant is synchronized to the grid), plus the time required to go from 20% to 100% power.
5. Cutsets containing only components not associated with the switchyard were deleted using CAFTA's "Delete term" tool. In this manner, cutsets associated with the turbine generator were removed (that system is evaluated separately, and the findings are contained in the Generator GRA document CNS-GRA-GENERATOR.doc)
6. The result is the amount of "equivalent full time hours" lost as a result of component failures.

6. Results

The yearly frequency for failures in the 345kv switchyard or in the path from the main generator to that switchyard that prevent transmission to the grid is 0.19 due to switchyard associated components only (including the NSST). This translates into one failure of the switchyard to provide power to the transmission lines roughly every 5 years.

When factoring in consequences (in other words, the amount of full power equivalent hours lost as a result of system unavailability), there are a total of roughly 24 effective full power hours (EFPH) per year lost, on average, due to 345kv switchyard related component failures. If full power is equal to 764 MWe, this means that there are an average of 18336 MWh lost per year due to switchyard related issues.

6.1 Top Contributors

The top contributor to the system failure frequency of 0.19 per year is a failure of the main transformer (NERC cause code 3620). Cooper has experienced three maintenance and/or forced

derate/outage events of this type according to NERC. Thus, the cause code failure rate reflects these events through the Bayesian update process. The overall system failure frequency is dominated by this cause code and its plant-specific event occurrences, at 0.18 per year. Thus, this event is by far the dominant contributor to the system failure frequency.

All other event contributors have failure rates that are reflective of the industry-wide (non-Cooper) data updated to reflect the fact that Cooper has experienced no events of those types. The next highest contributors to system failure are much lower in percent contribution to overall system failure frequency when compared to the main transformer contribution. Next on the list of contributors to overall system failure are common cause failures of PCB-3310 and 3312 to remain closed (roughly 0.001 per year) or PCB-3316 and 3318 failing to remain closed (also at .001 per year). An inadvertent fast transfer signal is next in line (again at approximately .001 per year), followed by failure of Auto Transformer T2 (cause code 3600).

When considering mean time to repair and restore power to 100% full power, the main transformer event remains the top contributor; its "equivalent full power hours loss" of 123 hours, multiplied by its yearly frequency, results in an average annual loss of 22.6 effective full power hours.

The next highest contributor to lost hours is the T2 transformer, with an average annual loss of less than 1 hour per year.

6.2 Comparison to Industry

Using the PC-GAR code, a comparison was completed for average MWh lost for all US commercial BWR plants to the value derived from the GRA model. For all outages (disconnections from the grid) due to switchyard causes (cause codes 3600-3621, and 3629), the average number of MWh lost for this set of plants was roughly 26400 per operating year, or about 44% greater than that calculated for Cooper. This difference, although not dramatic, may be from factors such as the generating capacity at plant full power output, Cooper design, etc.

To develop the generic values from NERC, the following assumptions were used:

1. The column "MWh lost per Unit Year" in the PC-GAR output represents all MWh from when the plant first experiences the event and drops from 100% load, until the plant is reestablished at 100% load.

2. Effective Full Power Hours per unit year can be calculated by dividing the total MWh lost per unit year (from all switchyard causes) by the median Net Dependable Capacity (in MW) for the set of plants contained in the database. Net Dependable Capacity is included on the report "Annual Unit Performance" in PC-GAR. For this evaluation and the set of plants chosen (i.e., all U.S. BWRs), this value is 891 MW.

3. To calculate on a "per operating year" basis, the "per unit year" values are multiplied by 8760 (the number of hours in a calendar year) and divided by the

average Unit Service Hours for the population included in the database. From PC-GAR for all U.S. BWRs, 1982-2003, this value is 6407 hours.

Employing these assumptions, the effective full power hours per operating year estimated by using information in PC-GAR for the BWR industry is 29.7 hours. This is similar to the value 24 hours derived from the GRA fault tree and the PRA2GRA code.

The frequency of a plant trip per operating year due to switchyard failures, using NERC data, is 0.25 per year, compared to the value of 0.19 derived using the fault tree. Again, this is very close agreement.

6.3 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the switchyard fault tree.

The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the system to lost generation given the current reliability of components as assumed in the GRA.

The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur if the reliability of the individual components was allowed to degrade significantly.

The most important component to current lost generation is that found in the upper right of the plot, namely, the main power transformer, data point 1 (which contributes about 18 MWh lost per year on average). Other components that impact the lost generation potential of the system, but to a lesser degree, are those in the upper part of the upper left quadrant. Those include the NSST (data point 9), the autotransformer (data point 3), common cause failures of circuit breaker pairs 3310/3312 and 3316/3318 (data points 4 and 5), and the fast transfer relay (data point 6).

The autotransformer (point 3) stands alone and above the other components in the upper left quadrant because it requires a longer time to repair and return to service than the other components it is grouped near.

The remaining components are scattered throughout the lower portion of the upper left quadrant, and throughout the lower left of the four quadrant plot. One exception is data point #2, CRB 1606, that straddles the threshold between the upper left and upper right quadrant. This circuit breaker must open in the event of a fault in the Auburn line in order to isolate the 161kv fault from the 345kv switchyard. Failure to do so is assumed to result in an unisolated fault within the 345kv switchyard, and a loss of the switchyard. The circuit breaker failure is only of concern if there is a fault in the 161kv line, and thus this basic event appears in double element cutsets, which is one reason why its relative importance in the four quadrant plot is as low as it appears.

Components in the lower left quadrant (and those truncated from the analysis) may be candidates for corrective maintenance programs provided they can be shown not to contribute significantly to lost generation in combination. Basic events in the lower left include those that represent individual 345kv lines failures due to various natural causes (ice, wind, fire, lightning). Since any one of the five 345kv lines is assumed to be capable of handling full load, there must be multiple line failures occurring before the 345kv switchyard fails to fulfill its GRA function. Of course there are many reasons why repairing a given line must be accomplished as quickly as possible if it fails, but from a GRA perspective individual line failures are not significant contributors to lost MWh.

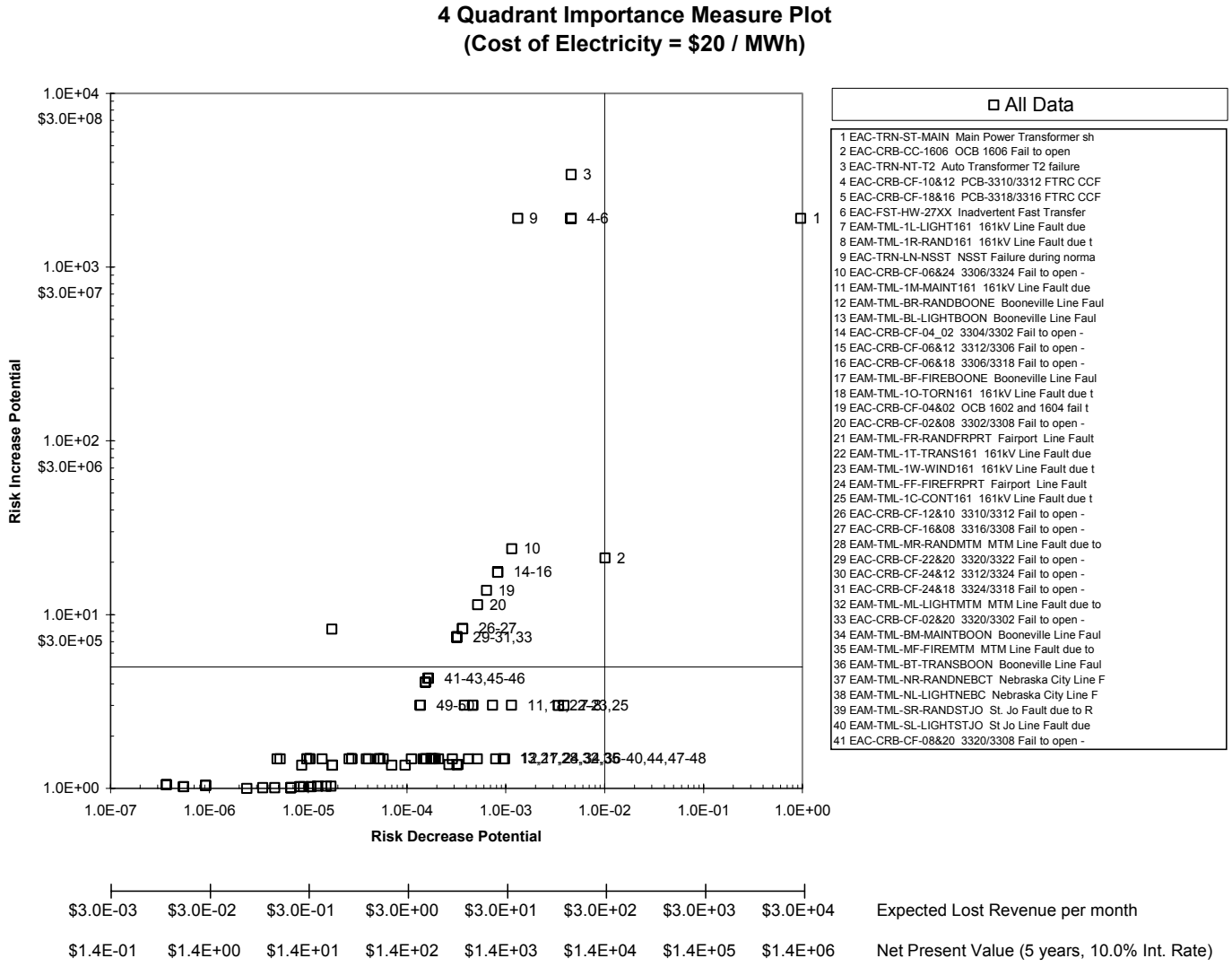


Figure 1
Four Quadrant Plot for 345kv Switchyard

6.4 Uncertainty Analysis

A switchyard uncertainty analysis was performed using UNCERT, a CAFTA add-in program. In the analysis, UNCERT assigns a correlation factor of 1 for all basic events with the same component type and failure mode.

The results of the analysis are shown in Figure 2, following the References section (multiply values in Figure 2 by 1E+06).

#Iterations = 10000
Mean lost generation = 23.1 effective full power hours (EFPH) lost per year
Std Deviation = 12.9 EFPH lost per year

Cumulative Probability	Lost Generation (EFPH)
5%	6.5
50%	21.0
95%	46.9

7. References

Fault Trees, Results, and Database

1. PLANT Centered LOSP 1_04.caf (original switchyard model), last saved December 14, 2004
2. EOOS ac sequence mitig1_045272.caf (from grid stability study), August 3, 2004
3. CNSGRASwyrdGenSWS4-7-05.rr
   4/7/2005 02:27:38 PM
4. No 345KV Switchyard BASIC EVENTS 4-7-05.txt
   4/7/2005 02:17:20 PM
5. No 345KV Switchyard for GRA 3-28-05.caf
   3/29/2005 01:25:32 PM
6. No 345KV Switchyard for GRA 4-7-05.cut
   3/29/2005 01:02:34 PM
7. No 345KV Switchyard for GRA FINAL - ONLY SWITCHYARD EVENTS - CONVERTED 4-7-05.cut 4/7/2005 02:25:10 PM
8. No 345KV Switchyard for GRA MTTR 4-7-05.cut
   4/7/2005 02:21:30 PM
9. Non-Switchyard cutsets for Delete Term 4-7-05.cut
   4/7/2005 02:20:40 PM
10. Switchyard 4 Quad Plot 4-7-05.xls
    3/29/2005 05:02:44 PM
11. UNCERT Log File No 345KV Switchyard for GRA 4-7-05.txt
    3/29/2005 05:03:30 PM

12. CNS Switchyard NERC bayes-gamma March 2005.xls

PC-GAR (NERC) Spreadsheets

1. 11-AnnualUnitPerformance 1982 All without CNS 3-15-05.xls 3/15/2005 08:44:22 AM
2. 11-AnnualUnitPerformance 1983 All without CNS 3-15-05.xls 3/15/2005 08:48:24 AM
3. 11-AnnualUnitPerformance 1984 All without CNS 3-15-05.xls 3/15/2005 09:10:00 AM
4. 11-AnnualUnitPerformance 1985 All without CNS 3-15-05.xls 3/15/2005 09:12:48 AM
5. 11-AnnualUnitPerformance 1986 All without CNS 3-15-05.xls 3/15/2005 09:14:40 AM
6. 11-AnnualUnitPerformance 1987 All without CNS 3-15-05.xls 3/15/2005 09:16:28 AM
7. 11-AnnualUnitPerformance 1988 All without CNS 3-15-05.xls 3/15/2005 09:17:56 AM
8. 11-AnnualUnitPerformance 1989 All without CNS 3-15-05.xls 3/15/2005 09:19:52 AM
9. 11-AnnualUnitPerformance 1990 All without CNS 3-15-05.xls 3/15/2005 09:21:18 AM
10. 11-AnnualUnitPerformance 1991 All without CNS 3-15-05.xls 3/15/2005 09:22:42 AM
11. 11-AnnualUnitPerformance 1992 All without CNS 3-15-05.xls 3/15/2005 09:24:04 AM
12. 11-AnnualUnitPerformance 1993 All without CNS 3-15-05.xls 3/15/2005 12:02:14 PM
13. 11-AnnualUnitPerformance 1994 All without CNS 3-15-05.xls 3/15/2005 12:07:18 PM
14. 11-AnnualUnitPerformance 1995 All without CNS 3-15-05.xls 3/15/2005 02:29:20 PM
15. 11-AnnualUnitPerformance 1996 All without CNS 3-15-05.xls 3/15/2005 02:31:58 PM
16. 11-AnnualUnitPerformance 1997 All without CNS 3-15-05.xls 3/15/2005 04:40:10 PM
17. 11-AnnualUnitPerformance 1998 All without CNS 3-15-05.xls 3/15/2005 05:00:38 PM
18. 11-AnnualUnitPerformance 1999 All without CNS 3-15-05.xls 3/15/2005 05:10:54 PM
19. 11-AnnualUnitPerformance 2000 All without CNS 3-15-05.xls 3/15/2005 05:13:52 PM
20. 11-AnnualUnitPerformance 2001 All without CNS 3-15-05.xls 3/15/2005 05:16:04 PM
21. 11-AnnualUnitPerformance 2002 All without CNS 3-15-05.xls 3/15/2005 05:33:10 PM

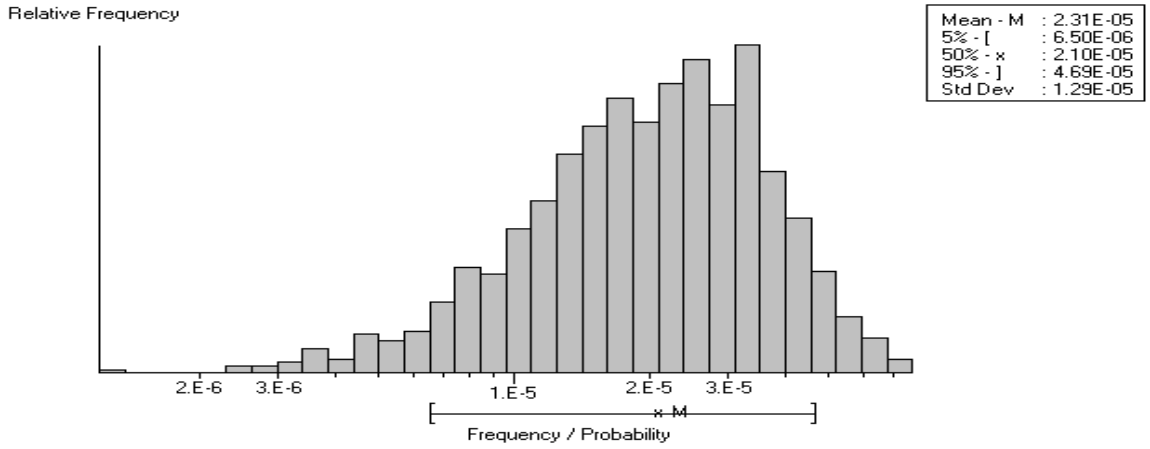
22. 11-IndCauseCodeTotals 1982 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:46:54 AM
23. 11-IndCauseCodeTotals 1983 Switchyard All without CNS 3-15-05.xls 3/15/2005 09:11:48 AM
24. 11-IndCauseCodeTotals 1984 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:23:02 PM
25. 11-IndCauseCodeTotals 1985 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:22:52 PM
26. 11-IndCauseCodeTotals 1986 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:24:04 PM
27. 11-IndCauseCodeTotals 1987 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:28:28 PM
28. 11-IndCauseCodeTotals 1988 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:29:36 PM
29. 11-IndCauseCodeTotals 1989 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:30:24 PM
30. 11-IndCauseCodeTotals 1990 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:31:18 PM
31. 11-IndCauseCodeTotals 1991 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:32:08 PM
32. 11-IndCauseCodeTotals 1992 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:32:48 PM
33. 11-IndCauseCodeTotals 1993 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:33:32 PM
34. 11-IndCauseCodeTotals 1994 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:34:40 PM
35. 11-IndCauseCodeTotals 1995 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:36:32 PM
36. 11-IndCauseCodeTotals 1996 Switchyard All without CNS 3-15-05.xls 3/15/2005 08:36:22 PM
37. 11-IndCauseCodeTotals 1997 Switchyard All without CNS 3-15-05.xls 3/15/2005 04:41:52 PM
38. 11-IndCauseCodeTotals 1998 Switchyard All without CNS 3-15-05.xls 3/15/2005 05:01:40 PM
39. 11-IndCauseCodeTotals 1999 Switchyard All without CNS 3-15-05.xls 3/15/2005 05:12:08 PM
40. 11-IndCauseCodeTotals 2000 Switchyard All without CNS 3-15-05.xls 3/15/2005 05:14:52 PM
41. 11-IndCauseCodeTotals 2001 Switchyard All without CNS 3-15-05.xls 3/15/2005 05:17:18 PM
42. 11-IndCauseCodeTotals 2002 Switchyard All without CNS 3-15-05.xls 3/15/2005 05:34:08 PM
43. 1-CompCauseCodeLosses - transformers - all US.xls 1/4/2005 03:15:14 PM
44. 1-IndCauseCodeTotals - transformers - all US.xls 3/15/2005 10:39:06 PM

45. 1-IndCauseCodeTotals ALL US, SWITCHYARD 1-6-05.xls 3/15/2005 04:43:20 PM
46. 2-IndCauseCodeTotals COOPER switchyard 1983 3-15-05.xls 3/15/2005 08:34:34 AM
47. 2-IndCauseCodeTotals COOPER switchyard 2000 3-15-05.xls 3/15/2005 08:40:02 AM
48. 2-IndCauseCodeTotals COOPER switchyard 2002 3-15-05.xls 3/15/2005 08:41:18 AM

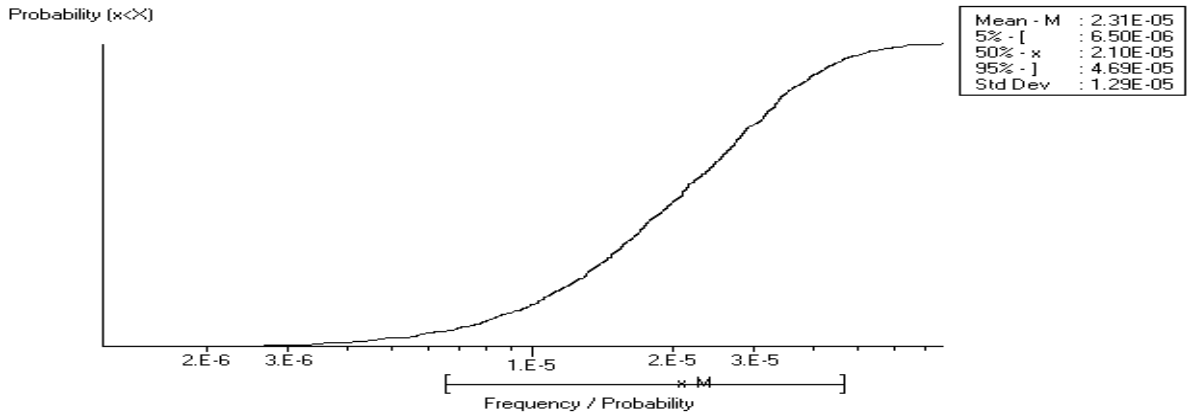
Other

1. North American Electric Reliability Council (NERC), "pc-GAR for Windows", release 2.06 v26, 2004
2. Applied Reliability Engineering, Inc. (AREI), "PRA2GRA", April 7, 2005
3. Electric Power Research Institute (EPRI), "CAFTA", version 5.1a, 2003
4. AREI, "Probabilistic Safety Assessment System Analysis Notebook, Cooper Nuclear Station, Electric Power System – Switchyard (Plant-Centered Loss Of Offsite Power)," January 26, 2004
5. Data Systems and Solutions (DS&S), "Method to Monitor Nuclear Power Risk from Transmission Grid Conditions," Rev. 0, September 30, 2004
6. Line fault probabilities 1-3-05.xls (based on spreadsheet from DS&S, supporting grid stability study, first created September 2004), January 3, 2005
7. Applied Reliability Engineering, Inc. (AREI), "SetEventStates.exe", March 2005.
8. Nuclenor, Iberdrola, and Data Systems and Solutions, "Uncert for Windows", Version 2.3a, 2002.

Density Function



Cumulative Function



(NOTE: Multiply all values by 1E+06 to obtain actual results.)

Figure 2
Uncertainty Analysis Results – Switchyard, 100% Derate

Turbine Equipment Cooling

Rev. 0 9/15/05

1. System Function

GRA Function: Turbine equipment cooling provides a cooling heat sink for various turbine and generator heat loads.

2. Success/ Failure Criteria

Plant Disconnected from Grid – 100% Derate

The success criteria of the TEC function is to ensure that heat loads are provided with adequate cooling to maintain operation of supported systems . This criteria is met by providing closed loop cooling at adequate temperatures and flow rates to meet all cooling requirements.

For the purposes of the Generation Risk Assessment (GRA), failure of any component that results in the inability to provide cooling at required flow rates and temperatures results in a plant trip and a 100% derate condition.

TEC requires the successful operation of the following support systems:

- AC power
- Instrument Air
- Service Water

Plant Derate - Derates Less Than 100%

Plant derates less than 100% are not considered in this assessment. This is based on the fact that power reductions are not effective in mitigation of the consequences caused by the loss of the turbine equipment cooling function. Thus partial derates do not prevent plant trips.

3. Fault Tree Modeling

3.1 Development of Fault Tree

Fault trees were developed using existing TEC system fault trees contained in the Cooper Nuclear Station (CNS) probabilistic safety assessment (PSA) model.

TEC system fault trees contained in the CNS 2005 average test and maintenance PSA model were extracted and converted to generation risk assessment fault trees.

Conversion of PSA fault trees to allow quantification of generation risk was done using PRA2GRA cutset conversion software. Overall, this conversion results in the quantification of the expected number of full power hours lost per year as a result of TEC system failures. PRA2GRA was utilized to perform the following tasks:

1. Generation of PSA TEC system cutsets that exclusively contain at least one basic event that would result in a loss of electrical generation. Generally, this involves elimination of all cutsets that contain only demand type failures. PSA TEC system cutsets that credited use of standby AC power systems were also eliminated since these cutsets are associated with plant trip conditions and not applicable for loss of generation quantification.
2. Addition of gates to reflect summer and winter operations. Specifically, summer operations consist of conditions where loss of any one of four pumps or one of two heat exchangers could result in a plant trip. Winter operations consist of conditions where at least 3 of 4 pumps or 2 of 2 heat exchangers must be lost before tripping the plant.
3. Conversion of the PSA, TEC, loss of generation cutsets from 24 hour mission times to 365 day mission times.
4. Identification of cutsets were repair could be credited and assigning repair time to recovery factors for those cutsets. This involved identification of cutsets that had two (2) or more run time failures and multiplying those cutset by a mean time to repair value.
5. Quantification of the expected number of full power hours lost as a result of TEC failures. This is quantified by multiplying each TEC loss of generation cutset by the resulting time required to recover from a derated condition (100% derate for TEC).
6. The resulting GRA fault trees were reviewed with a system engineer. This review verified that the GRA fault tree was valid. However the system engineer requested that flow/temperature control valves for TEC cooling loops be modeled. These control valves and their controlling instrumentation were added tot the fault tree.

Section 5 of this report details the cutset processing steps used to quantify TEC system cutsets.

3.2 Modeling Assumptions and Comments

1. For the GRA, the exposure time of interest for all components is one year. For the base model, operating times of 24 hours were assigned to the data, which were then updated to a one year exposure time using the PRA2GRA conversion code.
2. It is assumed that any event that results in a full plant derate (100% power) leading to cold shutdown causes the plant to implement the 3 day outage plan. This means that all cold shutdown events have minimum outage times of 72 hours before the plant begins to heat up to return to power. Thus, even if a component has a mean time to repair of less than 72 hours, the plant remains shutdown for 72 hours to complete other repairs.
3. See Section 4 for assumptions specific to data.

4. System Reliability Data

Failure rates (failure per hour) for all components included in the CNS PSA database were used.

5. Cutset Post Processing

The following was performed on the CNS PSA TEC system cutsets to obtain the final system top event frequency.

1. The PRA2GRA code was used to convert mission times from 24 hours to 1 year.

2. The PRA2GRA code also assigned "mean time to repair" values, based on assigned values.

3. PRA2GRA was then used to assign consequences, i.e., the number of equivalent lost full power hour hours associated with the component outage. This is calculated as a function of the derate and the amount of time required to restore the plant to 100% power. The time is in turn a function of the "mean time to repair the equipment", plus the "heat up time" (to restore the plant to 20% power, when the plant is synchronized to the grid), plus the time required to go from 20% to 100% power.

4. A code called SetEventStates (developed by AREI – see References) was used to help produce cutsets containing only non-TEC system basic events. These cutsets were then deleted from the results of the PRA2GRA evaluation, using CAFTA's "Delete Term" tool, to arrive at the final set of cutsets, namely, those containing at least one TEC system basic event.

5. The result is the amount of "equivalent full time hours" lost as a result of component failures associated with the TEC system.

6. Results

The yearly frequency for TEC system unavailability resulting in a 100% derate, as modeled for the GRA, is 2.2E-01. This failure rate is approximately one failure every 4.5 years. This is a higher rate than that experienced at CNS

When factoring in consequences (in other words, the amount of full power equivalent hours lost as a result of system unavailability), there are a total of 27.4 efph (equivalent full power hours) per year lost, on average, due to TEC system component failures resulting in 100% derates. Full power operations at CNS is equal to 809 Mwe. Thus, there is a potential average loss of 2216MWh per year due to TEC system related issues.

It must be noted that failures in support systems, such as Service Water, Instrument Air, AC power, etc., increase the frequency of TEC system unavailability. However, those support systems are or may be treated separately within the GRA, and their impacts should be addressed within the context of those evaluations. The results and discussions here and in subsequent sections focus solely on components explicitly identified as being part of the TEC system.

6.1 Top Contributors

100% Derate

The top contributor to system unavailability resulting in a 100% derate is failures of a TEC motor driven pump during summer operations. All cutsets that contain single pump motor failure events represent a probability of 7.5E-02 per year (9.22 EFPH/yr).

6.2 Comparison to Industry

Using the Closed Cooling Water cause codes within NERC, the US BWR population has experienced an average loss of approximately 0.1 EFPH per year, with an outage (shutdown) frequency of 2E-3 per operating year. These values are significantly lower than the values calculated for CNS using the GRA models.

One possible reason for this difference is that for some period of each year the TEC becomes essentially a single point vulnerability system, i.e., a failure of any of the four pumps, or either of the two heat exchangers, will result in a system and plant shutdown. Other plants may not have similar situations in which apparent redundancy is reduced to a series of single failure points. A more detailed review of industry data may verify this postulated explanation.

6.3 Four Quadrant Plot

Figure 1 presents a two dimensional plot of importance rankings for components modeled within the TEC fault tree.

> The x-axis of the plot (risk decrease potential) indicates the contribution of individual components within the system to lost generation given the current reliability of components as assumed in the GRA.
>
> The y-axis of the plot (risk increase potential) indicates the potential increase in lost generation that could occur if the reliability of the individual components was allowed to degrade significantly.

The four quadrant plot was reviewed by the system engineer to determine if existing preventative maintenance (PM) for the TEC systems was adequate. Three conclusions were drawn:

1. No unwarranted PM was found. This was determined by ensuring that any components in the lower left quadrant of the plot did not have significant PM resources applied to them.

2. PM activities may be developed for thermocouples installed in the temperature control loops for TEC. At the time of the GRA evaluation those components had a run to failure approach for maintenance. However, the results of the GRA clearly indicate the importance of thermocouple reliability to minimizing plant trips and lost generation.

3. TEC pump reliability is important in minimizing plant trips. At the time of the evaluation a predictive maintenance program (vibration, thermography) was being used to ensure reliability. This may not minimize generation loss. Predictive maintenance is performance based and may result in the requirement for pump change-out during the summer. This change-out would be unadvisable since a plant shutdown would be required. Based on this, preventative maintenance will be considered in the future to ensure that the pumps are reliable throughout summer months.

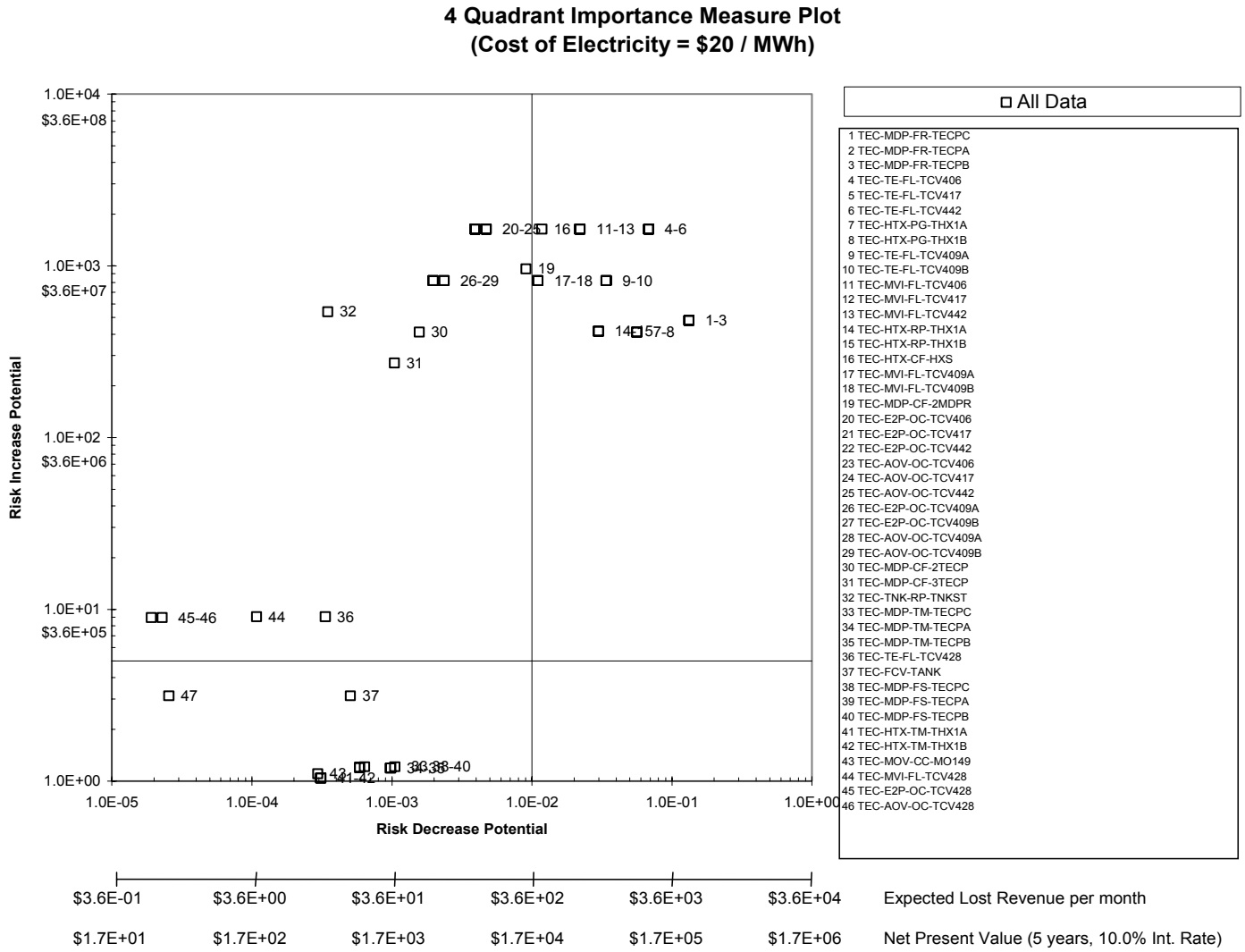


Figure 1
Four Quadrant Plot for TEC System

6.4 Uncertainty Analysis

A TEC system uncertainty analysis was performed using UNCERT, a CAFTA add-in program. In the analysis, UNCERT assigns a correlation factor of 1 for all basic events with the same component type and failure mode.

The results of the analysis are shown in Figure 2, following the References section (multiply values in Figure 2 by 1E+06).

#Iterations = 10000
Mean lost generation = 27.3 effective full power hours (EFPH) lost per year
Std Deviation = 17.4 EFPH lost per year

Cumulative Probability	Lost Generation (EFPH)
5%	15.1
50%	22.5
95%	54.6

7. References

Cooper Operating Procedures

1. 2.1.10 - Station Power Changes
2. 2.1.4.3 - Power Reduction to Less Than 25%
3. 5.2.AIR – Loss of TEC

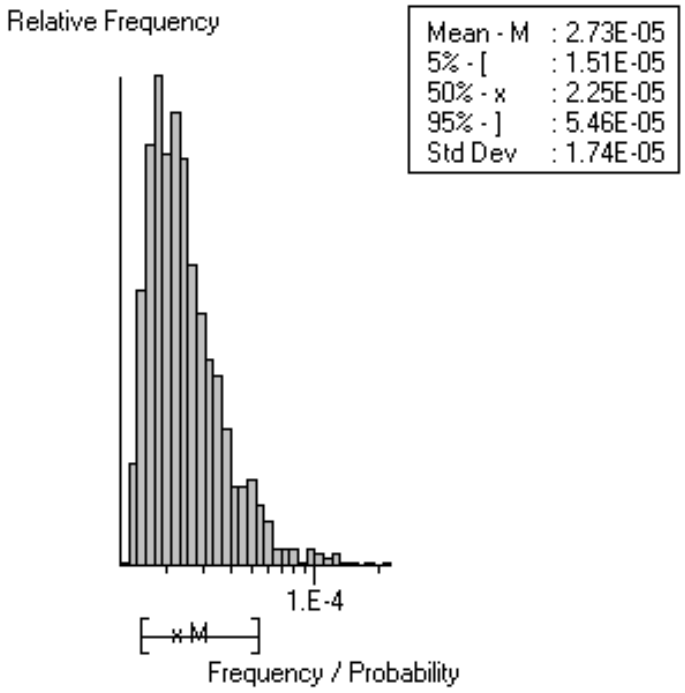
Cooper Operator Training – Lesson Plan

1. COR001701R17-L-OPS TEC
2. COR001701R17-S-OPS TEC

Fault Trees, Results, and Database

1. TEC.caf, CNS PSA, TEC System Fault Tree, Average Test and Maintenance Model, 2005
2. IASpra2001a.BE, CNS PSA Model Database, Average Test and Maintenance Model, 2005
3. pra2001a-gra_ias.rr, GRA Model Database, 10/25/05, 3624 kB
4. pra2gra.exe, Executable - Conversion of PSA Fault Trees to GRA Cutsets
5. SetEventStates.exe, Executable – Basic Event True/False Setting
6. TECPRA2005.caf, CAFTA GRA fault tree, 8/22/05, 25 kB
7. TECGRAJUNE2005.cut, GRA cut sets, 10/6/2005, 296 kB

Density Function



Cumulative Function

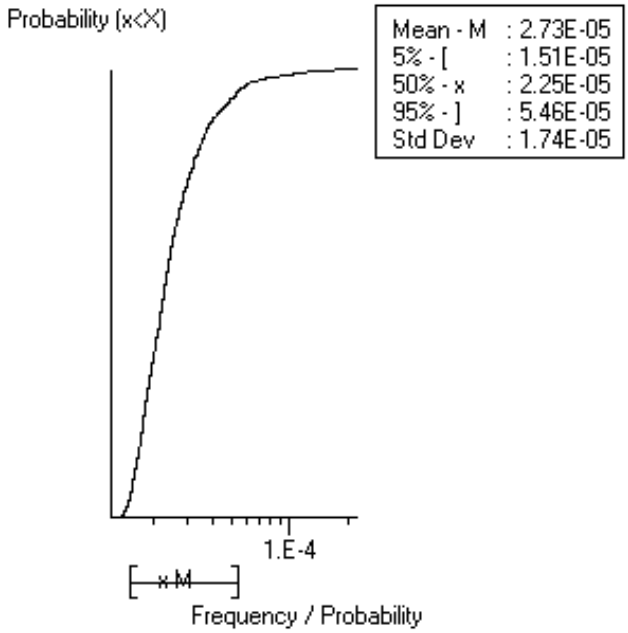


Figure 2
Uncertainty Analysis Results – TEC, 100% Derate (Equivalent Full Power Hours (EFPH))

Note: Multiply all results by 1E+06

B
BASIC EVENTS USING NERC DATA

Table B-1 contains a listing of basic events for which NERC data was used to estimate failure rates for the CNS GRA.

Table B-1
NERC-Derived Failure Rates Used in CNS GRA

Event Component Type	Description as Used in System Model (Fault Tree)	Basic event IDs in fault tree	NERC Cause Code	NERC-derived failure rate (per hour)
Switchyard circuit breaker or disconnect	Test or maintenance	EAC-CRB-TM-3302 EAC-CRB-TM-3304 EAC-CRB-TM-3306 EAC-CRB-TM-3308 EAC-CRB-TM-3320 EAC-CRB-TM-3322 EAC-CRB-TM-3324 EAC-CRB-TM-3326 EAC-CRB-TM-MTM	3611	2.1E-6
Switchyard disconnect switch	Disconnect Failure (fails in open position)	EAC-DIS-HW-33021 EAC-DIS-HW-33022 EAC-DIS-HW-33041 EAC-DIS-HW-33042 EAC-DIS-HW-3305L EAC-DIS-HW-33061 EAC-DIS-HW-33062 EAC-DIS-HW-33081 EAC-DIS-HW-33082 EAC-DIS-HW-33101 EAC-DIS-HW-33102 EAC-DIS-HW-33121 EAC-DIS-HW-33122 EAC-DIS-HW-33161 EAC-DIS-HW-33162 EAC-DIS-HW-33181 EAC-DIS-HW-33182 EAC-DIS-HW-33201 EAC-DIS-HW-33202 EAC-DIS-HW-33221 EAC-DIS-HW-33222 EAC-DIS-HW-33241 EAC-DIS-HW-33242	3619	3.7E-6

Event Component Type	Description as Used in System Model (Fault Tree)	Basic event IDs in fault tree	NERC Cause Code	NERC-derived failure rate (per hour)
		EAC-DIS-HW-3440L EAC-DIS-HW-3499L EAC-DIS-HW-3501L EAC-DIS-HW-3517L		
NSST	Failure during normal operation	EAC-TRN-LN-NSST	3621	9.99E-6
Auto Transformer T2	Transformer failure	EAC-TRN-NT-T2	3600	3.2E-6
Main power transformer	Transformer short/fault - requires switchyard isolation	EAC-TRN-ST-MAIN	3620	2.7E-5
NSST or NSST disconnects	NSST, 3312-D1, 3310-D2 out of service due to MPT (NSST) Test/maintenance	EAC-TRN-TM-NSST	3621	1.4E-6
Disconnects or Auto Transformer T2	1602-D2 ,1604-D1,3318-D1,3316-D2,T2 open: T2 T/M	EAC-TRN-TM-T2	3600	1.4E-6
CRB	CRB-3326 or Disconnects out for Test/Maintenance	EAM-CRB-TM-3326	3611	2.1E-6
H2 coolers	Cooler failure	H2_-CLR-FF-611	4611	7.3E-7
Other H2 system problems	Other H2 Problems	H2_-MSC-FF-619	4619	1E-6
H2 cooling system piping and valves	Failure	H2_-PIP-FF-610	4610	1.8E-6
H2 seals	Failure	H2_-SLS-FF-613	4613	1E-6
Bearings and lube oil system	Failure	LO_-GEN-FR-550	4550	7.2E-7
Main shaft oil pump	Failure (assume similar to cause code 4550)	LO_-PMP-FR-MSOP	4550 assumed	--
Generator (H2) seal oil system and seals	Failure	LOG-OIL-HW-640	4640	7.2E-7
End belts and bolting	Failure	TG_-BLT-FF-580	4580	3.6E-7
Generator Brushes and brush rigging	Failure	TG_-BSH-FF-540	4540	3.6E-7
Other Cooling System	Failure	TG_-CLR-XX-650	4650	1.1E-6
Generator Output Breaker	Failure (fails in open position)	TG_-CRB-XX-810	4810	3.6E-7

Event Component Type	Description as Used in System Model (Fault Tree)	Basic event IDs in fault tree	NERC Cause Code	NERC-derived failure rate (per hour)
Other Exciter Problems	Failure	TG_-EXC-FF-609	4609	6.2E-6
Exciter Drive – Motor	Fails to function	TG_-EXC-FR-600	4600	1E-8
Exciter Cummutator and Brushes	Fail to function	TG_-EXC-XX-602	4602	3.6E-7
Exciter Field Rheostat	Fail to function	TG_-EXT-FF-601	4601	3.6E-7
Generator Vibration	Excessive vibration	TG_-GEN-VB-560	4560	1E-8
Generator Main Leads	Fail to function (e.g., short)	TG_-LED-FF-800	4800	1.4E-6
Generator Metering Devices	Fail to function	TG_-MET-FF-710	4710	1E-8
Other Generator Controls and Metering	Fail to function	TG_-MSC-FO-750	4750	3.6E-7
Other Miscellaneous Generator Issues	Fail to function	TG_-MSC-ZZ-899	4899	1.4E-6
Generator Protection (Trip) Devices	Fail to function	TG_-REL-FO-740	4740	7.3E-7
Generator Rotor Windings	Failure (e.g., short)	TG_-RTR-FF-500	4500	3.6E-7
Gen. Stator Windings, Bushings, and Terminals	Fail to function	TG_-STR-FF-520	4520	1.1E-6
Generator Synchro. Equipment	Fail to function	TG_-SYN-FF-720	4720	3.6E-7
Generator Voltage Control	Fail to function	TG_-VCL-FF-700	4700	6.99E-6
Generator Current and Potential Transformers	Fail to function	TG_-XMR-FF-730	4730	7.3E-7

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.

Printed on recycled paper in the United States of America

The Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI), with major locations in Palo Alto, California, and Charlotte, North Carolina, was established in 1973 as an independent, nonprofit center for public interest energy and environmental research. EPRI brings together members, participants, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of electricity generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States. International participation represents nearly 15% of EPRI's total research, development, and demonstration program.

Together...Shaping the Future of Electricity

Program:

Nuclear Power

1011924

ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue, Palo Alto, California 94304-1395 • PO Box 10412, Palo Alto, California 94303-0813 USA

800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com