NUREG/CR-4462
PNL-5690

17

A Ranking of Sabotage/Tampering Avoidance Technology Alternatives

Prepared by W. B. Andrews, A. S. Tabatabai, T. B. Powers, P. M. Daling, B. A. Fecht, B. F. Gore, T. D. Overcast, W. R. Rankin, R. E. Schreiber, J. J. Tawil

Pacific Northwest Laboratory
Operated by
Battelle Memorial Institute

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-4462
PNL-5690

A Ranking of Sabotage/Tampering Avoidance Technology Alternatives

Manuscript Completed: November 1985
Date Published: January 1986

Prepared by
W. B. Andrews, A. S. Tabatabai, T. B. Powers, P. M. Daling, B. A. Fecht,
B. F. Gore, T. D. Overcast, W. R. Rankin, R. E. Schreiber, J. J. Tawil

Pacific Northwest Laboratory
Richland, WA 99352

Prepared for
Division of Systems Integration
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN B2548

ABSTRACT

Pacific Northwest Laboratory conducted a study to evaluate alternatives to the design and operation of nuclear power plants, emphasizing a reduction of their vulnerability to sabotage. Estimates of core melt accident frequency during normal operations and from sabotage/tampering events were used to rank the alternatives. Core melt frequency for normal operations was estimated using sensitivity analysis of results of probabilistic risk assessments. Core melt frequency for sabotage/tampering was estimated by developing a model based on probabilistic risk analyses, historic data, engineering judgment, and safeguards analyses of plant locations where core melt events could be initiated. Results indicate the most effective alternatives focus on large areas of the plant, increase safety system redundancy, and reduce reliance on single locations for mitigation of transients. Less effective options focus on specific areas of the plant, reduce reliance on some plant areas for safe shutdown, and focus on less vulnerable targets.

EXECUTIVE SUMMARY

Pacific Northwest Laboratory (PNL) has conducted a study that evaluates alternatives to the basic design of nuclear power plants, based on reducing plant vulnerability to sabotage. This study was completed for the U.S. Nuclear Regulatory Commission (NRC) in support of Generic Safety Issue A-29, Nuclear Power Plant Design for the Reduction of Vulnerability to Sabotage (U.S. NRC 1978).

The NRC identified a total of 25 sabotage and tampering avoidance technology (STAT) alternatives to be ranked in this study. These alternatives cover a wide range of potential plant design and operational changes. Some represent alternatives for future plant designs. Others are possible design changes for all plants to reduce the threat from persons with access to plant equipment (insiders). The remaining alternatives were selected from NUREG/CR-2585, Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection (U.S. NRC 1982a), as examples of damage control measures to mitigate the effects of sabotage.

SCOPE

The PNL study is an assessment of core melt frequency (CMF) for the purpose of relative comparisons between STAT alternatives. Results of probabilistic risk assessments (PRAs), vital area studies, and historic data were used to complete the analysis. Design-basis threat assessment results were not used because of their lack of frequency information, and physical protection simulations were judged to be too resource-intensive and thus were not used in the study.

The approach developed assumes that STAT can reduce the frequency of accident initiating events and can improve the capability of the plant to mitigate transients prior to core damage. The effects of changes in plant operation and design were measured in terms of reduced CMF from accidents and deliberate acts of sabotage and tampering. The methodology is an extension of the CMF reduction analysis approach developed in another NRC project, the Prioritization of Generic Safety Issues (NUREG-0933, U.S. NRC 1983a).

Core melt frequency was chosen to measure risk due to the limitations imposed by current models of nuclear power plant resistance to sabotage and by PRAs. Vital area models measure combinations of equipment failures as to their potential for causing any release of radioactivity, with little or no differentiation based on release size or composition. PRAs consider only acts leading to core melt. Thus, release of material from storage locations at power plants or diversion and dispersal of material at other locations were not considered.

Major simplifications have been required in development of the methodology to produce an approach that can be implemented with the resources available for the ranking of STAT alternatives. First, historic acts of sabotage and tampering data were used to define the threat to be evaluated. Data on sabotage and tampering are very limited in scope. Data for power reactors, test reactors, and fuel cycle facilities were combined to expand the available

experience. The combined data is believed to be a reasonable representation of the scope of actions that have occurred. Second, no rigorous uncertainty calculations were performed. This project focused instead on the development of point estimates. Sensitivity analyses of critical assumptions were considered adequate to rank STAT alternatives. A third means of simplifying the approach was to use existing risk results for the evaluation of future plants. This simplification may have introduced significant errors, since future plants are likely to have many differences in addition to those introduced for the purposes of avoiding sabotage and tampering. Finally, modification of the NRC definition of sabotage was necessary. In the context of PRA, a core melt event is possible only if both an accident initiator and equipment failures occur. Initiation of accident sequences was defined in this study as an act of sabotage. Core melt probabilities given an accident sequence can then be described in terms of both deliberate and random equipment failures. Acts that do not initiate accident sequences were defined as tampering. Tampering requires that a random accident initiator take place to cause core melt.

Simplifications required to complete the analysis limit its applicability to situations in which relative results are adequate. The study results are not intended to be used for absolute evaluations of public risk from sabotage and tampering.

APPROACH

The analysis was performed in three steps:

1. Base levels of CMF attributable to sabotage and tampering were determined.

2. The effectiveness of each STAT alternative in reducing CMF from sabotage and tampering and in normal operations was evaluated.

3. The CMF reductions were calculated and the 25 STAT alternatives were ranked.

Sabotage and tampering contributions to CMF were added to a PRA based model of plant risk using information from the following three sources:

- vital area studies (safeguarded information that is not publicly available)
- sabotage/tampering threat model
- a PRA study resolvable to the cut set level.

Vital area studies are safeguarded analyses that indicate minimal combinations of locations in which equipment essential to the prevention of core melt and radioactive material release are installed. The sabotage/tampering threat model was developed by the study. Based on historic acts of damage in NRC and U.S. Department of Energy (DOE) facilities, it calculates the frequency and probability of damage associated with various types of actions.

A base CMF was determined by calculating the frequency attributable to sabotage and tampering and adding it to PRA results. This was done by first selecting a specific vulnerable location from the vital area studies. Second,

the affected equipment and the probability of equipment failure given an attack were determined using the threat model. Finally, the equipment failure probabilities and accident initiator frequencies were modified in the PRA model and an adjusted-case CMF was calculated. Results of PRAs for Grand Gulf and Arkansas Nuclear Unit-1 (ANO-1) (U.S. NRC 1982) were used in the analysis to represent BWRs and PWRs, respectively.

The CMF reduction due to implementation of a STAT alternative is the difference between the base-case and the adjusted-case CMF. These cases were estimated based on judgments by PNL staff of the effectiveness of each alternative in reducing sabotage and tampering contributors.

The 25 alternatives were ranked based on prioritization categories (high, medium, low/drop priorities from NUREG-0933 [U.S. NRC 1983a]). The use of the CMF categories developed in NUREG-0933 was a convienience for presentation. The STAT alternatives could also be ranked on a purely relative basis, independent of NUREG-0933 criteria. Changes in or deletion of assumptions used in the CMF calculations could result in significant changes in the magnitude of CMF reduction. This would change the divisions between high, medium and low/drop priority categories, but would have little effect on the relative ranking.

RESULTS

Results include the development of a threat model based on historic events and the evaluation of the 25 STAT alternatives. Results of the threat model are summarized in Table S.1. Significant events are a fraction of actual events in which potential or actual plant damage occurred. The fractional weights were developed using judgment and data on observed damage levels. Tampering is the most likely act, with vandalism and arson the most likely form of attack. Sabotage is much less likely, based on historic data.

TABLE S.1. Summary of the Facility Threat Model

Act	Percent of Significant Events
Tampering	
Bombs	2.4
Intrusion	6.9
Vandalism	73
Arson	13
Sabotage	
With tampering	0.22
Without tampering	2.2

Several conclusions can be drawn from the threat model:

- Intrusion is a minor contributor to plant threat. Damage done by intruders has also been minor.
- Vandalism is a major contributor to plant threat. The majority of the more serious of these acts stem from employee malcontent, from mental illness, and from political idealism.
- The sabotage value is based on transients initiated to embarrass plant management.
- Sabotage-with-tampering frequencies are based on one act at a test reactor. Data for this category are very limited and may overestimate the threat for power reactors.

Estimates of the contributions to CMF from sabotage and tampering are shown in Table S.2. The results indicate that, based on CMF, accident initiation without equipment damage (sabotage) has not had a significant effect on safety. Based on a single act by insiders, sabotage with tampering is significant. However, as stated above, the absolute magnitude of the sabotage-with-tampering CMF is highly uncertain, based on the methodology developed in the PNL study. Tampering alone is between one and two orders of magnitude less important than sabotage with tampering. Assumptions made in the selection of a primary target indicate that protected areas may make as great a contribution to plant CMF vulnerabilities as areas with augmented physical protection (e.g., "important areas").

TABLE S.2. Sabotage and Tampering CMF Contribution

Scenario	Core Melt Frequency Contribution, events/reactor year	
	Grand Gulf	ANO-1
Tampering (primary target indicated)		
Protected location	3E-6	3E-5
Important location	9E-7	3E-5
Sabotage only	1E-7	3E-7
Sabotage with tampering	2E-4	2E-4

Results of the CMF reduction assessment for the 25 STAT alternatives are shown in Table S.3. The rationale for the rankings was based on NUREG-0933. Each STAT alternative was ranked based on its potential for CMF reduction in normal operations, tampering, and sabotage with tampering. The values in Table S.3 are the highest of either the tampering or sabotage-with-tampering category. The nominal overall ranking was based on results for sabotage and tampering categories. Normal-operation CMF reductions were used to raise the rankings by

up to two levels (i.e., low to high) if the values were significant. Alternative 20 was reduced by one level due to a predicted increase in CMF during normal operations. Alternative 4, dealing with the SNUPPS design, was not considered due to limited information.

The trend in the overall ranking indicates that high priority alternatives focus on wide areas of the plant, provide significant increases in redundancy, and reduce the reliance on the control room for the mitigation of accidents. Medium priority alternatives focus on smaller areas of the plant, are effective in increasing the redundancy in a few systems, and reduce reliance on combinations of a small number of locations in the plant. Low/drop priority alternatives focus on systems with little vulnerability or are alternatives that were judged ineffective in reducing potential damage from sabotage and tampering.

TABLE S.3. Prioritization of STAT Alternatives

No.	Sabotage/Tampering CMF Reduction Frequency (1/reactor year)	Title
High Priority		
1	2E-5	Three 100% trains of safety related equipment
2	1E-4	For a BWR--two additional bunkered RCIC pumps For a PWR--two additional bunkered AFW pumps
5	1E-5	Implementation of the two man rule
7	1E-5	Manual/local operation of BWR safety-relief valves
8	2E-6	Feed-and-bleed operation of suppression pool
13	1E-5	Use control rod drive hydraulic system to supply reactor coolant makeup
21	2E-6	Provide cross-connection between Class IE/ non-Class IE
Medium Priority		
6	2E-6	Installation of TV cameras in vital areas
11	2E-7	Use of fire water as source of cooling RHR heat exchangers
12	3E-8	Connect SI pump in series to raise discharge pressure
14	2E-6	Use main condenser pump to provide reactor coolant makeup

injection?

TABLE S.3. (Contd)

No.	Sabotage/Tampering CMF Reduction Frequency (1/reactor year)	Title
15	2E-6	Cross-connect service water with essential service water (ESW)
17	2E-6	Use ESW to directly cool components cooled by CCW
18	2E-6	Provide local pressurizer and SG level indication
19	2E-6	Provide local readouts for SG pressure
24	2E-6	Provide a standby non-Class IE combustion turbine generator
Low/Drop Priority		
3	0	A passive steam condenser for the steam generators of a PWR
9	3E-8	Use of safety-injection (SI) pumps to supply water to steam generators (SGs)
10	0	Provide spring-loaded safety valves for venting steam generators
16	2E-7	Cross-connect fire system and ESW
20	2E-6	Provide emergency AC power to nonsafety related equipment
22	0	Provide multiple DC feeders to DC powered components
23	0	Provide an alternate water source to maintain coolant inventory (PWR)
25	0	Provide capability to place an emergency diesel generator in service without DC power

CONCLUSIONS

This project combined available plant vulnerability models and probabilistic risk assessment to yield a ranking of 25 alternatives for sabotage and tampering mitigation. The results offer an insight different than that available from evaluations using physical protection models. With refinements, the model could be used to evaluate additional alternatives and suggest the development of others.

The results of this study are intended for use in selecting some of the 25 alternatives for additional work in support of resolving Generic Safety Issue A-29. No accurate, absolute measure of sabotage and tampering was developed. Historic data were was used solely for the purposes of scaling the frequency of damage to be, to the extent possible, consistent with PRAs.

Data indicate that most acts of damage in power plants are committed by insiders. Intruders from offsite and unauthorized access to restricted areas by onsite staff are a small part of the acts to date. Insider acts to date cover a wide range of damage. Most acts have had no offsite consequences and there is no evidence of obvious intent to cause them. However, the acts with intent to cause plant damage have been committed by those knowledgeable of the safety systems and with access to sensitive equipment. There are several methods of dealing with this threat. The first, covered to some extent by the 25 STAT alternatives evaluated in this report, is to reduce vulnerabilities through increased operating flexibility and surveillance. The second is the subject of other NRC actions addressing staff qualifications and access to sensitive areas.

Sabotage (initiation of an accident) with concurrent tampering failures of safety equipment is one to two orders of magnitude more important than tampering alone. Sabotage with tampering may also be a significant contributor to core melt accident frequency. STAT alternatives that increase the availability of important equipment to mitigate damage or reduce the opportunity for sabotage from a single or a few locations could be effective in controlling the sabotage-with-tampering threat. Tampering alone is more difficult to control due to the number of options available to a motivated person or persons. Areas of augmented physical protection, if selected on the basis of sabotage, may not optimize prevention of tampering acts.

ACKNOWLEDGMENTS

The contributions of the following team members were essential to the study presented in this report:

W. E. Bickford	Member of review team
P. M. Daling	STAT Alternatives 7, 11, 13, 14, 15, 16, 17, 23, 24, 25
B. A. Fecht	STAT Alternatives 9, 10, 18, 19
B. F. Gore	STAT Alternatives 8, 12, 20, 21, 22
M. R. Guttenberg	Typing
S. E. King	Editing
K. J. Morgan	Typing
T. D. Overcast	Data analysis, STAT Alternatives 5 and 16
T. B. Powers	Normal operations analysis, review team
W. L. Rankin	Data analysis, Issues 5 and 6
R. E. Schreiber	STAT Alternatives 1, 2, 3
A. S. Tabatabai	Normal operations analysis, Sabotage/tampering analysis, review team
J. J. Tawil	Data analysis
J. Young*	PRA consultant, review team

* Energy Incorporated

W. B. Andrews
Project Manager

CONTENTS

FIGURES

TABLES

LIST OF ACRONYMS

ADS	Automatic depressurization system
AFW	Auxiliary feedwater
AFWS	Auxiliary feedwater system
BWR	Boiling water reactor
CC	Component cooling
CCW	Component cooling water
CMF	Core melt frequency
CRDHS	Control rod drive hydraulic system
CST	Condensate storage tank
CTG	Combustion turbine generator
DG	Diesel generator
ECCS	Emergency core coolant system
EDG	Emergency diesel generator
EFIC	Emergency feedwater initiation and control
ESF	Engineered safety feature
ESFAS	Engineered safety feature actuation system
ESW	Essential service water
FWCI	Feedwater coolant injection
HPCI	High pressure coolant injection
HPCS	High pressure core spray
HPI	High pressure injection
HPSI	High pressure safety injection
ICS	Integrated control system
LOCA	Loss of coolant accident
LOOP	Loss of offsite power
LPCI	Low pressure coolant injection
LPCS	Low pressure coolant spray
LWR	Light water reactor
MCS	Main condensate system
MSIV	Main steam isolation valve
NNI	Non-nuclear instrumentation

LIST OF ACRONYMS (contd)

PORV	Power operated relief valve
PRA	Probabilistic risk assessment
PWR	Pressurized water reactor
RCIC	Reactor core isolation cooling
RCS	Reactor coolant system
RHR	Residual heat removal
RPS	Reactor protection system
RWST	Refueling water storage tank
SG	Steam generator
SI	Safety injection
SNUPPS	Standardized nuclear unit power plant system
SRV	Safety relief valve
SSWS	Standby service water system
SW	Service water
TBS	Turbine bypass system

1.0 INTRODUCTION

This report documents a methodology used by Pacific Northwest Laboratory (PNL) to aid the U.S. NRC's Office of Nuclear Reactor Regulation in developing strategies to prevent sabotage and tampering in nuclear power plants or to mitigate their effects. This report has ranked alternatives in the operation and design of nuclear power plants based on their ability to protect the public from intentional releases of radioactive material. This report describes the methodology that was developed to perform this ranking and summarizes data on historic sabotage incidents that were collected to implement the method. Information presented in this report, along with other factors, can be used by the NRC to focus future regulatory and research activities.

1.1 BACKGROUND

Generic Safety Issue A-29, Nuclear Power Plant Design for the Reduction of Vulnerability to Sabotage (U.S. NRC 1978), considers alternatives to the basic design of nuclear power plants, with emphasis on reducing their vulnerability to sabotage. Present plant designs and physical security systems provide a great deal of inherent protection against industrial sabotage. Issue A-29 explores an alternative approach to more fully consider reactor vulnerabilities along with economy, operability, reliability, maintainability, and safety during the preliminary design phase.

The NRC objective in ranking alternatives in sabotage and tampering avoidance technology (STAT) is to use NRC and industry resources to produce the greatest safety benefits at a reasonable cost. Numerous factors are considered in the implementation of STAT. These include risk to the public, core melt frequency (CMF), dose to power plant workers, and cost to the NRC and industry. This report is intended to quantify, on a relative basis, the portion of the decision.

Core melt frequency was chosen as the risk measure due to the limitations imposed by current models of nuclear power plant resistance to sabotage. These models currently resolve these events as to their potential for causing any release of radioactivity. Little or no differentiation is currently made on release size or composition. To be consistent with previous risk assessments, only acts leading to core melt were considered. Release of material from storage locations at power plants or diversion and dispersal of material at other locations were not considered.

The CMF reduction term is defined based on previous work by the NRC in the prioritization of generic safety issues (U.S. NRC 1983a) as the product of the number of plants affected by the STAT, the average remaining life of the plants, and the average risk reduction due to offsite releases from accidents. This can be stated as:

$$(\Delta F)_{Total} = \left[\begin{array}{c}\text{CMF before STAT} \\ \text{Implementation}\end{array}\right] - \left[\begin{array}{c}\text{CMF after STAT} \\ \text{Implementation}\end{array}\right]$$

$$= \bar{F}_o \sum_i N_i \bar{T}_i \frac{(\Delta F)_i}{F_{oi}}$$

where i = the index of the representative plant type

N_i = the number of affected plants to which representative plant-type i corresponds

$\bar{T}_i$ = the average remaining operating life of affected plant-type i

$(\Delta F)_i$ = the CMF reduction for representative plant-type i in events/reactor-year

$\bar{F}_o$ = average original total CMF level for plants with PRAs

F_{oi} = total original CMF for representative plant i.

Since comparison between current plant population and future plant population is not possible, all comparisons in this report are based on individual plants. The number of plants affected by any one alternative was considered, to the extent that the information was available, as a secondary factor in assigning the final rankings.

1.2 ALTERNATIVES FOR THE PREVENTION AND/OR MITIGATION OF SABOTAGE

The NRC defined a total of 25 alternatives to prevent or mitigate the effects of sabotage. These alternatives are listed in Table 1.1. The first four were intended to represent alternatives for future plant designs. Items 5 and 6 are applicable to all plants to reduce the threat from insiders. Items 7 through 25 were selected from NUREG/CR-2585 (U.S. NRC 1982) as examples of damage control measures to mitigate the effects of sabotage. Each of the alternatives is described in additional detail in Appendix A.

TABLE 1.1. Summary of STAT Alternatives

No.	Description of Alternative
1	Three 100% trains of safety related equipment
2	For a BWR--two additional bunkered RCIC pumps For a PWR--two additional bunkered AFW pumps
3	A passive steam condenser for the steam generators of a PWR
4	The SNUPPS design with complete separation

TABLE 1.1. (Contd)

No.	Description of Alternative
5	Implementation of the two man rule
6	Installation of TV cameras in vital areas
7	Manual/local operation of BWR safety-relief valves
8	Feed-and-bleed operation of suppression pool
9	Use of safety-injection (SI) pumps to supply water to steam generators (SG)
10	Provide spring-loaded safety valves for venting stream generators
11	Use fire water as source of cooling RHR heat exchangers
12	Connect SI pump in series to raise discharge pressure
13	Use control rod drive hydraulic system to supply reactor coolant makeup
14	Use main condenser pump to provide reactor coolant makeup
15	Cross-connect service water with essential service water (ESW)
16	Cross-connect fire system and ESW
17	Use ESW to directly cool components cooled by CCW
18	Provide local pressurizer and SG level indication
19	Provide local readouts for SG pressure
20	Provide emergency AC power to nonsafety related equipment
21	Provide cross-connection between Class IE/non-Class IE
22	Provide multiple DC feeders to DC powered components
23	Provide an alternate water source to maintain coolant inventory (PWR)
24	Provide a standby non-Class 1E combustion turbine generator
25	Provide capability to place an emergency diesel generator in service without DC power

1.3 APPROACH TO THE RANKING OF STAT ALTERNATIVES

This is the first attempt at the calculation of CMF from historic data on sabotage and tampering acts. The approach was developed after a review of information available from probabilistic risk assessments (PRAs), threat assessments, historic data, vital area studies, and physical protection simulations. The attributes of each technique of interest to this project are as follows:

- Probabilistic Risk Assessment - PRA is a structured method to quantify safety through the integration of historic data, engineering analysis, and engineering judgment. NRC uses this tool to rank research objectives and evaluate new rules.

- Historic Data on Sabotage and Tampering - It was recognized that data in NRC and DOE files is limited for sabotage and tampering. However, acts have occurred at NRC and DOE facilities that cover a broad range of potential damage and motivations.

- Threat Assessment - Threat assessment is based on a review of the facility and a determination of the resources needed to complete acts resulting in various levels of damage. Frequencies of threats are not usually considered.

- Physical Protection Simulations - These simulations predict the level of damage and area of attack based on facility access control, the resources available to the attackers, and the response of plant personnel.

- Vital Area Studies - These studies evaluate combinations of locations in the plant where destructive acts could lead to releases of radioactive material. Vital area studies can be integrated with physical protection simulations to provide a list of likely sabotage targets and the acts required to cause a release.

The original intent of this study was to combine results of the bulleted techniques above to calculate the contribution of sabotage to public risk. Limitations imposed by the various model results, resources available to the project, and historic data forced the scaling back of the conceptual approach. It was decided that a practical goal would be to use the results of PRAs, historic data, and vital area studies to bound the contribution of sabotage and tampering to CMF for the purposes of relative rankings of STAT alternatives. If additional information becomes available to reclassify release categories and their consequences, this method could be extended to pubic risk calculations. Physical protection simulations were not used due to resource limitations.

An underlying assumption of the study is that STAT can impact accident initiators and/or can improve the capability of the plant to terminate transients prior to core damage. The effects of changes in plant operation and design can then be measured in terms of reduced CMF from accidents and deliberate acts of sabotage and tampering. The methodology described in this report is an extension of the CMF reduction analysis developed for the prioritization of generic safety issues (NUREG-0933, U.S. NRC 1983a).

The relatively large number of alternatives to be analyzed required that the methodology emphasize estimates of CMF reduction for only those alternatives that are technically defensible and within the project budget.

Major simplifications have been required to produce an approach that can be implemented with the level of effort available for the ranking of STAT alternatives. For example, historic acts of sabotage and tampering were used to define the threat to be evaluated. The uncertainty in these data is large. However, the data are believed to be a reasonable representation of the scope of actions that have occurred, and assumptions made in the use of the data significantly overestimate the extent of damage that has occurred. Use of historic data is a break from traditional physical protection analyses that postulate scenarios for the design of physical protection equipment. This is consistent with PRA analyses that predict the future experience in terms of consequences and frequency rather than on the evaluation of design bases. The relative relationship between the historic acts and the design basis threat can be developed if the frequency of design basis events can be estimated.

No rigorous uncertainty calculations were performed because they were considered beyond the resources and scope of the project. This project has focused instead on the development of point estimates. Sensitivity analyses of critical assumptions were considered adequate to rank STAT alternatives.

Other simplifications include the use of existing risk results for the evaluation of future plants and the use of several plants with PRA results to represent all existing plants. These simplifications introduce significant errors, since future plants and current plants not specifically considered have many differences in addition to those introduced for the purposes of avoiding sabotage and tampering. Also, the existing CMF equations do not model the impact of STAT directly. Modifications of original equations, in addition to the threat model, are developed on a case-by-case basis to accommodate alternative-specific information. Finally, alternatives treated by using this method are assumed to be independent.

An additional assumption is in the definition of sabotage for this study. An act of sabotage is defined by the NRC as a deliberate act that could endanger the health and safety of the public by exposure to radiation. Interpreting this definition on a probabilistic basis could include all acts of damage to the plant that in any way degrade safety equipment, since these acts would reduce the ability of the plant to respond to accidents. It could also be interpreted as only those acts in which releases of radioactivity actually occur. NRC practice suggests a definition closer to the latter based on no recorded acts of sabotage. In the context of PRA, a core melt event is only possible if both an accident initiator and equipment failures occur. Equipment failures can result from deliberate acts or from random failures. Thus, the initiation of accident sequences was assumed necessary and sufficient as a sabotage initiator. Releases can then be described probabilistically in terms of both deliberate and normal equipment failures. Acts that do not trigger an initiator were treated as tampering. Tampering requires that a random accident initiator take place to impact plant safety by decreasing the availability of plant safety systems.

1.4 REPORT CONTENTS

The remainder of this report provides guidance on developing the CMF information for use in ranking STAT alternatives. A six-step procedure was used:

1. Quantify the general level of CMF attributable to sabotage and tampering.
2. Catalog impacts of each STAT alternative on plant vulnerabilities.
3. Order the STAT alternatives based on their relative effectiveness in reducing sabotage and tampering impacts.
4. Scale the ordered list of STAT alternatives to the results of Step 1.
5. Compare CMF reductions for each STAT alternative in normal operations and impacts on sabotage and tampering.
6. Complete the final ranking.

Chapter 2 of this report develops a threat model based on historic data. Chapter 3 develops additional details of the methodology to calculate general CMF levels due to sabotage and tampering. Appendixes are provided to discuss details of selected portions of the analysis. Appendix A contains a description of each issue, the calculation of the issue contribution to CMF reduction during normal operation, and a description of the process ranking for sabotage and tampering. Appendix B is a safeguarded (unpublished) description of the sabotage CMF reduction calculation for the Grand Gulf and ANO-1 plants.

2.0 SABOTAGE AND TAMPERING DATA COLLECTION AND THREAT ASSESSMENT

Available data from the DOE and the NRC were compiled on the frequency, type, and severity of incidents that have occurred in federal and commercial nuclear facilities. This chapter summarizes the data collected and assumptions made in the formulation of the historic sabotage and tampering threat model. This threat model is then used to estimate the impact of sabotage and tampering acts on CMF levels.

2.1 NRC RECORDS

The major source of information on events at licensed nuclear facilities is described in the Safeguards Summary Event List (SSEL) (U.S. NRC 1983b), which covers the period 1976 through 1983. This document provides brief summaries of several hundred safeguards-related events involving nuclear material or facilities regulated by the NRC. Events are described under the following categories:

- Bomb-related: concerned with explosive or incendiary devices, or incendiary material and related threats. These events are divided into actual and unsubstantiated threats.
- Intrusion: includes incidents of attempted or actual penetration of safeguards systems or a facility barrier.
- Missing and/or allegedly stolen: includes those events in which licensed material is missing.
- Transportation: deals with incidents away from the licensee site.
- Tampering/vandalism: includes destruction or attempted destruction of property, parts, and equipment that does not directly cause a radioactive release; or hoax incidents, threats, and associated harassment.
- Arson: includes intentional acts involving incendiary materials and resulting in damage.
- Firearms related: concerned with the discharge, discovery, or loss of firearms at a licensed facility.
- Radiological sabotage: the occurrence of any deliberate act directed against a licensed activity that could endanger public health and safety by exposure to radiation.
- Miscellaneous: events with some significance that do not fit into any of the other categories.

Table 2.1 is a summary of the events covered in the NRC listing. A total of 833 events have occurred during the period covered by the study. The majority of the events have involved bomb threats. Nine bombs have been found outside critical areas. Detonations that have occurred have not damaged

TABLE 2.1. Summary of NRC Safeguards Events (1976-1983)

Type of Event	No. of Events
Bombs	
Threats	424
Device Present	9
Potential to damage one system	1
Potential to damage multiple systems	5
Damage to plant systems	0
Intrusion	
Listings	48
Unknown or Malevolent Intent	17
Protected Areas	
Potential to damage one system	3
Potential to damage multiple systems	14
Actual damage to plant system	0
Important Areas[a]	
Potential to damage one system	0
Potential to damage multiple systems	5
Plant damage occurred	0
Missing and Assumed Stolen	
Incidents	167
Those with Power Plant Safety Implications	0
Vandalism	
Total Acts	47
Damage to plant systems	37
Protected Areas (total/operating plants)	
Damage to one system[b]	24/18
Damage to multiple systems	13/5
Important Areas[a] (total/operating plants)	
Damage to one system[d]	8/5
Damage to multiple systems	8/2
Arson	
Total Events	13
Damage to plant systems	6
Protected Areas (total/operating plants)	
Damage to one system	1/0
Damage to multiple systems	5/4
Important Areas (total/operating plants)	
Damage to one system	0/0
Damage to multiple systems	2/2
Sabotage[d]	0
Firearms	
Total Events	38
Unknown or Potential Factor in Other Events	3[c]
Miscellaneous	
Total Events	100
Related to Power Plant Safety	0

(a) Included in protected area incidents.
(b) 2 plant trips results (1 from feedwater), 1 potential LOCA.
(c) Gun taken from employee in one of plant trip events. Not used directly in crime.
(d) NRC defines sabotage as deliberate attempts to endanger public health and safety.

safety-related equipment. Intrusions with unknown or malevolent intent have occurred 17 times. These acts were judged to have the potential to damage plant systems because the intruders were not always caught, and because they had occupied protected and important areas of the plant, unobserved, for significant amounts of time. No damage has ever been attributed to intruders. Vandalism has been the largest contributor to plant damage. Damage to single and multiple systems has occurred in plants both under construction and in operation. Three events judged to be contributors to an accident initiator have occurred. Significant events have involved the closure of emergency coolant valves, the repositioning of switches and wires, damage to diesel generators and new nuclear fuel elements, initiation of plant trips, and damage to core cooling water piping. Arson has occurred in both protected and important areas of operating and partially completed plants. Damage to multiple systems has been the most likely consequence.

Most of the damage to date has occurred during the construction phase of the facility. During this phase, access is much easier and the potential consequences of damage are not as great as during operations. However, to be conservative, all significant damage attempts were included in the data base for this study as if they had occurred at operating plants.

2.2 DOE RECORDS

The U.S. DOE (IAEL 1983) has maintained records of incidents in DOE facilities over the last 35 years. Over 4000 violations have occurred. A summary of the incidents is shown in Table 2.2. The non-nuclear designation discriminates between those crimes that involved nuclear materials, processes, components, and information, and those that did not, even though they may have occurred at a nuclear facility. The nuclear designation does not necessarily indicate a release of radioactivity.

In general, the DOE statistics show that the majority of violations were of little consequence. Between 75% and 80% of the cases involved relatively minor cases of theft, malicious mischief, or vandalism, and general forms of personal misconduct of little significance (as measured by costs and actual or potential harm). The remaining crimes and incidents had or could have had an impact on national security or public health and safety (IAEL 1983). Table 2.3 lists the number of significant crimes (based on the degree of consequence or loss) that occurred within the DOE facilities. Only 20 percent of the 822 cases fall into this more serious category. The 97 nuclear cases considered serious in magnitude compose less than 2.5% of the total cases recorded. "Sabotage events" in the DOE data base were reviewed individually because of their potential importance to this study. It was found that, with one exception, these events do not fall under the NRC definition of sabotage; they conform more to the definition of vandalism in the NRC system.

Insider motivation is recorded in the DOE files. The information was derived from interpretations of information recorded in violation files, contents of interoffice notes, and interviews with DOE or contractor security personnel involved in or familiar with the cases. Of the case files, 32% contained entries documenting the motivation of the offender. Table 2.4 illustrates the distribution of the known motivations for the various types of crimes. Table 2.5 deals with the motivations of potentially significant crimes

TABLE 2.2. Total Crimes Recorded in the DOE Data Base (IAEL 1983)

Type of Crime	Non-Nuclear	Nuclear	Total
Arson	12	2	14
Assault and battery	18	1	19
Bombing/attempted bombing	2	1	3
Bomb threat (insider)	1	1	2
Commercial bribery	5	2	7
Personal bribery	3	0	3
Breaking and entering	127	3	130
Conflict of interest	19	1	20
Contraband possession	8	0	8
Contractor irregularities	17	0	17
Possession/sale of drugs or alcohol	93	1	94
Destruction of information	6	0	6
Embezzlement	14	0	14
Espionage/treason	6	8	14
Extortion	2	1	3
Forgery	35	2	37
Fraud	122	4	126
Gambling	6	0	6
Hoax	2	1	3
Kickback	16	0	16
Kidnapping	2	0	2
Libel	3	0	3
Misuse of classified information	17	22	39
Murder/attempted murder	5	1	6
Misappropriation of:			
- materials/equipment	138	5	143
- funds	29	0	29
Racketeering	2	0	2
Rape/attempted rape	5	0	5
Sabotage/attempted sabotage	21	5	26
Suicide	8	1	9
Sale/possession of stolen property	70	3	73
Sexual harassment	21	0	21
Theft of materials	515	16	531
Theft of equipment	1794	5	1799
Theft of money	385	0	385
Threat of violence	26	2	28
Vandalism/malicious mischief	263	10	273
Violence	18	1	19
Wiretapping	3	0	3

TABLE 2.3. Number of Crimes of Significance in the DOE Data Base (IAEL 1983)

Type of Crime	Non-Nuclear	Nuclear	Total
Arson	10	1	11
Assault and battery	11	0	11
Bombing/attempted	1	1	2
Bomb threat (insider)	1	1	2
Commercial bribery	3	0	2
Personal bribery	2	1	3
Breaking and entering	14	3	17
Conflict of interest	9	1	10
Contractor irregularities	5	0	5
Possession/sale of drugs or alcohol	19	1	20
Destruction of information	1	0	1
Embezzlement	11	0	5
Espionage/treason	4	6	10
Extortion	2	0	2
Forgery	16	2	18
Fraud	57	3	60
Gambling	3	0	3
Kickback	14	0	14
Kidnapping	1	0	1
Misuse or compromise of classified information	2	13	15
Murder/attempted murder	4	1	5
Misappropriation of:			
- materials/equipment	33	1	5
- funds	13	0	13
Racketeering	1	0	1
Rape/attempted rape	5	0	5
Sabotage/attempted sabotage	10	5	15
Suicide	5	0	5
Sale/possession of stolen property	32	3	35
Sexual harassment	10	0	10
Theft of materials	101	9	101
Theft of equipment	235	4	239
Theft of money	26	0	26
Threat of violence	13	0	13
Vandalism/malicious mischief	28	3	31
Violence	5	0	5
Wiretapping	2	0	2

TABLE 2.4. Insider Motivation Reported in the DOE Data Base

Intent	Percentage of Total
Greed/personal use of gain	49
Opportunity/availability	20
Disgruntlement	6
Personal loyalty	5
Game playing	4
Mental illness/drugs	3
Cover-up	2
Political/ideological	2
Revenge	2
Company loyalty	2
Gain recognition	1
Bribery	1
Gain power	1
Pay debts	1
Coerced	1
Fund cause	1
Peer pressure	0.4
Gambling debts	0.1
Threatened	0.1
Religious	0.05

TABLE 2.5. Significant Characteristics of High-Consequence Crimes Reported in the DOE Data Base (IAEL 1983)

	Motivation %				
Type of Crime	Political/ Ideological	Disgruntle-ment	Revenge	Peer Pressure	Mental Illness
Arson	20	40	5	0	10
Assault and battery	3	56	9	0	9
Bombing	67	17	17	0	0
Destruction of information	22	44	11	0	11
Kidnapping	0	0	33	0	33
Murder/attempted	50	0	13	0	29
Rape	0	0	14	0	25
Sabotage	10	47	10	4	2
Suicide	0	17	0	0	66
Threat of violence	3	27	16	0	24
Violence	0	62	14	0	10

such as sabotage, nuclear theft, and violent crimes. The distribution of motivations changes when high consequence crimes are involved. Disgruntlement is a prime motivation in many destructive or violent crimes. Bombing incidents usually involve political/ideological motivations. Sabotage is the only category in which peer pressure played a role. Again, sabotage was viewed as similar to vandalism in the NRC system. The data suggest that most disgruntled employees who are upset enough with the work environment to act in an illicit manner do so by harming the facility rather than their fellow employees.

2.3 USE OF DATA

One data set was created to estimate the frequencies of the various acts and the conditional probabilities associated with various states of damage. Several steps were taken to complete this task:

1. Integrate the NRC and DOE data.

2. Establish the base of experience to estimate incident frequencies.

3. Develop a severity function to combine events of potential damage with events of actual damage.

4. Present the information in a usable form.

For Step 1, the DOE data had to be limited in scope. It was assumed that only those significant incidents recorded in the Nuclear category (see Table 2.3) would be considered. Next, a correlation was made between the categories in Table 2.3 and those in Table 2.1 (the NRC data). Results of this correlation are shown in Table 2.6. Bombings and bomb threats in the NRC and DOE data bases were added; it was assumed that incidents in the DOE bomb category had the potential to damage multiple systems. DOE breaking and entering data were added to the NRC intrusion data. It was assumed that these attempts had the potential to damage multiple systems in either protected or important areas of the plant. The DOE categories of theft of materials, theft of equipment, and theft of money were added to the NRC category of "missing and assumed stolen." It was assumed that there were no events with safety significance to power plants in this category. Vandalism events were added. DOE events were assumed analogous to events in protected and important areas of operating plants that damaged multiple systems. Arson events recorded by the NRC were added to DOE events with damage to multiple systems in protected and important areas of operating plants.

A fundamental issue in the combination of data was the definition of sabotage. The review of the events listed as sabotage in the DOE files indicated that four out of five are a double counting of NRC events in other categories. However, the DOE data also indicate a suspected intentional act that destroyed the SL1 reactor in Idaho Falls. If this event had occurred it might have been included as a sabotage event. Firearm events were not listed separately by DOE. All other categories were similar to the NRC miscellaneous category and assumed unimportant to safety.

A time period had to be defined to calculate a frequency for the sabotage and tampering events. Based on the number of U.S. operating plants in 1983, 575 years of operating experience were specified. While the NRC data base does not

cover the entire period that plants have operated, the addition of the DOE data was assumed to make the total number of acts equivalent to what it would be if the NRC data had been gathered for the operating life of all plants.

Alternative bases could be developed to model historic events. An example would be the number of person-years expended at the plant. Information to perform this evaluation was not directly available, although if staffing questions are to be addressed in the future, it could be developed.

A number of assumptions were made to weight the significance of acts that occurred during construction. Acts were assumed to be less severe than those occurring during plant operations due to increased access and a lessened chance of immediate discovery. In weighting historic events of each type, it was assumed that significant plant damage had occurred. These adjusted numbers of events were then divided by 575 reactor-years to yield the frequency for each event. Results are shown in Table 2.7. If these weighting factors are omitted, the contribution from outsiders would be larger.

The assumed weighting factors for the prediction of plant damage from bombs were set at 0.5 for one system and 0.1 for multiple systems, due to the size of the devices that have been found and the fact that no large bombs have ever been placed in proximity to safety-related equipment. Likewise, no damage has ever been recorded from intruders. However, opportunities for intruders to commit acts of damage have occurred. A value of 0.5 was assumed for acts that damage one system. Acts that damage multiple systems were assigned a value of 0.1, based on the roughly 10 acts that have been observed in the protected area. Acts in important areas were assigned a value of 0.05, since roughly 20 acts have occurred and no damage was observed.

Weighting factors for vandalism and arson were set to the ratio of the number of incidents at operating plants to the number of incidents at nonoperating plants. The weighting factor for sabotage with plant damage was set to 0.1, due to the differences between commercial plants and the reactor at Idaho Falls. A weighting factor of 0.5 was used for plant trips, since it appeared that the intent was to embarrass management rather than cause a release. Firearms were considered a factor in only one of three events.

TABLE 2.6. Summary of Historic NRC and DOE Insider Events

Type of Event	NRC	DOE	Total
Bombs			
Threats	424	1	425
Device Present	9	1	10
Potential to damage one system	1	0	1
Potential to damage multiple systems	5	1	6
Damage to plant systems		0	0
Intrusion			
Listings	48	3	51
Unknown or Malevolent Intent	17	3	20
Protected Areas			
Potential to damage one system	3	0	3
Potential to damage multiple systems	14	3	17
Actual damage to plant system	0	0	0
Important Areas[a]			
Potential to damage one system	0	0	0
Potential to damage multiple systems	5	3	8
Plant damage occurred	0	0	0
Missing and Assumed Stolen			
Incidents	167	13	180
Those with Power Plant Safety Implications	0	0	0
Vandalism			
Total Acts	47	3	50
Damage to plant systems	37	3	40
Protected Areas (total/operating plants)			
Damage to one system[b]	24/18	0	24/18
Damage to multiple systems	13/5	3/3	16/8
Important Areas[a] (total/operating plants)			
Damage to one system	8/5	0	8/5
Damage to multiple systems	8/2	3/3	11/5
Arson			
Total Events	13	1	14
Damage to plant systems	6	1	7
Protected Areas (total/operating plants)			
Damage to one system	1/0	0	1/0
Damage to multiple systems	5/4	1/1	6/5
Important Areas[a] (total/operating plants)			
Damage to one system	0	0	0/0
Damage to multiple systems	2/2	1/1	3/3
Sabotage			
Damage to plant systems	0	1	1
Trip initiated	2	0	2
Firearms			
Total events	38	0	38
Unknown or Potential Factor in Other Events	3	0	3[c]
Miscellaneous			
Total Events	100	31	131
Related to Power Plant Safety	0	0	0

(a) Included in protected area incidents.
(b) 2 plant trips resulted (1 from feedwater): 1 potential LOCA. Also known in sabotage (NUREG-0525, U.S. NRC 1983b).
(c) Gun taken from employee in one of plant trip events. Not used directly in crime.

TABLE 2.7. Summary of NRC and DOE Insider Events

	Actual Events (Col.1)	Weight for Low-Damage Events (Col.2)	Normalize Events to Predict Damage (Col.1xCol.2)	Event Frequency (plant-year^{-1}) (Col.3)
Bombs				
Threats	425			
Device Present	10			
Potential to damage one system	1	0.5	0.5	8.7E-04
Potential to damage multiple systems	6	0.1	0.6	1.0E-03
Damage to plant systems	0	---	---	---
Intrusion				
Listings	51			
Unknown or Malevolent Intent	20			
Protected Areas				
Potential to damage one system	3	0.5	1.5	2.6E-03
Potential to damage multiple systems	17	0.1	1.7	3.0E-03
Actual damage to plant systems	0			
Important Areas[a]				
Potential to damage one system	0	---	---	---
Potential to damage multiple systems	8	0.05	0.40	7.0E-04
Plant damage occurred	0	---	---	---
Missing and Assumed Stolen				
Incidents	180			
Those with Power Plant Safety Implications	0	---	---	---
Vandalism				
Total Acts	50			
Damage to plant systems	40			
Protected Areas (total/operating plants)				
Damage to one system[b]	24/18	0.75	22.5	3.9E-02
Damage to multiple systems	16/8	0.5	12	2.1E-02
Important Areas (a) (total/operating plants)				
Damage to one system	8/5	0.75	7.25	1.3E-02
Damage to multiple systems	11/5	0.5	8.0	1.4E-02
Arson				
Total Events	14			
Damage to Plant Systems	7			
Protected Areas (total/operating plants)				
Damage to one system	1/0	0.5	0.5	8.7E-04
Damage to multiple systems	6/5	0.80	5.8	1.0E-02
Important Areas[a] (total/operating plants)				
Damage to one system	0/0	---	---	---
Damage to multiple systems	3/3	1.0	3.0	5.2E-03
Sabotage				
Damage to Plant System	1	0.1	0.1	1.7E-04
Trip initiated	2	0.5	1.0	1.7E-03
Firearms				
Total Events	38			
Unknown or Potential Factor in Other Events	3[c]	0.3	1	1.7E-03
Miscellaneous				
Total Events	131	---	---	---
Related to Power Plant Safety	0			

(a) Included in protected area incidents.
(b) Two plant trips results (1 from feedwater): 1 potential LOCA.
(c) Gun taken from employee in one of plant trip events. Not used directly in crime.

3.0 SABOTAGE AND TAMPERING RISK CALCULATIONS

In Chapter 1, safety benefits of implementing 25 STAT alternatives were defined as reductions in CMF. Core melt frequency is reduced by reducing the frequency and severity of sabotage and tampering attempts. This chapter presents the development of a general CMF model and the methods to estimate each of these CMF variables, including the use of sabotage/tampering information developed in Chapter 2. Detailed calculations for the 25 STAT alternatives are presented in Appendixes A and B.

3.1 DEVELOPMENT OF A GENERAL CMF MODEL

To calculate the relative value of each STAT alternative, a model was created that includes major contributors to plant CMF from random failures and failures due to sabotage and tampering. The model was then exercised to determine the change in relative plant CMF due to the implementation of each STAT alternative. The impact of changes in plant design and operation to prevent and/or mitigate sabotage and tampering was calculated by a method similar to that used in the examples shown in NUREG-0933 (U.S. NRC 1983a), except that it was expanded to consider the effects of sabotage and tampering.

Overall plant CMF is generally defined as the sum of the frequencies of all anticipated accidents. Contributors to CMF are called accident sequences. Each accident sequence is expressed in terms of accident initiator frequencies and system failure probabilities. Boolean algebra is used to combine the combinations of plant equipment failures that contribute to accident sequences. Each combination is called a cut set.

The CMF reduction for each STAT alternative is the difference between the base (before STAT alternative) and the adjusted (after STAT alternative) CMF. For all STAT alternatives, only the accident sequences leading to core melt were considered.

Some STAT alternatives are not directly related to the existing parameter in the CMF sequences. It was necessary to modify the existing sequences to consider the frequency and effect of tampering (which was considered an additional failure mode for equipment), and sabotage acts (which were considered an additional contributor to accident initiators). Implementation of the STAT alternatives was assumed to affect sabotage, tampering, and random contributions to system failure probabilities and accident initiators. Development of techniques to modify the CMF equations to cover sabotage and tampering is discussed in Sections 3.2.2 and 3.2.3.

3.2 ESTIMATION OF CMF VALUES

The reduction in CMF at a representative plant due to a STAT alternative resolution is estimated by subtracting the CMF before implementation (base case) from the CMF after implementation (adjusted case). PRAs do not include sabotage/tampering. To define a base case, they were added to the PRA results. Implementation of the STAT alternative would alter the total CMF value to some

adjusted-case level. Only accidents leading to core melt are analyzed here. Previous work (Hall et al. 1979) has concluded that less severe accidents are only minor threats to public safety.

Several steps are involved in estimating CMF reduction:

- issue definition and selection of the plant model
- development of the sabotage/tampering model
- identification of affected parameters in the CMF equations
- calculation of the base-case CMF
- calculation of the adjusted-case CMF
- calculation of the CMF reduction.

These steps are discussed in the following subsections.

3.2.1 Issue Definition and Selection of the Plant Model

A STAT alternative must be clearly defined in terms of its impacts on sabotage/tampering, plant systems, and the applicable plants. A systematic procedure is described in the following sections to aid the analyst, but knowledge of plant systems is needed to utilize the procedure effectively.

STAT alternatives are generic, affecting a wide range of nuclear plants. An accurate estimate of all plant types which each alternative affects is required. Ideally, the CMF equation and sabotage/tampering threat are known for each plant. However, only certain plants have currently been subjected to CMF and sabotage/tampering vulnerability studies. The analyst must select one or more of these plants to represent the entire group of affected plants. For this analysis two plants, Arkansas Nuclear 1 (ANO-1) and Grand Gulf, were selected as representative PWR and BWR plants, respectively.

3.2.2 Equipment Failure

The damage evaluation model was developed to quantify the probability of equipment failure in a nuclear power plant given the potential acts of tampering described in Table 2.7. Sabotage acts were assumed to fail targeted equipment.

This section describes the conditional probabilities for equipment failure given an act, discovery/repair given a failure, and the probability of repair during an accident sequence. Results of this assessment are shown in Table 3.1.

Bomb damage functions were set to the values shown based on the size of the bombs that have been placed in plants to date. Bombs have been small and of the type that are most likely to be aimed at other individuals. A large bomb of this type was assumed to fail equipment in the vicinity with a probability of 0.1.

Intrusion and damage by outsiders were assumed to be successful 90 percent of the time in failing one piece of equipment. Detection by security and prevention of further damage were assumed to lower the probability to 0.1 for multiple pieces of equipment. This assumption was made to account for the possibility of an area-type threat (i.e., a bomb) to all pieces of equipment in the vicinity.

TABLE 3.1. Damage Function Parameters and Values

Threat	Probability of Equipment Failure from Act	Months for Discovery and Repair (non-accident)	Probability of Repair (accident)
Bombing			
Damage to one system	0.5	1	0
All affected systems	0.1	1	0
Intrusion			
Protected Areas			
Damage to one system	0.9	1	0
All affected systems	0.1	1	0
Important Areas			
Damage to one system	0.9	1	0
All affected systems	0.1	1	0
Vandalism			
Protected Areas			
Damage to one system	1	1	0.25
All affected systems	0.1	1	0.25
Important Areas			
Damage to one system	1	1	0.25
All affected systems	0.1	1	0.25
Arson			
Protected Areas			
Damage to one system	0.5	1	0
All affected systems	0.2	1	0
Important Areas			
Damage to one system	0.5	1	
All affected systems	0.2	1	0

Vandalism was assumed to be 100 percent effective in failing one piece of equipment. An act aimed at multiple pieces of equipment was assumed to fail equipment in the vicinity 10 percent of the time. Recovery during an accident sequence was assumed 25 percent of the time.

Arson was assumed to fail pieces of equipment based on the size of the fires that have been set to date. A single piece of equipment was assumed to fail in 50 percent of the attempts. Larger fires were assumed to fail the equipment in the vicinity 20 percent of the time.

The length of time to discover and repair damage as a result of tampering acts, in the absence of system demand, was assumed to be 1 month in every case. It is recognized that most acts would be quickly discovered and that repairs may compose the bulk of the down time. It was assumed that the plant would not shut down or trip during this time. Modifications to this assumption may be appropriate, depending on the location of the act assumed in the use of the PRA results.

Repair probability is the chance of repair given an accident in progress. Most events were assumed to be nonrecoverable during the course of an accident.

3.2.3 CMF Evaluations

This section describes an approach for adding sabotage and tampering to CMF. Three sources of information were needed to complete the process:

- vital area studies
- PRA study resolvable to the cut set level
- sabotage/tampering threat model.

Vital area studies are safeguarded analyses that indicate minimal combinations of locations in which equipment and systems that are essential to the prevention of core melt and radioactive material release are installed. Both core melt and dispersal releases are modeled. Results of the analyses include "location cut sets." These are sets of locations that, if completely protected, would preclude the release of radioactivity for the modeled sequences. Access to any of these location combinations is a necessary condition for release. The plant response to sabotage and tampering was interpreted in this study as a function of both the number and order (i.e, single, double, and higher order combinations) of location cut sets, the level of protection that the rooms are given, and the response of equipment contained in the rooms to the sabotage/tampering threat model developed previously.

Safety is presumably improved through:

- improvements in access control
- improvements in equipment resistance to attack
- reductions in the frequency or severity of attack
- reduction in the number or increase in the size of location cut sets
- determination of alternatives to the use of damaged equipment.

A multi-step procedure is followed to establish a base case for sabotage and tampering contributions to CMF:

1. Determine a set of locations for likely attack.

2. Define the equipment and important failure modes in the selected locations.

3. Evaluate the frequency of sabotage/tampering-related failures.

4. Modify PRA data to reflect the sabotage/tampering contribution. Establish the base level of the sabotage/tampering contribution to CMF.

Step 1: Determine Attack Locations

Attack locations were selected from the representative plant vital area study based on the judgment of the analyst, since NRC and DOE data are not sufficiently detailed to support a location-specific analysis. No more than two areas were considered. Multiple failures were assumed to occur in only one of the areas, based on historic data, which indicate that damage in more than one area is rare. The incidents of multiple area attack also indicate that small numbers of equipment pieces are damaged in each area.

It was assumed that a person attacking the plant would have detailed knowledge of the plant. It was also assumed that a set of two locations, one potentially in an important area and one in a protected area, represents the most sensitive configuration for the modifications being considered by this project. The selection of the two-location sets is based on historic occurrences of tampering in single areas. The damage from historic acts is more conservatively modeled if spread over two locations.

An important location was defined to have more access control than a protected location and was selected on the basis of the vital area studies to avoid unrestricted access to any combination of location that could lead to a core melt accident. Sets of important locations would have tightened access control for both locations and were deemed less likely targets. Sets of protected areas with potential for core melt accidents were precluded. Sabotage from a single location was assumed less likely due to increased access control, resistance to damage, or the fact that the location is normally occupied by personnel.

To determine a potential attack location, the vital area study is first reviewed following this procedure:

1. List all locations in the two-location cut sets.

2. List the number of times that each location appears in the two-location cut sets.

3. List the total number of times that each location appears in all location cut sets. This is available directly from the listing.

4. Identify all locations not included in each level of minimal protection sets. Consider larger protection sets until the number of locations not included is narrowed to a few.

5. List the total number of events that are included in each location.

The two-location set is to be selected using the judgment of the analyst and the above information. The two locations must include at least one location that may not be designated as important, and they must form a two-location cut set. It is desirable to maximize the number of events in the locations to affect the largest number of systems. Results of the above exercise using Grand Gulf and ANO-1 are shown in Appendix B.

Step 2: Define Equipment and Equipment Failure Modes

This step is intended to catalog equipment in the target location, failure modes for sabotage and tampering, and the affected systems to a level that is consistent with the plant PRA. A worksheet for individual items in a room is shown in Figure 3.1. The reason that a differentiation is made between the failure modes of equipment is that equipment that is considered failed in its normal operating position was assumed vulnerable to all threats. Equipment that requires a change in status to be in a failed state was assumed vulnerable to specific actions rather than to area-wide threats such as fires and bombs. An important function of the worksheets is to identify combinations of failures in the two rooms that could result in the failure of complete systems. These

combinations are identified by tracking the consequences of individual failures and combinations of failures through the vital area study to determine their impact on system performance. Each item must be tracked at least to a level at which its relationship to the PRA can be determined. Combinations that result in accident initiation and equipment failures are potential sabotage mechanisms. Completed sheets for Grand Gulf and ANO-1 are shown in Appendix B.

Location: _____
Protected/Important (Circle one)

Description (Vital Area System, PRA system, sabotage/tampering):

Failure Mode (check one):
Failed in normal position/operation (Vulnerable to all threats)

_____ Single Failure Fails System

_____ Fails System in Conjunction with other Components

List Related Components/Events:
Fails in Altered Position/State (Vulnerable to Intrusion and Vandalism)

_____ Single Component Fails System

_____ Fails System with Other Components/Events

List Related Events/Components:

Summary of Vital Area Tree:

FIGURE 3.1. Equipment Listing, Failure Mode, and Frequency

Step 3: Evaluate the Probability of Sabotage/Tampering Failures

This step assigns a probability of failure to variables in the plant PRA that correspond to equipment failures (single failures or groups of failures) in the vital area study. Failure probabilities due to tampering are calculated for specific pieces of equipment and for all equipment in a specific location. The approach for these calculations is as follows:

- Single Failure Case - This case quantifies the probability of failure of a piece of equipment located in an important area or protected area due to acts of tampering. This piece of equipment is the primary target.

- Multiple Failure Case - This case quantifies the probability of failure of multiple pieces of equipment located in an important or protected area due to acts of tampering. This affects all equipment not considered the primary target.

The damage probability calculated by the single failure model represents the "additional" unavailability imposed on a piece of equipment or a system due to acts of tampering. This estimate can then be added to the failure probability of the pieces of equipment modeled in the PRA study. By doing so, the consequences of a damage attempt can be quantified in terms of CMF. In cases where direct correspondence of equipment does not exist between the vital area study and the PRA, these probabilities were summed on a functional basis. The following is a mathematical description of the single failure case:

$$P_{Damage} = \sum_{i=1}^{N} (Freq_i)(PFail_i)(PRepair_i)$$

where:

P_{Damage} = Average unavailability of one piece of equipment due to intentional acts of damage and tampering.

N = Number of tampering categories.

$Freq_i$ = Relative frequency of occurrence of act i (i.e., number of bombings/total normalized events; see Table 2.7).

$PFail_i$ = Failure probability of a piece of equipment or an equipment due to act i (see Table 3.1).

$PRepair_i$ = Discovery and repair time of a piece of equipment or an equipment after act i has occurred (in months) (see Table 3.1).

The multiple failure case was developed to determine the additional unavailability imposed on all equipment in a single location not considered under the single failure model as a primary target for tampering. A single target in the second room of the two-location cut sets is also selected by the analyst as a multiple failure to maximize the number of systems/trains that would be disabled. The attack on a single piece of equipment in the second location was assumed to represent the extent of tampering in multiple locations based on historic data. This case is evaluated in the same manner as the single failure case, except that multiple failure values from Table 2.7 are used.

Sabotage with tampering was treated nonmechanistically due to limited historic data. The model used applied judgment to the potential for each STAT alternative to 1) reduce the number of targets (in this case, targets refer to locations where these acts could be successful), 2) make general improvements in plant mitigation capabilities, and 3) reduce insider opportunities. Sabotage

threats were evaluated by changing accident initiation frequencies (see Step 4) to those in Table 3.7, setting failure probabilities of equipment identified by the two-location cut sets to unity, and calculating a new CMF level. A worksheet for each location is shown in Figure 3.2. A completed worksheet for Grand Gulf and ANO-1 is shown in Appendix B.

Sensitivity cases can be performed at this point to test the effect of critical assumptions. The selection of important and protected designations for each room is one example of a critical assumption. This assumption is evaluated for Grand Gulf and ANO-1 in Appendix B.

Location: _____
Protected/Important (Circle one)
Location: _____
Protected/Important (Circle one)

PRA Variable	Tampering Threat					PRA Value	
	Bomb	Intrusion	Vandalism	Arson	Total Threat Probability	Affected Original	Total (Threat + Original)

Secondary Tampering Target Component/Event:

Sensitivity Cases and Assumptions:

FIGURE 3.2. Worksheet of System/Train Failure Probabilities

Step 4: Modify PRA to Reflect Sabotage/Tampering Contribution and Calculate Base Case and CMF Reductions

This step involves the calculation of base and adjusted CMFs using the results of Step 3 and the PRA. CMF is calculated by subtracting the adjusted-case CMF levels after implementation of the STAT alternative from the base case CMF levels before implementation. This section summarizes discussion of the calculations developed for the prioritization of safety issues (U.S. NRC 1983a) as the method applies to STAT.

Base-Case CMF. The base case CMF is calculated by assuming values for the affected parameters that are characteristic of the STAT alternatives before implementation. These are developed using Steps 1 to 3 and then substituted into the CMF equation of the representative plant. The affected parameters have values that are the sum of those used in the original PRA study and the threat model.

Normal PRA methods would calculate the unavailability of equipment due to tampering and add it directly to the published results. This would underestimate the contribution because the PRA model assumes independence of equipment failures. To correct for common cause effects, conditional failure probabilities given tampering or sabotage with tampering were added to random failure values in the PRA. Accident initiator frequencies were then modified to account for tampering coincidental with random accident initiators or sabotage.

Modified accident initiator frequencies were calculated using Figure 3.3. For sabotage, the frequency of the act was substituted for the normal accident initiator frequency. For tampering, accident initiators are assumed to occur randomly during the period in which the damage is not repaired. Thus the frequencies are reduced to account for the incidence of tampering, the total number of reactor years' experience and repair time. The frequency can be calculated using the following formula:

Tampering accident frequency = (PRA initiator freq)(47 events/575 reactor years)(1/12 year repair time)

Plant Name:

Alternative for analysis.

Initiator	Tampering		Sabotage			
			With Tampering		Without Tampering	
	Base	Adjusted	Base	Adjusted	Base	Adjusted

Sensitivity Cases and Discussion:

FIGURE 3.3. Accident Initiator Calculations

Once the base-case values for the affected parameters and accident initiator frequencies have been estimated, the frequencies of the minimal cut sets (those containing affected parameters) are quantified. These are summed to yield the frequencies of the accident sequences. Once the base-case frequencies for the accident sequences have been estimated, the frequencies of the core-melt release categories are summed to yield the total CMF. The adjusted case CMF due to the STAT alternative is compared against this base case CMF to yield the CMF reduction for issue resolution.

Adjusted-Case CMF. The adjusted case, affected CMF is calculated by changing the values for the affected parameters to ones that would be characteristic of the alternative subsequent to its implementation. These values are then substituted into the CMF equation of the representative plant. This could be done directly for calculation of CMF in normal operations. However, with the limitations imposed by the sabotage/tampering model, an approach was used that estimated CMF reductions directly.

Adjustment of the affected parameter values primarily involve engineering judgment, since the analyst is essentially projecting a future situation for which no data currently exist. The analyst generally modifies assumptions and frequencies in the tampering model. Results of the model are then used in the PRA equations. If commonly caused failures were incorporated into the base case CMF calculations, they must also be retained in the adjusted case. Quantification of the frequencies of the minimal cut sets and accident sequences for the adjusted case parallels that for the base case.

CMF Reduction Calculation. The CMF reduction (ΔF) due to the STAT alternative is the difference between the base-case (F) and the adjusted-case CMF. This calculation is performed for the two representative plants. The total CMF reduction is the sum of the total contribution from all affected plants of each representative type over their average remaining operating lives. Because some of the STAT alternatives in this report deal with future designs, it was decided to compare them on an individual plant basis. Thus for all of the analyses N and T were set equal to unity:

$$(\Delta F)_{Total} = \sum_i N_i \bar{T}_i \frac{(\Delta F)i}{F_{oi}}$$

where i = the index of the representative plant-type

N_i = the number of affected plants to which representativ plant-type i corresponds

$\bar{T}_i$ = the average remaining operating life of affected plant-type i

$(\Delta F)_i$ = the CMF reduction for representative plant-type i in events/reactor-year

F_{oi} = total original CMF for representative plant i.

This formula could be applied directly to CMF reductions in normal operations. However, sabotage/tampering CMF reductions used insights derived from historic data, PRAs, and vital area studies with engineering judgment to evaluate the effectiveness of STAT alternatives in reducing tampering and sabotage with tampering. These evaluations were then scaled to the CMF estimates for Grand Gulf and ANO-1 to estimate the adjusted case value for each alternative. This procedure was done in three steps:

1. Parameters for the cases of sabotage with tampering and tampering alone were defined. Sabotage without tampering was not treated due to the relatively low contribution to CMF calculated in Appendix B. Each parameter was assigned a scale based on its importance for the evaluation.

2. STAT alternatives were assigned a rating for each parameter and these values were summed for an overall rating of each STAT alternative.

3. STAT alternatives were then scaled on the basis of a maximum and minimum effectiveness to estimate CMF reductions.

Sabotage/tampering parameters considered the following concepts: historic tampering data suggested that plant equipment failures from tampering can cover a wide area. Acts have failed single systems or small groups of systems. Tampering failures are controlled by opportunity, system resistance to damage, and reduction of motivations to commit the acts. Sabotage with tampering, to be successful, must focus on a relatively small portion of the plant. It is controlled by target accessibility and response of the plant to mitigate transients with concurrent equipment failures. Parameters were defined as follows:

Sabotage with Tampering:

- Single-Location Cut Set Reduction. This insight was from the vital area studies. These areas are important because of their relationship to all equipment in the plant. These are the areas in which it is possible to initiate a transient and disable all safety systems from a single location. A scale of 0 to 12 was used for this parameter.

- Two-Location Cut Set Reduction. This parameter was based on the vital area studies and was included because damage at more than one location is credible based on historic data on tampering. Two-location cut sets are those areas that require tampering in two rooms to initiate a transient and disable all safety systems. A scale of 0 to 5 was used for this parameter.

- Reduce Sabotage Threat. This parameter is based on trends observed in tampering data. It was chosen to indicate increased physical protection and deterrence to committing acts of sabotage with tampering. A scale of 0 to 6 was used for this parameter.

- System Availability Increase. This parameter was chosen based on the vital area study results and tampering data. It indicates the degree to which the equipment is hardened against successful attack. A scale of 0 to 3 was used.

- Backup System Availability Increase. This parameter was developed based on PRA insights. It indicates the relative importance of the affected equipment in the operability of other equipment. A scale of 0 to 5 was used.

Tampering:

- Reduction in Opportunity. This parameter is based on vital area study results and indicates improvements in physical protection and surveillance. A scale of 0 to 6 was used.

- Increase System Availability. This indicates improvements in system resistance to attack. A scale of 0 to 6 was used.

- Reducing Tampering Motivation. This is based on the threat model and represents reductions in motivation based on deterrence and plant-wide reductions in available targets. A scale of 0 to 6 was used.

Results for the 25 STAT alternatives are presented in Tables 3.2 and 3.3. The basis for the individual ratings is discussed in Appendix A.

Scaling was done by defining a maximum and minimum effectiveness for tampering and sabotage with tampering. A nonlinear scale was used to bias the results in favor of parameters with greater importance and penalize STAT alternatives with small contributions. In this way, items with smaller and more uncertain benefits would be ranked lower than items with more promise. The following numerical values were used. Scaling parameter ranges were used for effectiveness determinations (effectiveness is the lowest category satisfying the inequalities).

Act	Effectiveness (%)					
	0	1	5	10	25	50
Sabotage with tampering	<3.2	<7.6	<12	<16.4	<20.8	>20.8
Tampering	<1.6	<4.8	<8	<11.2	<14.4	>14.4

The results of all CMF calculations are presented in Table 3.4. The STAT alternative CMF results were categorized to provide an overall priority ranking. The values set for high, medium, low/drop priorities are taken from NUREG-0933 (U.S. NRC 1983a). This framework was selected primarily for convenience, since the absolute values of the CMF reduction are uncertain. Numerous assumptions were made in order to perform the CMF calculations. Changes or deletion of these assumptions could have a large impact on the magnitude of CMF reduction results. However, little or no change in the ranking order is anticipated.

In assigning STAT alternatives to the priority categories, the primary consideration was the CMF reduction for sabotage with tampering. This initial category was raised or lowered by one or two levels based on the CMF reduction predicted for tampering alone and normal operations.

TABLE 3.2. Sabotage With Tampering Effectiveness Summary

Issue #	Title	Parameters/Range: Single Location Cutset Reduction (0-12)	Two Location Cutset Reduction (0-5)	Backup System Availability Increase (0-5)	Reduce Sabotage Threat (0-6)	System Availability Increase (0-3)	Parameter Total	Sabotage With Tampering Effectiveness (%)	Core-Melt Frequency Reduction
1	Three 100% Trains of safety equipment	0	5	5	0	3	13	10	2E-5
2	For a BWR--two additional bunkered RCIC pumps For a PWR--two additional bunkered AFW pumps	12	5	5	0	2	24	50	1E-4
3	A passive steam condenser for the steam generators of a PWR	SEE #2							
4	The SNUPPS design with complete separation	NOT TREATED							
5	Implementation of the two man rule	0	2	0	6	1	9	5	1E-5
6	Installation of TV cameras in vital areas	0	0	0	4	0	4	1	2E-6
7	Manual/local operation of BWR safety-relief valves	8	INCREASE	0	0	2	10	5	1E-5
8	Feed-and-bleed operation of suppression pool	0	0	5	0	2	7	1	2E-6
9	Use of safety-injection (SI) pumps to supply water to steam generators (SG)	0	0	1	0	1	2	0	0
10	Provide spring-loaded safety valves for venting steam generators	0	0	0	0	1	1	0	0
11	Use fire water as source of cooling RHR heat exchangers	SEE #16							
12	Connect SI pump in series to raise discharge pressure	SEE #9							
13	Use control rod drive hydraulic system to supply reactor coolant makeup	0	3	3	0	2	8	5	1E-5

H = High Priority (> 1E-5/ry)
M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)

TABLE 3.2. (Contd)

Issue #	Title	Parameters/Range: Single Location Cutset Reduction (0-12)	Two Location Cutset Reduction (0-5)	Backup System Availability Increase (0-5)	Reduce Sabotage Threat (0-6)	System Availability Increase (0-3)	Parameter Total	Sabotage With Tampering Effectiveness (%)	Core-Melt Frequency Reduction
14	Use main condenser pump to provide reactor coolant makeup	0	1	3	0	1	5	1	2E-6
15	Crossconnect service water with essential service water (ESW)	0	1	3	0	2	6	1	2E-6
16	Crossconnect fire system and ESW	0	1	1	0	1	3	0	0
17	Use ESW to directly cool components cooled by CCW	SEE #15							
18	Provide local pressurizer and SG level indication	4	0	3	0	0	7	1	2E-6
19	Provide local readouts for SG pressure	SEE #18							
20	Provide emergency AC power to nonsafety related equipment	SEE #21							
21	Provide crossconnection between Class 1E/non-Class 1E	0	3	0	0	2	5	1	2E-6
22	Provide multiple DC feeders to DEC powered components	SEE #25							
23	Provide an alternate water source to maintain coolant inventory (PWR)	0	0	1	0	1	2	0	0
24	Provide a standby non-Class 1E combustion turbine generator	0	3	1	0	2	6	1	2E-6
25	Provide capability to place an emergency diesel generator in service without DC power	0	0	1	0	1	2	0	0

H = High Priority (> 1E-5/ry)
M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)

TABLE 3.3. Tampering Effectiveness Summary

Issue #	Title	Parameters/Range: Reduction in Opportunity (0-6)	Increase Mitigation System Availability (0-6)	Reduce Motivation (0-6)	Total Rating	Tampering Reduction Effectiveness (%)	Core-Melt Frequency Reduction (1/ry)
1	Three 100% Trains of safety equipment	6	6	4	16	50	1E-5
2	For a BWR--two additional bunkered RCIC pumps For a PWR--two additional bunkered AFW pumps	2	4	0	6	5	1E-6
3	A passive steam condenser for the steam generators of a PWR	SEE #2					
4	The SNUPPS design with complete separation	NOT TREATED					
5	Implementation of the two man rule	4	0	4	8	10	2E-6
6	Installation of TV cameras in vital areas	2	0	4	6	5	1E-7
7	Manual/local operation of BWR safety-relief valves	0	4	0	4	1	3E-8
8	Feed-and-bleed operation of suppression pool	0	4	0	4	1	3E-8
9	Use of safety-injection (SI) pumps to supply water to steam generators (SG)	0	4	0	4	1	3E-8
10	Provide spring-loaded safety valves for venting steam generators	0	0	0	0	0	0
11	Use fire water as source of cooling RHR heat exchangers	SEE #16					
12	Connect SI pump in series to raise discharge pressure	SEE #9					
13	Use control rod drive hydraulic system to supply reactor coolant makeup	0	0	0	0	0	0
14	Use main condenser pump to provide reactor coolant makeup	0	0	0	0	0	0
15	Crossconnect service water with essential service water (ESW)	0	2	0	2	1	2E-7
16	Crossconnect fire system and ESW	0	2	INCREASES	2	1	2E-7
17	Use ESW to directly cool components cooled by CCW	SEE #15					

M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)

(a) Average of BWR and PWR core-melt frequency reduction

TABLE 3.3. (Contd)

Issue #	Title	Parameters/Range: Reduction in Opportunity (0-6)	Increase Mitigation System Availability (0-6)	Reduce Motivation (0-6)	Total Rating	Tampering Reduction Effectiveness (%)	Core-Melt Frequency Reduction (1/ry)
18	Provide local pressurizer and SG level indication	0	0	0	0	0	0
19	Provide local readouts for SG pressure			SEE #18			
20	Provide emergency AC power to nonsafety related equipment			SEE #21			
21	Provide crossconnection between Class IE/non-Class IE	0	0	0	0	0	0
22	Provide multiple DC feeders to DEC powered components			SEE #25			
23	Provide an alternate water source to maintain coolant inventory (PWR)	0	0	0	0	0	0
24	Provide a standby non-Class IE combustion turbine generator	2	4	0	6	5	1E-7
25	Provide capability to place an emergency diesel generator in service without DC power	0	0	0	0	0	0

H = High Priority (> 1E-5/ry)
M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)
(a) Average of BWR and PWR core-melt frequency reduction

TABLE 3.4. Results of CMF Assessments

Issue #	Title	Normal Operations CMF Reduction RY-1[a]	Rank	Tampering CMF Change RY-1	Rank	Sabotage CMF Change RY-1	Rank	Total Ranking
1	Three 100% Trains	1E-5	H	1E-5	H	2E-5	H	H
2	For a BWR--two additional bunkered RCIC pumps For a PWR--two additional bunkered AFW pumps	1E-5	H	1E-6	H	1E-4	M	H
3	A passive steam condenser for the steam generators of a PWR	0	D	0	D	0	D	D
4	The SNUPPS design with complete separation	NOT ESTIMATED		NOT ESTIMATED		NOT ESTIMATED		
5	Implementation of the two man rule	1E-7	L	2E-6	H	1E-5	H	H
6	Installation of TV cameras in vital areas	0	L	1E-7	D	2E-6	M	M
7	Manual/local operation of BWR safety-relief valves	4E-7	L	3E-8	D	1E-5	H	H
8	Feed-and-bleed operation of suppression pool	2E-5	H	3E-8	D	2E-6	M	H
9	Use of safety-injection (SI) pumps to supply water to steam generators (SG)	2E-6	M	3E-8	D	0	D	L
10	Provide spring-loaded safety valves for venting steam generators	0	D	0	D	0	D	D
11	Use fire water as source of cooling RHR heat exchangers	2E-5	H	SEE #16		SEE #16		M
12	Connect SI pump in series to raise discharge pressure	1E-5	H	SEE #9		SEE #9		M
13	Use control rod drive hydraulic system to supply reactor coolant makeup	3E-6	M	0	D	1E-5	H	H
14	Use main condenser pump to provide reactor coolant makeup	2E-7	L	0	D	2E-6	M	M
15	Crossconnect service water with essential service water (ESW)	1E-5	H	2E-7	L	2E-6	M	M
16	Crossconnect fire system and ESW	1E-5	H	2E-7	L	0	D	L
17	Use ESW to directly cool components cooled by CCW	2E-6	M	SEE #15		SEE #15		M
18	Provide local pressurizer and SG level indication	2E-6	M	0	D	2E-06	M	M
19	Provide local readouts for SG pressure	2E-6	M	SEE #18		SEE #18		M

H = High Priority (> 1E-5/ry)
M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)

(a) Average of BWR and PWR core-melt frequency reduction
(b) PWR Results
(c) (-) indicates an increase in plant risk

TABLE 3.4. (Contd)

Issue #	Title	Normal Operations CMF Reduction RY-1[a]	Rank	Tampering CMF Change RY-1	Rank	Sabotage CMF Change RY-1	Rank	Total Ranking
20	Provide emergency AC power to nonsafety related equipment	-3E-6	D	SEE #21		SEE #21		D
21	Provide crossconnection between Class 1E/non-Class 1E	1E-5	H	0	D	2E-6	M	H
22	Provide multiple DC feeders to DEC powered components	7E-6	M	SEE #25		SEE #25		L
23	Provide an alternate water source to maintain coolant inventory (PWR)	5E-7	D	0	D	0	D	D
24	Provide a standby non-Class 1E combustion turbine generator	4E-6	M	1E-7	D	2E-6	M	M
25	Provide capability to p ace an emergency diesel generator in service without DC power	1E-6	M	0	D	0	D	L

H = High Priority (> 1E-5/ry)
M = Medium Priority (> 1E-6/ry, < 1E-5/ry)
L = Low Priority (> 1E-7/ry, < 1E-6/ry)
D = Drop Priority (< 1E-7/ry)

(a) Average of BWR and PWR core-melt frequency reduction
(b) PWR Results
(c) (-) indicates an increase in plant risk

REFERENCES

Hall, R. et al. 1979. A Risk Assessment of a Pressurized Water Reactor for Class 3-8 Accidents. NUREG/CR-0603, Brookhaven National Laboratory, Upton, New York.

Hatch, S. et al. 1982. Reactor Safety Methodology Applications Program: Grand Gulf Unit 1 BWR Power Plant. NUREG/CR-1659 #3, Sandia National Laboratories, Albuquerque, New Mexico.

IAEL. 1983. The Insider Adversary Study. IEAL-294, International Energy Associates Limited, Washington, D.C.

Kolb, G. J. et al. 1982. Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear Unit-1 Power Plant. NUREG/CR-2787, Sandia National Laboratories, Albuquerque, New Mexico.

McCormick, N. J. 1981. Reliability and Risk Analysis Methods and Nuclear Applications. Academic Press, New York.

Minarick, J. W., and C. A. Kukielka. 1982. Precursors to Potential Severe Core Damage Accidents: 1969-1979. NUREG/CR-2497, Science Applications, Inc., Oak Ridge National Laboratory, Oak Ridge, Tennessee.

U.S. NRC 1978. Task Action Plans for Generic Activities (Category A). NUREG-0371, U.S. Nuclear Regulatory Commission, Washington, D.C.

U.S. NRC 1982a. Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection. NUREG/CR-2585, U.S. Nuclear Regulatory Commission, Washington, D.C.

U.S. NRC 1983a. A Prioritization of Generic Safety Issues. NUREG-0933, U.S. Nuclear Regulatory Commission, Washington, D.C.

U.S. NRC 1983b. Safeguards Summary Event List. NUREG-0525, U.S. Nuclear Regulatory Commission, Washington, D.C.

U.S. NRC 1983c. Guidelines for Nuclear Power Plant Safety Issue Prioritization Information Development. NUREG/CR-2800, U.S. Nuclear Regulastory Commission, Washington, D.C.

WASH-1400. 1975. Reactor Safety Study. U.S. Nuclear Regulatory Commission, Washington, D.C.

APPENDIX A

CORE MELT FREQUENCY CALCULATIONS FOR 25 SABOTAGE AND TAMPERING AVOIDANCE TECHNOLOGY ALTERNATIVES

APPENDIX A

CORE MELT FREQUENCY CALCULATIONS FOR 25 SABOTAGE AND TAMPERING AVOIDANCE TECHNOLOGY ALTERNATIVES

This appendix provides supporting documentation for the core melt frequency (CMF) reductions discussed in Chapter 3. Also presented are a description of each of the 25 STAT alternatives and the CMF reductions for random accidents and for tampering and sabotage.

CALCULATION OF CMF REDUCTIONS FOR RANDOM ACCIDENTS

STAT ALTERNATIVE 1:

THREE 100 PERCENT SAFETY TRAINS

This STAT alternative refers to three independent safety trains. The present arrangement in plants is to have two independent safety trains--from sensors; through logic circuitry; through engineered safeguards actuation; to the paths for safety injection, containment isolation/spray, and emergency power generation. This arrangement provides separation of the train components in such a way that the single failure criterion is met, acceptable levels of reliability are established, and convenient means of surveillance testing are possible without shutting down the plant. Vital areas are physically and administratively protected, and equipment is shielded against missiles and protected against natural phenomena. Still, it would be possible for a knowledgeable and determined group of individuals to quickly knock out a sufficient amount of equipment to paralyze many plant safety functions, including reactor protection.

ASSUMPTIONS

To be effective, a third isolated safety train would have to be located in different facilities than those that now exist at each plant. In the first place, there is no physical room to add another set of systems with all the diversity, fail-safeness and other requirements mentioned above. In the second place, merely locating a third train where it would be exposed to the same sabotage threat as the first two would not increase the overall availability of systems important to safety; it would just take a longer period of time or a larger group to accomplish the same result. An entirely new, protected, and possibly passive failsafe system would have to be created. In the case of existing plants, a specially hardened facility independent of the existing auxiliary building and tankage would be necessary to achieve the same imperviousness as the passive system mentioned above.

The following assumptions were used to apply this measure to ANO-1, whose PRA was used in the evaluation:

1. There are already three independent engineered safeguards features electrical busses, so no additional bus was assumed.

2 Manual initiation of the high pressure injection (HPI) system is not affected by the existence of a third safety train.

3. HPI system pipe faults are generally assumed to be mitigated by the presence of the third train. The third train is not modeled in the PRA, so its effect has been added to the PRA dominant minimal cut set elements directly related to safety train behavior.

4. The assumption was made that the emergency diesel generators would not be affected by the presence or action of a third independent safety train.

5. The assumption was made that the high pressure recirculation system would not be affected by the third safety train.

The elements affected in the PRA are listed below. These elements were selected based on the interpretation that this measure would significantly affect systems dominated by independent failure modes. To determine the impact of adding a third 100 percent train on overall plant safety, the redundant systems created by this STAT alternative were added to the appropriate cut sets. This was numerically simulated in the PRA by assuming that the added term will have the same failure probability as the existing systems. Therefore, the product of these two terms was inputted in the existing cut sets. This is illustrated below.

Parameter	Base-Case Value	Adjusted-Case Value
LF-HPI-H14	1.4E-2	2E-4
LPI-1407A-VCC-LF	8.2E-03	7E-5
LF-LPI-L25	1E-04	1E-8
LPI-1408B-VCC-LF	8.2E-03	7E-5
LF-DC-D07	1.1E-03	1.2E-6
LF-DC-D06	1.1E-03	1.2E-6
LF-DC-D02	1E-04	1E-08
LF-AC-A3	2.4E-04	6E-08
LF-DC-D01	1E-04	1E-08
LF-AC-B5	4.4E-04	2E-07
LF-LPI-L19	2.6E-02	7E-04
LF-LPI-L20	2.6E-02	7E-04

EFFECT ON CORE MELT FREQUENCY

The reduction in core melt frequency at ANO-1 is computed to be 2.0E-05/ry for application of this measure.

The following are assumptions for application of the measure to Grand Gulf, whose PRA was used in the evaluation:

1. Similar to the ANO-1 evaluation, the impact of adding a third independent safety train was analyzed by changing the values of dominant minimal cut sets.

   The purpose of the reactor core isolation cooling (RCIC) system is to supply high pressure makeup water to the reactor vessel when the reactor is isolated from the main condenser and the condensate and feedwater system is not available. The functional classification of the RCIC system is that of a safety related system and an engineered safety feature (ESF), but it is not part of the ECCS, although it can help maintain the core coolant level in the event of a small (< 1 in.) break LOCA. No credit is taken for the RCIC in LOCA analyses, but the RCIC is considered an ESF because of its role in mitigating the consequences of a control rod drop accident. Should a rod drop accident occur, it is possible that the main steam lines might isolate on a high radiation signal. The RCIC system then performs its normal isolation cooling function.

   The RCIC system consists of a steam turbine driven pump and associated valves and piping capable of delivering water to the reactor vessel. The turbine is driven by the steam produced from decay heat. Water is taken from either the condensate storage tank (CST) or the suppression pool and delivered to the reactor vessel to maintain an adequate level. Turbine exhaust is directed to the suppression pool, where it is condensed.

   The RCIC system is also used in conjunction with the residual heat removal (RHR) system in the steam condensing mode to pump condensate from the RHR heat exchangers back into the reactor vessel.

   Alternate flow paths are provided to allow recirculation to the CST for testing purposes, discharge to the suppression pool to ensure minimum flow through the pump, and recirculation for turbine lube oil cooling.

   Because the RCIC is a safety related system, it is reasonable to postulate that a parallel system could be installed as part of the definition of "third train." The impact of adding a third train is once again determined by changing the valves of dominant minimal cut sets.

2. The impact of adding a third train on availability of the flow path from the suppression pool to the core spray nozzles was also determined by changing the valves of appropriate cut sets.

3. Systems not affected by the addition of a third safety train were the RHR system, the low pressure coolant injection system, and the standby service water system, because these systems already have three trains.

4. The suppression pool makeup system has only two trains. The impact of adding a third train was also considered.

Similar to the procedure adopted for ANO-1, the values of appropriate element cut sets were adjusted to reflect the impact of design change. The elements affected and their "adjusted" failure probabilities are listed below.

Parameter	Base-Case Value	Adjusted-Case Value
R	0.051	0.003
RACT	0.0012	0.0000015
L	0.021	0.0004
SA	0.014	0.0002
SB	0.014	0.0002
SAACC	0.0012	0.0000015
SBACC	0.0012	0.0000015
SCVA	0.032	0.001
SCVB	0.032	0.001

The reduction in core melt frequency at Grand Gulf due to implementation of this STAT alternative was computed to be 6.5E-06/ry.

STAT ALTERNATIVE 2:

FOR A BWR - TWO ADDITIONAL BUNKERED RCIC PUMPS

This STAT alternative refers to the addition of two additional reactor core isolation cooling (RCIC) pumps in a protected environment. Early model BWRs (BWR/2 and some BWR/3 plants) have no RCIC system. Instead they have an inventory conserving system called the isolation condenser system or emergency condenser system. This system has much the same results as use of the RCIC system with the steam condensing mode of the residual heat removal (RHR) system. The remainder of this description is specific to the RCIC system. In present RCIC designs, there is typically one RCIC pump driven by a steam turbine. The turbine is run with steam from the main steam line. The purpose of the RCIC system is to supply high pressure makeup water to the reactor vessel when the reactor is isolated from the main condenser and the condensate and feedwater system is not available. The RCIC system is not part of the BWR emergency core cooling system, and no credit is taken for the RCIC in LOCA analyses. The RCIC system is considered to be an engineered safety feature (ESF) system because of its role in mitigating the consequences of a control rod drop accident. The RCIC system is completely backed up by the high pressure core spray (HPCS) system, which is one of the emergency core cooling systems.

ASSUMPTIONS

It is assumed that a separate facility with totally independent systems, utilizing one motor and one steam driven pump, will be necessary to achieve measurable gain against the sabotage threat. Extending the cross connections among the water and steam systems will make it more difficult for a saboteur, but the gain in availability may be difficult to calculate because the increase complexity tends to reduce availability.

The following special consideration is important for application of this measure to Grand Gulf, whose PRA was used in the evaluation. Any element of the dominant minimal cut sets whose unavailability affected the present RCIC pump was assumed to represent an effective reduction in its unavailability of 75 percent due to the additional pumps and related hardware.

Parameter	Base-Case Value	Adjusted-Case Value
R	0.051	0.01275
RACT	0.0012	0.0003

EFFECT ON CORE MELT FREQUENCY

The reduction in core melt frequency was computed to be 4.2E-06/ry for application of this measure to Grand Gulf.

STAT ALTERNATIVE 2:

FOR A PWR - TWO ADDITIONAL BUNKERED AFW PUMPS

This STAT alternative refers to the addition of two additional auxiliary feedwater pumps in a protected environment. In present designs, there are typically three auxiliary feed pumps: two that are electric motor driven and one that is steam driven. The plumbing is cross connected in such a way that any one motor driven pump can fail and the other pumps can carry the load. The steam driven pump automatically comes on when the motor driven pumps are not available, such as in a blackout (loss of site power). This would also be the case if the AC electrical busses were sabotaged. The source of steam is either the steam generators, which are still steaming when a blackout occurs and the plant is operating, or the auxiliary (aux) steam boiler(s), which is oil fired. The aux boiler is used for warming up a cold plant, as well as providing for other steam-heated or driven equipment on the plant site when main steam is not available. On multiple plant sites, the auxiliary steam systems are interconnected, and it is possible to interconnect the auxiliary feedwater systems.

ASSUMPTIONS

The present amount of redundancy and diversity of aux feed is ample for the normal perils envisaged, but may not be impervious to a determined sabotage effort. Bunkering of the pumps (they are at present in protected vital areas) in itself may not provide sufficient protection against sabotage. A separate facility with totally independent systems, utilizing both motor- and steam-driven pumps, will be necessary to achieve measurable gain against the sabotage threat. Extending the cross connections among the water and steam systems will make sabotage more difficult, but the gain in availability may be difficult to calculate because the increased complexity tends to reduce availability. It should be kept in mind that there is no room in existing plants for additional aux feed pumps. A new facility will have to be built, but that will have to be done anyway to make a meaningful reduction of the sabotage threat. Along with additional pumps, greater security against loss of aux feed will be achieved if new sources of water are provided as well.

The following special considerations are important for application of this measure to ANO-1, whose PRA was used in the evaluation:

1. The diesels were assumed not to be affected by this measure because the steam turbine driven pumps make separate electric power sources unnecessary.

2. All of the dominant minimal cut sets consisting of the turbine driven pumps were affected due to the additional pumps and related hardware. This applied to control power (batteries) as well. The affect was quantified by adding the two additional AFW pumps to appropriate cut sets.

Similar to the approach in evaluating STAT Alternative 1, the valves of affected elements in the appropriate cut sets were adjusted to reflect addition of two bunkered AFW pumps. The listing of those elements and their values is provided below. Note that it is assumed the added systems have the same failure probability and reliability as the existing systems.

Parameter	Base-Case Value	Adjusted-Case Value
LF-DC-DO7	1.1E-03	1E-09
LF-DC-DO6	1.1E-03	1E-09
LF-EFS-E11	4E-03	6E-08
LF-EFS-E4	0.012	2E-06
LF-EFC-ACBD4	0.011	1E-06
LF-EFC-VCD2	9.4E-03	8E-07
LF-EFS-E29	8.1E-03	5E-07
LF-EFC-BB7B1CM	5.4E-03	2E-07
LF-EFS-E5	0.012	2E-06
LF-EFW-E28	8.1E-03	5E-07
LF-EFS-E22	3E-04	3E-07
LF-EFC-CSY2	3.9E-03	6E-08
LF-EFS-E2	1E-04	1E-12

EFFECT ON CORE MELT FREQUENCY

The change in core melt frequency for ANO-1 was computed to be 1.7E-05/ry.

STAT ALTERNATIVE 3:

A PASSIVE STEAM CONDENSER FOR THE STEAM GENERATORS OF A PWR

This STAT alternative refers to the provision of an alternative means of condensing steam if the main condenser is unavailable. At present, the main steam condensers are not available unless there is adequate vacuum and at least half of the circulating water capacity is operating (one of two pumps). If the condenser is not available, the steam is vented to the atmosphere. If there is a tube leak or rupture that allows radioactive primary coolant to reach the secondary side, the unavailability of the condenser leads to a gaseous release of activity. This is the situation if there is a station blackout at the same time a tube rupture occurs. It is the basis of primary coolant radioactivity limits. Sabotage of the condenser does not threaten the plant, but can result in a release of activity.

This STAT alternative has no effect on core melt frequency, but since it concerns the possibility of radioactive material release to the atmosphere, it should be considered.

ASSUMPTIONS

If the objective of the sabotage prevention measure is to reduce the likelihood of radioactive releases to the atmosphere, a passive condenser would fulfill the requirement. Two types of passive steam condensers may be considered; one would be similar to the suppression pool used with BWRs. It could be located outdoors, underground, or be combined with existing tankage, ponds, or other water quench arrangements for the steam. There is no assurance that the noncondensible gases would be contained with such a system, unless it was closed to the atmosphere. The other solution would be a large air-cooled condenser using natural circulation. This would be isolatable from the atmosphere. Some combination of the two techniques could also be employed. One novel arrangement would be to have a large piping array built into the inside of a natural draft cooling tower. The piping would drain to a retention tank. The piping would be nonfunctional during normal operation of the plant, but secondary steam could be diverted into the piping array when the condenser was unavailable. The heating effect inside the tower, even though the water cascade structure at the base was not necessarily operating, would be sufficient to create an air draft. Mixed cooling systems involving forced air and then water spray are being proposed now for full power operation of plants in water-short areas, so the technology could easily be adapted to this application, where the heat to be dissipated by natural circulation would be far less than that at full power. The plant would be tripped by the effect of the sabotage, just as it would be by a blackout leading to the same scenario.

The following special consideration is important for attempted application of this measure to ANO-1: no elements of the dominant minimal cut sets of ANO-1 seem to relate to the availability of atmospheric steam dumps or secondary safeties. This is because the ANO-1 PRA concentrates on core melt frequency, which is unaffected by condenser availability. Clearly, though, the release

to the public due to loss of station power would be zero if all steam were contained by a passive condenser system. Since the passive condenser is a backup to the main condenser during normal operation, this STAT alternative will not result in any change in core melt frequency.

STAT ALTERNATIVE 4:

THE SNUPPS DESIGN WITH COMPLETE SEPARATION

This STAT alternative was not analyzed due to the unavailability of a PRA and a vital area study related to the SNUPPS design.

STAT ALTERNATIVE 5:

IMPLEMENTATION OF THE TWO MAN RULE

This STAT alternative would limit the access to important areas to teams of workers with at least two persons of equivalent experience. If work were being done in an important area, one person would be working while the second person, with equivalent experience in the task being performed, would be observing the first person.

This STAT alternative will have potential positive and negative effects on normal plant operation. The potential positive effects would be related to improvements in maintenance outage. If the second person (observer) could catch mistakes of the first person, the maintenance outage could be reduced either by speeding up the task or by eliminating additional maintenance outage due to previous maintenance mistakes. The potential negative effects would relate to the need for either more workers to accomplish the given two man tasks or more time to accomplish the tasks. This potential negative effect is considered more of an economic effect rather than a risk related effect.

ASSUMPTIONS

To calculate the risk change due to implementing the two man rule during normal operation, an assumption was made related to improvement in maintenance outages. It is assumed that a 5 percent decrease in maintenance outage could be achieved by implementing the two man rule. This 5 percent decrease is applied to all maintenance outage terms in both the ANO-1 and Grand Gulf PRA dominant cut sets. The reduction in core melt frequency for ANO-1 was calculated to be 1.4E-07/ry. The reduction in core melt frequency for Grand Gulf was calculated to be 1.3E-07/ry.

STAT ALTERNATIVE 6:

INSTALLATION OF TV CAMERAS IN VITAL AREAS

This STAT alternative would allow for observation of the total field of view within an important area. It is assumed that the TV cameras will be monitored in the control room. It is also assumed that because of all the other activities occurring in the control room besides monitoring the TV cameras, the TV cameras will have no significant effect on normal operational risk.

STAT ALTERNATIVE 7:

MANUAL/LOCAL OPERATION OF BWR SAFETY-RELIEF VALVES

All light water reactors are provided with some means of relieving the reactor coolant system pressure to avoid overpressurizing the system. This capability is provided by pressure relief valves located in the main steam lines. These valves can be operated automatically or manually from the control room. In addition to overpressure protection, these valves are required to perform another function: automatic depressurization of the primary system in the event of a small-break LOCA. In a small-break LOCA event, primary coolant system pressure remains high. The automatic depressurization system (ADS) is used to reduce primary system pressure to allow core cooling using the low pressure cooling systems. ADS is needed because the low pressure systems are not capable of injecting cooling water into the core when primary coolant system pressure is high.

The ADS logic has two independent channels, either of which can cause ADS valve actuation. Typically, both low reactor water level and high drywell pressure indications are needed for automatic actuation of the ADS to occur. Remote/manual ADS actuation can be accomplished via remote manual switches in the control room. For plants with a high pressure emergency cooling system, the ADS operates only in the event of a failure in the high pressure system. For older plants that are not provided with high pressure cooling systems, the ADS actuates to reduce primary coolant system pressure to allow core cooling by means of low-pressure cooling systems.

In the sabotage scenario, a loss-of-offsite-power transient is assumed to occur, which causes the turbine-generator to trip on loss of load. The high pressure injection systems are assumed to be unavailable, so the ADS system will be needed to reduce primary coolant system pressure. The sabotage action is assumed to prevent automatic and remote/manual actuation of the ADS system, which prevents the operators from using low pressure injection systems to provide cooling water to the core. This proposed STAT alternative would provide a third means of actuating ADS by adding local/manual valve actuation capability. This capability could be provided by adding manual handwheel actuators to the ADS valves. Local/manual actuation of the ADS valves would only be used if both automatic and remote/manual actuation was not successful.

ASSUMPTIONS

The overall unavailability of the ADS system is not specified in the Grand Gulf PRA. One element of ADS unavailability, the failure of the control room operator to actuate ADS under transient conditions (cut-set element OP), is included in many of the minimal cut sets for the dominant accident sequences. In transients, it is expected that monitored containment parameters do not reach LOCA initiation setpoints, so manual actuation by the operator is required. It is assumed that operator failure is the dominant contributor to ADS unavailability under transient conditions. This assumption is consistent with the Grand Gulf PRA. The probability of operator failure under these

conditions was estimated at 0.0015 per demand. Thus, the base-case unavailability of the ADS system is assumed to be 0.0015 per demand.

The proposed STAT alternative will increase the availability of the ADS system by providing a third means of actuation. If ADS is not activated automatically and the operator is not successful in activating ADS remotely from the control room, it is possible that an operator could be sent to operate the hand-wheel on the ADS valves. The resulting fault tree for failure of ADS to reduce primary system pressure is shown in Figure A.1. It is assumed that failure of a sufficient number (four of eight) of ADS valves to open given that the operator actuates them is a nondominant contributor to ADS unavailability. This assumption is consistent with the results of the Grand Gulf PRA. The probability that the operator fails to activate the ADS valves locally was assigned a value of 0.5/demand, assuming that the operator would be required to act correctly within 30 minutes of a stressful situation. The valve failure to open on demand is assumed to be 1E-3 based on WASH-1400 data. As a result, the adjusted-case probability of ADS failure to reduce primary system pressure is 0.00075.

AFFECTED PARAMETERS

The resolution of this potential sabotage issue affects only one parameter: the unavailability of the ADS system to reduce primary coolant system pressure. This value of this parameter was assumed to be dominated by the frequency of operator failure to activate the ADS (parameter OP in NUREG/CR-2800, Appendix B, U.S. NRC 1983c). The base-case and adjusted-case values for this parameter appear below.

Parameter	Base-Case Value	Adjusted-Case Value
OP	0.0015	0.00075

EFFECT ON CORE MELT FREQUENCY

The reduction in core melt frequency was computed to be 4.2E-07/ry for application of this measure to Grand Gulf.

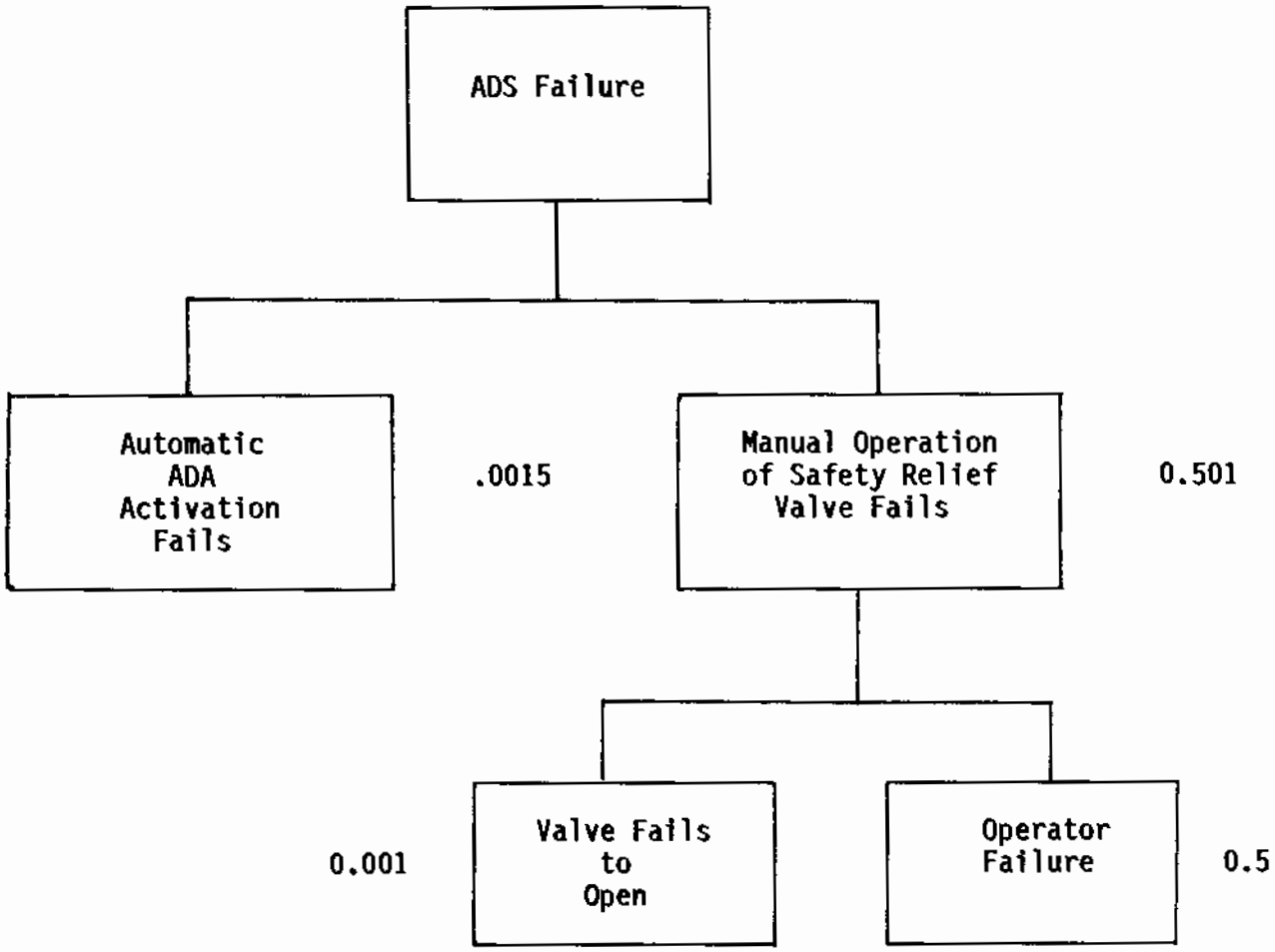

FIGURE A.1. Revised Fault Tree for Unavailability of the Automatic Depressurization System (ADS)

STAT ALTERNATIVE 8:

FEED-AND-BLEED OPERATION OF SUPPRESSION POOL

This STAT alternative would provide an alternative method for cooling the suppression pool in the event that normal suppression pool cooling systems are disabled. Acceptable suppression pool temperature would be maintained by supplying "cold" water to the pool and draining off "hot" water. Radioactively contaminated water from the pool would be transferred to large onsite tanks where possible (condensate storage tank [CST] or refueling water storage tank [RWST]), or to a large onsite settling basin.

The normal heat removal path from the reactor, steam blowdown to the main condenser, is lost following a loss of offsite power due to loss of the main circulating water system which cools the condenser and maintains its vacuum. When this occurs, steam is vented to the suppression pool when safety/relief valves open due to high pressure. Cooling water is supplied to the core by the reactor core isolation cooling (RCIC) system, the high pressure coolant injection (HPCI) system, or the high pressure core spray (HPCS) system. After initial supplies of water stored in the CST and/or RWST are exhausted, these systems are realigned to draw water from the suppression pool. Suppression pool cooling is provided via heat exchange to component cooling (CC) and/or service water (SW) systems, which transfer heat to the ultimate heat sink. This is accomplished by a single-mode containment spray system or by an operating mode of another system such as the low pressure core spray (LPCS) system, the low pressure coolant injection (LPCI) system, or the residual heat removal (RHR) system. If suppression pool cooling is lost, the pool will heat up to its design temperature/pressure limit within a matter of hours. This STAT alternative would provide an alternative method to prevent such heatup.

In the sabotage scenario a loss of offsite power is assumed to occur coincidentally with sabotage of the suppression pool cooling systems. Other safety related systems are assumed to operate normally, including those supplying water from the suppression pool to the core, and the emergency diesel generators.

ASSUMPTIONS AND AFFECTED PARAMETERS

In the suppression pool of the Grand Gulf plant, cooling is provided by the RHR system. In the PRA, dominant minimal cut sets of dominant accident sequences contain elements representing various RHR and/or SW system failures. These include failures of control circuitry, valves, and pumps. These cut sets also include a factor, RECOVERY1, defined as failure to restore maintenance/test faults or to take other corrective actions within 30 hours.

For this analysis it is assumed that the effects of operator initiation of feed-and-bleed cooling of the suppression pool on core melt probability can be modeled by modifying the value of the parameter RECOVERY1. This is reasonable since operator action is required to initiate feed-and-bleed operation. This is in fact a recovery mode.

The value of RECOVERY1 (the probability of failure to recover suppression pool cooling within 30 hours) used in the Grand Gulf PRA is 0.21. If plant modifications are made so that water supplied by other systems (RCIC, HPCI, HPCS) can be piped to alternative storage/cooling locations, the value of RECOVERY1 is assumed to become the product of its present value multiplied by the probability of failure of the new cooling method (assuming system independence). The failure probability of the feed-and-bleed cooling method is assumed to be 0.1. This is a reasonable and conservative value for systems requiring operator action to initiate, where hardware failure probability is expected to be much lower.

Based on the discussion above, for normal operations in which sabotage is not a factor, the value of RECOVERY1 should be 0.21 x 0.1.

Parameter	Base-Case Value	Adjusted-Case Value
RECOVERY1	0.21	0.021

Inputting the above valves in the PRA results in an estimated reduction in core melt frequency of 1.65E-05/ry.

STAT ALTERNATIVE 9:

USE OF SAFETY-INJECTION PUMPS TO SUPPLY WATER TO STEAM GENERATORS

The purpose of this STAT alternative is to supply water to the steam generators through the use of the safety injection pumps in the event that the auxiliary feedwater (AFW) is disabled through actions of sabotage. This assumes a loss of the main feedwater system (i.e., loss of offsite power [LOOP] and main turbine trip on loss of load will result in loss of main feedwater) (NUREG/CR-2585, U.S. NRC 1982a).

In some plants the loss of steam generator function will result in a loss of a portion of the decay heat removal function. Eventually this results in a high reactor coolant system (RCS) pressure. In this condition the plants with safety injection systems which cannot pump against full RCS pressure do not have the capacity to provide coolant makeup with the emergency core coolant system (ECCS) because the reactor pressure exceeds the shutoff head of the high pressure safety injection pumps.

Under the postulated sabotage condition a total loss of feedwater results when main feedwater is lost and there is a coincident sabotage of the AFS. Initially, the power-operated relief valves (PORVs) will open and then close. It is anticipated that the RCS temperature will drop after valve closure due to greater energy being removed by the steam generator than that being input to the system by the stored and decay heat from the core. This balance changes as the steam generators boil dry and secondary side cooling capacity is lost. Consequently, more heat is added to RCS and the RCS temperature and pressure increase to the PORV or pressurizer safety valve setpoints. After steam generator dryout, blowdown through the pressurizer safety relief valves is the only significant decay heat removal pathway for RCS. Consequently, the primary system remains at high pressure. At this point the plants with safety injection systems capable of pumping against a full RCS pressure will be able to maintain adequate core cooling inventory and should maintain a safe condition through feed-and-bleed operations. The plants without safety injection systems capable of pumping against full RCS would probably not be able to maintain adequate coolant inventory with the low capacity charging system alone (U.S. NRC 1982a).

The resolution of this sabotage issue proposes a physical connection between the safety injection system and the AFS. An example of a safety injection system modified to provide backup AFS capability is illustrated in Figure A.2. The following items, taken directly from NUREG/CR-2585, describe the basic features of a backup AFS system.

- Valving is provided to align individual safety injection pump discharges to the RCS or the steam generator, as required. Initially, realignment of two safety injection pumps to the steam generators would likely be required. Any remaining safety injection pump(s) could perform its normal reactor coolant inventory controls function. As AFW coolant demands decrease, an additional safety injection pump could be returned to its normal alignment.

- Valving is provided to align individual safety injection pump suctions to the refueling water storage tank (RWST) or to the condensate storage tank (CST), as required. Safety injection pumps performing a reactor coolant inventory control function would be aligned to the RWST and would provide borated water to the RCS. This would be the normal system alignment. When providing coolant to the steam generators, the corresponding pump suctions would be aligned to the CST, which is the normal water supply for the AFW system. This alignment would preserve the inventory of borated water in the RWST for primary coolant inventory control.

- Interlocks would be provided to match suction and discharge valve alignment if power-operated valves are used. This would prevent the inadvertent introduction of unborated water from the CST into the RCS. If manual valves are used, operating procedures must be developed to ensure proper valve alignment.

- Interlocks are provided to prevent realignment of safety injection pump discharges to the steam generators during large LOCA conditions. Heat removal via the steam generators is not required during large LOCAs. Suitable logic, such as the coincidence of low RCS pressure and high containment pressure, could provide the required interlocks.

- The physical connection between the safety injection system and the AFW system should be selected on a plant-specific basis. A possible location would be immediately upstream of the containment isolation valves in the AFW supply lines to each steam generator. No new containment penetrations or containment isolation valves would be required, and the impact of faults in the AFW system on the new backup AFW capability would be minimized. The interconnection should also be upstream of any valves operated by the AFW loop selection logic (if provided), which identifies and isolates a failed steam generator. This logic ensures that AFW flow is only provided to an intact steam generator.

- Electrical separation and independence of safety injection trains must be maintained throughout the interconnection with the AFW system.

ASSUMPTIONS

This analysis assumes that the interconnect between systems is done after a plant by plant examination, and that procedures and hardware development preclude inadequate core coolant inventory when a portion of the safety injection system is serving to provide water to the AFW. This analysis also assumes that the physical interconnect is either a temporary spooling piece or that interlocks are provided which prevent an interfacing LOCA condition. With these assumptions the advantage of installing a backup water supply to the auxiliary feedwater system (AFWS) is assumed to increase its availability in affected dominant accident sequences where AFWS parameters influence core melt frequency.

AFFECTED PARAMETERS

The system parameters affected are those influencing the unavailability of the AFWS. It is assumed that only parameters associated with AFW are affected and that the availability of the control signal path is unchanged. For the adjusted case it is assumed that operator action and timing are critical to realignment of valves and spool pieces, if used. Therefore, a 20 percent decrease in unavailability of the AFWS turbine-driven pump as a part of LF-EFS-E11 is assumed in the adjusted case.

Parameter	Base-Case Value	Adjusted-Case Value
LF-EFS-E11	3.7E-03	3.0E-03

Base-Case Affected Core Melt Frequency	Adjusted-Case Affected Core Melt Frequency	Change in Core Melt Frequency
8.78E-06/ry	7.13E-06/ry	1.6E-06/ry

The reduction in CMF is then estimated to be 1.6E-06/ry.

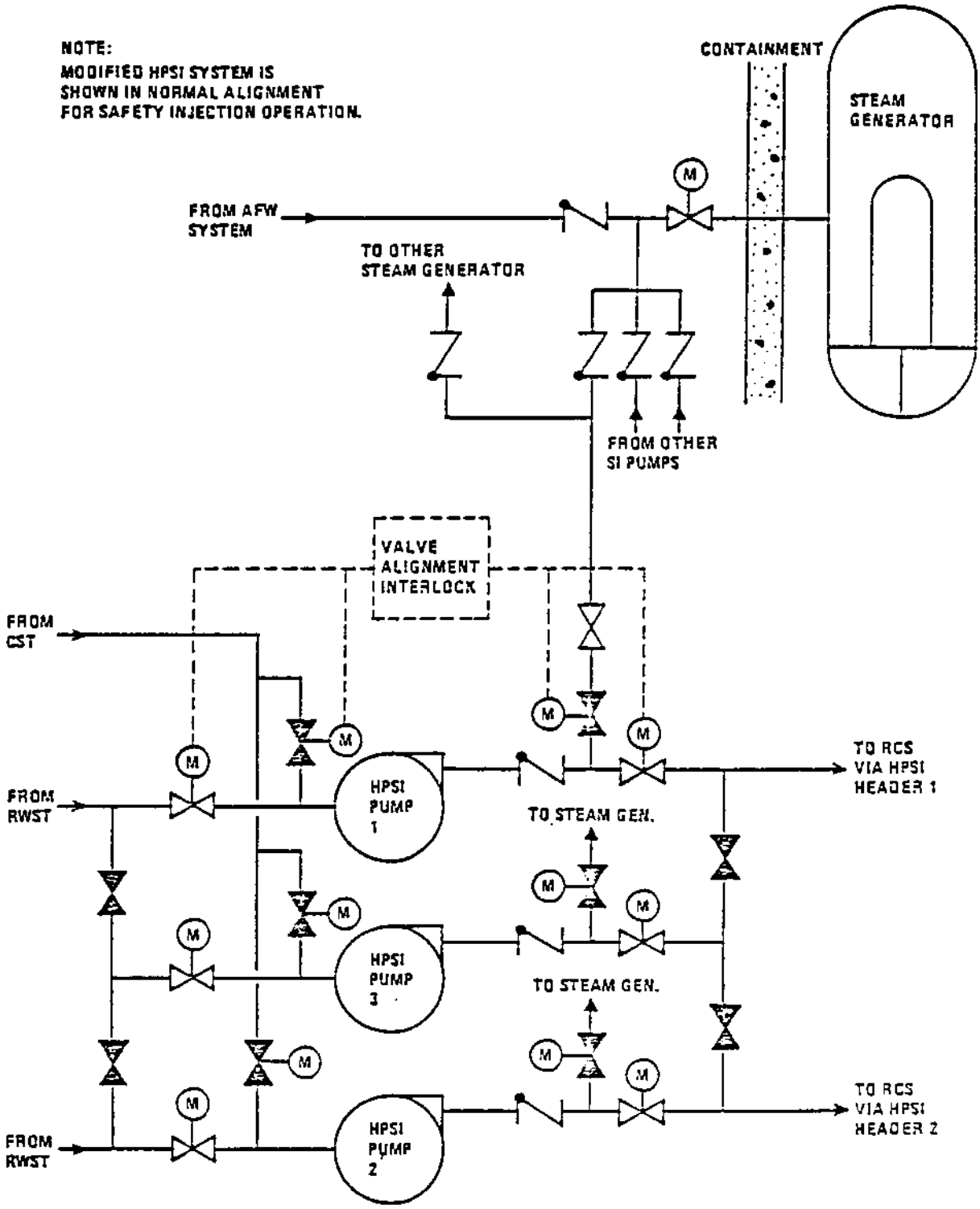

FIGURE A.2. Modifications to HPSI System to Provide Backup AFW Capability (U.S. NRC 1982a)

STAT ALTERNATIVE 10:

SPRING-LOADED SAFETY VALVES FOR VENTING STEAM GENERATORS

The purpose of this proposed STAT alternative is to provide a decay heat removal and overpressure protection capability by venting the steam generators to the atmosphere via the main condensers or supplying additional secondary side spring-loaded safety valves in the event that main steam line safety valves and the power-operated atmospheric dump valves are disabled.

Each main steam line from the steam generator to the main steam isolation valve (MSIV) has both spring-loaded safety valves and power-operated atmospheric dump valves. These provide overpressure protection for the secondary side of the steam generator and the main steam piping as well as the controlled removal of reactor decay heat when the condenser is not in service and in conjunction with the auxiliary feedwater system when the main feedwater system is not in service (e.g., following loss of offsite power, or LOOP).

Figure A.3 illustrates a simplified diagram of the safety valves and the main turbine bypass system (TBS). The TBS system is automatically actuated and designed to limit the main steam pressure following different transients and for decay heat removal when the condenser is available as a heat sink. The turbine bypass capacity in PWR plants is in the range of 15 to 85 percent of the rated main steam line flow. However, the TBS is not available when the main condenser vacuum is less than the setpoint value (approximately 18 inches Hg absolute). This condition would likely occur following loss of the main circulating water system, loss of air ejectors and LOOP. In addition, the bypass valves fail closed on loss of pneumatic system pressure or electrical power to the control system or solenoid pilot valve (U.S. NRC 1982a).

It should also be noted that the MSIVs are required to be open during bypass operations and that the valves fail closed on loss of hydraulic system pressure or loss of electric power to the MSIV control system. Conditions that may initiate MSIV closure include, among other things, high or low steam generator pressure (U.S. NRC 1982a).

The sabotage scenario assumes a LOOP, a turbine trip, and a TBS unavailability due to LOOP. This results in reduced flow from the steam generators to the turbine and an increased pressure in the steam generator secondary side and main steam lines. Under these conditions pressure would normally be controlled by releases via the safety valves. Under postulated sabotage conditions all safety valves are assumed to be forced closed, which negates overpressure protection for the steam generator and main steam lines, causing potential overpressurization of the system.

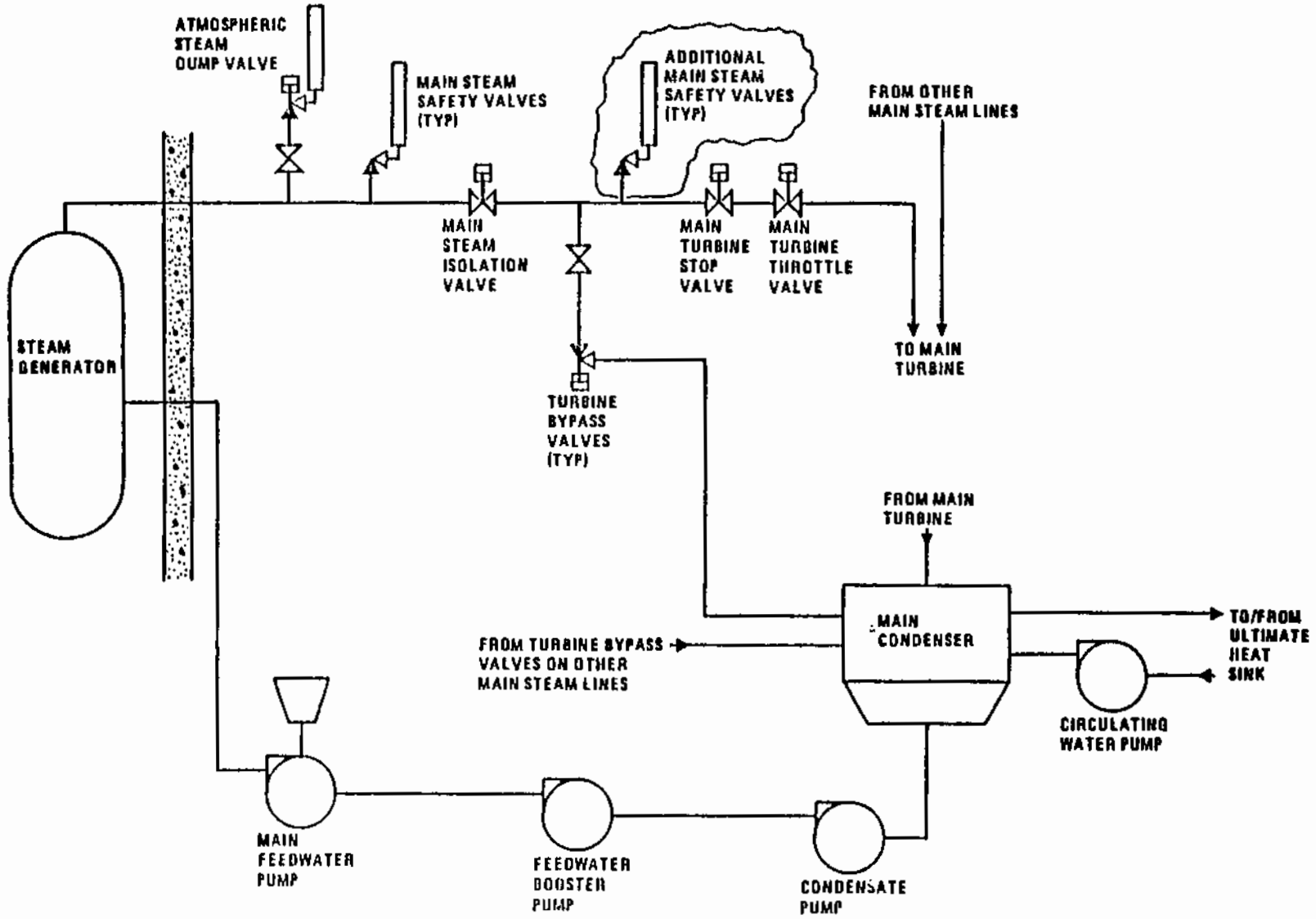

FIGURE A.3. Simplified Main Turbain Bypass System Diagram (U.S. NRC 1982a)

Under normal operating conditions there are two ways in which the addition of spring-loaded safety valves can affect the probability of core melt. These include the unavailability of the valves when demanded open and the failure of the valves to close following a demand. Neither of these scenarios is considered a dominant accident sequence in the ANO-1 representative PRA. However, in an effort to estimate the order of magnitude effect on core melt frequency when installing additional safety valves, the first scenario is investigated as the upper bound condition.

The initiating conditions assume LOOP (0.2/ry), turbine trip, and loss of TBS. The latter two conditions are given in this scenario and are considered to have a probability of 1.0. A progression of events from this point includes reactor trip, demand for emergency power, and failure of the auxiliary feedwater system (AFWS). Assumptions here include a steam driven AFWS that needs no electrical power and failure of the AFWS at some point in time due to deadheading against steam pressure. At this point overpressure is assumed to occur and relief valves are demanded. A conservative assumption is that the relief capacity of each valve is between 750 and 1050 klb/hr. Assuming a total rated main steam flow of approximately 8000 klb/hr, 8 valves would be required. If the plant had a maximum of 20 valves, 13 would have to fail in order to have overpressure conditions. The probability of failing 13 of 20 valves in parallel, assuming a single failure probability of 1E-05, is calculated below:

$$P(13/20) = \sum_{n=13}^{20} \frac{20!}{n!(20-n!)} \quad (1E\text{-}05)]^{(20-n)}$$

$$P(13/20) = \leq 1E\text{-}08 \qquad \text{insignificant}$$

Figure A.4 illustrates the event sequence up to the random failure of all safety valves under normal conditions. This sequence could continue to core melt by postulating additional failures on the primary side. For example, decay heat removal requirements would demand relief valves and high pressure injection, and a feed-and-bleed scenario might progress. These additional events have not been analyzed because the failure probability is already much less than E-08.

AFFECTED PARAMETERS

Resolution of this sabotage issue affects the number of safety valves on the main steam line. Assuming that the number of total relief valves is increased by 50% and that 8 valves are still required to vent total steam pressures, the failure probability would now be calculated assuming 23 valve failures out of 30 valves. The probability of 23 random failures is also insignificant. Although there may be order of magnitude changes in core melt frequency due to resolution of this issue, core melt frequencies still approach zero. Therefore, the resolution of this issue is assumed to have an insignificant contribution to core melt frequency.

pressures, the failure probability would now be calculated assuming 23 valve failures out of 30 valves. The probability of 23 random failures is also insignificant. Although there may be order of magnitude changes in core melt frequency due to resolution of this issue, core melt frequencies still approach zero. Therefore, the resolution of this issue is assumed to have an insignificant contribution to core melt frequency.

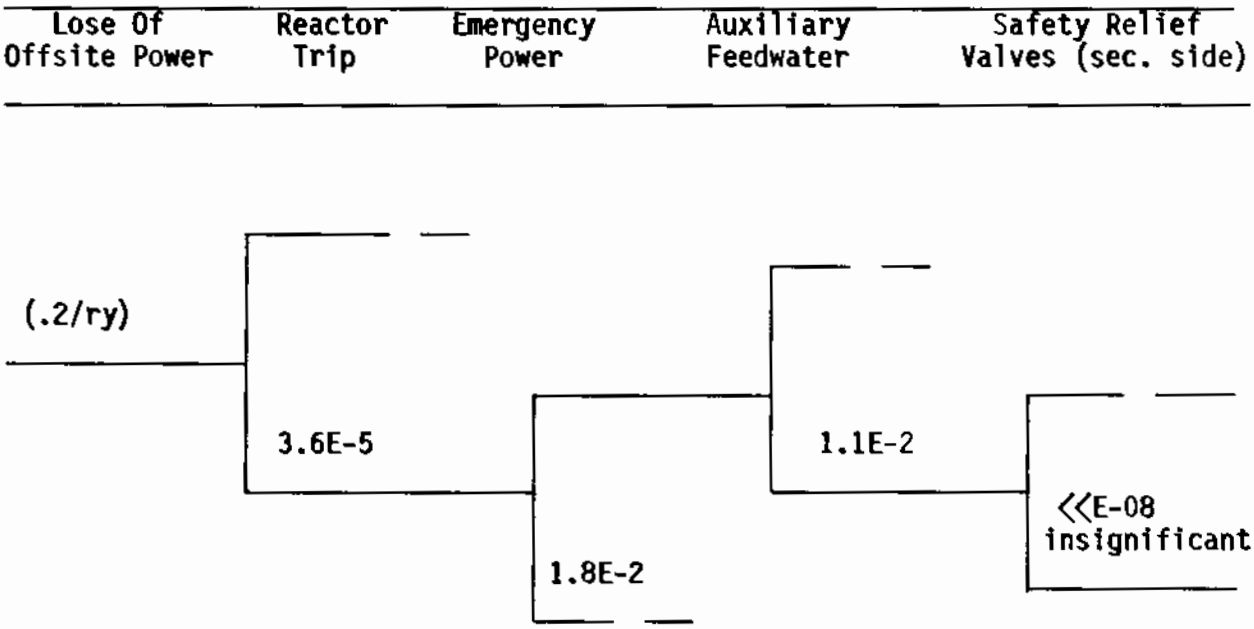

FIGURE A.4. Events Leading to Safety Relief Valve Failures on Secondary Side (probabilities from NUREG/CR-2497, Minarick and Kukielka 1982; and NUREG/CR-2800, U.S. NRC 1983c)

STAT ALTERNATIVE 11:

USE FIRE WATER AS A SOURCE OF COOLING RHR HEAT EXCHANGERS

The essential service water (ESW) system in a BWR is used to transfer heat from the residual heat removal (RHR) heat exchangers to the ultimate heat sink during normal and emergency conditions. The ESW system is also used to remove heat directly from several components, including diesel generator cooling systems and several safety-related pump and room coolers (e.g., LPCI, LPCS, RHR, RCIC, HPCI, and HPCS pump and room coolers). The ESW system typically consists of three independent trains with one train assigned to provide cooling to the high-pressure coolant systems after an accident. The other two trains supply cooling water to safety- and nonsafety-related components and are in operation during normal plant conditions.

The sabotage scenario associated with this STAT alternative assumes that a loss-of-offsite-power transient occurs coincidentally with successful sabotage of the ESW pumps that supply cooling water to the suppression pool cooling or RHR heat exchangers (in most BWR plants, these are the same heat exchangers). The RCIC, HPCS, and HPCI systems operate to maintain coolant inventory. These systems maintain reactor coolant level and exhaust to the suppression pool. The heated water in the suppression pool is then pumped through the RHR heat exchangers, where the decay heat is transferred to the ESW system and then to the ultimate heat sink. The RHR (or suppression pool cooling) system is operable, but a complete heat transfer path to the ultimate heat sink cannot be established because no coolant flow path to the secondary side of the RHR heat exchanger is available. Under these conditions, suppression pool temperature will continue to rise unless an alternative source of service water can be established. This proposed STAT alternative would use the plant fire water system as an alternative coolant supply for the secondary side of the RHR heat exchanger.

ASSUMPTIONS

It is assumed here that major fire water system design changes are implemented. The design changes would include increased pumping capabilities to provide both fire protection and alternative ESW services. It is also assumed that the fire protection system pumps will be supplied with Class 1E electric power or will be diesel-engine driven so they will be operable following a loss of offsite power.

AFFECTED PARAMETERS

Using the fire protection system as an alternative coolant source the ESW system effectively provides an additional coolant flow path to transfer heat from the RHR heat exchangers to the ultimate heat sink. This would increase the availability of coolant for component cooling.

To determine the impact of this STAT alternative, the availability of fire water has been added to appropriate cut sets in the PRA. Based upon available data, it is assumed that the failure probability (unavailability) of fire water is 0.1. This is a conservative estimate and considers the inadequacy of the current design and capacity of the fire water system. In other words, this is like increasing the availability of coolant for component cooling by a factor of 10.

This STAT alternative provides alternative ESW coolant capabilities similar to STAT Alternative 15, which uses the nonsafety plant service water system as an alternative source of ESW system cooling water. Use of the fire protection system to provide this capability would produce an equivalent change in core melt frequency because both "fixes" essentially add redundancy to the ESW system; i.e., both fixes add an additional ESW system pump train. As a result, the effect on core melt frequency for implementing this STAT alternative would be equivalent to the change in core melt frequency estimated for STAT Alternative 15. The reduction in core melt frequency is therefore estimated to be 2.4E-05/ry.

STAT ALTERNATIVE 12:

CONNECT SI PUMPS IN SERIES TO RAISE DISCHARGE PRESSURE

This STAT alternative would allow the connection of high pressure safety injection (HPSI) pumps in series, to increase the resulting injection pressure above reactor coolant system (RCS) safety valve operating pressure. This is needed to allow core cooling when all feedwater, i.e., both main feedwater (MFW) and auxiliary feedwater (AFW), is lost.

When all feedwater is lost to the steam generators, they rapidly boil dry. Consequently this path of heat removal from the reactor core is lost. RCS temperature and pressure increase until power-operated relief valves (PORVs) and safety valves open at about 2500 psig. This provides an adequate heat removal path from the core into the containment as long as RCS inventory is maintained and the core is covered.

In more than half of the operating plants the HPSI systems cannot produce sufficient pressure to inject against safety valve operating pressure (approximately 2500 psig). Normal charging pumps, which can inject against this pressure, provide insufficient flow to compensate for relief/safety valve losses when steam generator cooling is lost. Consequently reactor vessel water level will drop, reaching the top of the core roughly an hour after feedwater loss. This STAT alternative would allow adequate HPSI flow to keep the core covered when steam generator cooling is lost.

In the sabotage scenario, a loss of offsite power is assumed to occur coincidentally with a loss of main and auxiliary feedwater. This results in reactor and turbine trip, and a need for high pressure safety injection at system design pressure. Emergency diesel generator operation is not affected; the generators start and supply the emergency busses.

Aligning the HPSI pumps in series may increase output pressure, but the adequacy of flow is uncertain for all scenarios.

ASSUMPTIONS

It is assumed that all valves and plumbing to allow the option of HPSI pump operation in series is made to the plant.

Due to the complex nature of this STAT alternative and the limited resources to perform the analysis, the change in core melt frequency due to implementing this alternative is assumed to be 10 percent of the total core melt frequency of ANO-1 (5.1E-05/ry). The reduction in core melt frequency is thus 5.1E-06/ry.

STAT ALTERNATIVE 13:

USE CONTROL ROD DRIVE HYDRAULIC SYSTEM TO SUPPLY REACTOR COOLANT MAKEUP IN A BWR

The control rod drive hydraulic system (CRDHS) supplies pressurized water to operate and cool the control rod drive mechanisms. The CRDHS typically has two 100 percent capacity pumps, each capable of delivering approximately 100 gpm at reactor operating pressure (about 1000 psig). These pumps take suction from the condensate storage tank, and the water used to perform the CRDHS functions is ultimately discharged to the reactor vessel.

In the sabotage scenario, it is assumed that a loss-of-offsite-power transient occurs coincidentally with successful sabotage of the high pressure injection systems, which may include the reactor core isolation cooling (RCIC) system, the high pressure core injection (HPCI) system, the high pressure core spray (HPCS) system, or the feedwater coolant injection (FWCI) system. The proposed STAT alternative would use the CRDHS as an additional high pressure injection system. Availability of any of the other high pressure injection systems would negate the need for using the CRDHS as a source of high pressure coolant makeup. It is assumed that low pressure injection systems are unavailable due to the inability of the operator to actuate the automatic depressurization system (ADS); i.e., failure to depressurize the reactor vessel to the point where the low pressure systems can be used.

ASSUMPTIONS

It is assumed here that the necessary water connections for water supply and controls are added to the CRDHS to allow its use as a source of high pressure reactor coolant makeup. The CRDHS pumps are powered from the Class 1E electrical system and are considered nonsafety loads. This means that an operator must start the CRDHS pumps manually after a loss-of-offsite-power transient occurs and the diesel generators are energized. Failure of these pumps to start after an accident occurs was not examined.

The proposed STAT alternative could not be implemented without significant plant changes. These changes would be needed to provide additional pumping capacity and larger piping and valves. The plants are assumed to implement these changes. The unavailability of the CRDHS to provide coolant to the core is assumed to be modeled similarly to the RCIC and HPCS systems. For these systems, it was determined (see the Grand Gulf PRA [Hatch et al. 1982]) that greater than 40 percent of the unavailability was a result of combined hardware and maintenance unavailability. This was assumed to apply to the modified CRDHS.

AFFECTED PARAMETERS

Using the CRDHS as a potential source of high pressure reactor coolant makeup is not modeled in WASH-1400 or the Grand Gulf RSSMAP. To estimate the

impact of this STAT alternative on plant safety, the frequencies of events involving unavailability of the high pressure injection systems were adjusted to account for an additional flow path. The first step was to review the Grand Gulf LOCA and transient event trees and identify the accident sequences that include failure of the high pressure injection systems. The affected accident sequences are:

- T_1QUV: loss-of-offsite-power transient followed by failure of the power conversion system (Q), and failure of the high pressure systems (U) and low pressure injection systems (V) to provide emergency core cooling. The frequency of this accident sequence is:

  $T_1QUV = 1.9E-06$

- T_1PQE: loss of offsite power followed by a stuck-open relief valve (P), which leads to a LOCA. All emergency core cooling systems, including high and low pressure systems, are unavailable (E). The frequency of this sequence is:

  $T_1PQE = 2.3E-07$

- T_{23}PQE: transients other than loss of offsite power followed by a stuck-open relief valve and failure of all emergency core cooling systems (E). The frequency of this sequence is:

  $T_{23}PQE = 5.4E-07$

  The Boolean equation used to model event U is:

  U (base case) = HPCS * RCICS = 1.7E-03

  This equation was modified to account for the increased availability of high pressure coolant as follows:

  U (adjusted case) = HPCS * RCICS * CRDHS = 1.7E-3 * CRDHS

It is assumed that the unavailability of the CRDHS is equivalent to the unavailability of the HPCS (3.3E-2). Substituting this value into the latter equation results in a new value of 5.6E-05 for the adjusted-case U. The next step was to substitute the adjusted-case U into accident sequence T_1QUV along with known values for the parameters T_1 (0.2/ry), Q (1), and V (4.4E-03). The adjusted-case frequency for this accident sequence is then 4.9E-08/ry.

This represents approximately a factor of 30 reduction in core melt frequency for this particular accident sequence.

A similar procedure was followed to estimate adjusted-case frequencies for the other two accident sequences. This involved calculating base-case and adjusted-case values of E for T_1 and T_{23} transients. Both accident sequences are initiated by a transient but become small LOCAs because of a stuck-open relief valve.

The base-case value of E, which is defined as the failure of the emergency core cooling system to provide reactor coolant makeup, was calculated by solving the Boolean equations for E and substituting known values of T_1 and T_{23}, P, and Q. These equations take the form:

$$E(T1) = (2.3E\text{-}07) / T_1PQ = 1.25E\text{-}05$$

$$E(T23) = (5.4E\text{-}07) / T_{23}PQ = 7.7E\text{-}07$$

The base-case Boolean equation that models event E for small LOCAs, as presented in the Grand Gulf RSSMAP, is:

E = RCICS * HPCS * ADS or HPCS * RCICS * LPCS * 2-out-of-3 LPCI

This equation was adjusted to account for the additional coolant makeup supply provided by the CRDHS as follows:

E (adjusted case) = RCICS * HPCS * ADS * CRDHS

or

HPCS * RCICS * LPCS * CRDHS * 2-out-of-3 LPCI

The value of E is different for T_1 (loss-of-offsite-power) and T_{23} (other than loss-of-offsite-power) transients. The adjusted-case values of E for these transients were calculated by substituting the parameter values from the Grand Gulf RSSMAP into the above equation. These values are:

HPCS(T1)	= 3.3E-02	LPCIA(T1)*	= 4.1E-02
HPCS(T23)	= 2.2E-02	LPCIB(T1)	= 4.1E-02
RCICS(T1 and T23)	= 5.2E-02	LPCIC(T1)	= 3.6E-02
LPCS(T1)	= 3.5E-02	LPCIA(T23)	= 2.8E-02
LPCS(T23)	= 2.2E-02	LPCIB(T23)	= 2.8E-02
		LPCIC(T23)	= 2.3E-02

* LPCIA refers to train A of the LPCI system.

As shown in the Boolean equation for E, there is a 2-out-of-3 failure criterion for the LPCI system. For a close approximation of the unavailability of the LPCI system, it was assumed that the unavailability of each loop was equal to the unavailability of the least reliable loop; i.e., loop A. The unavailability of a two-out-of-three system can then be approximated using the following equation (McCormick 1981):

$$\text{LPCI (2/3)} = 3(\text{LPCI})^2 - 2(\text{LPCI})^3$$

Then, the values of LPCI were calculated for T_1 and T_{23} type transients and substituted into the adjusted-case Boolean equation for E. The following adjusted-case values for E for both types of transients were determined:

E(T1) = 9.5E-08 E(T23) = 3.9E-08

These values were substituted for the base-case values of E in the accident sequences, as follows:

T_1PQE = (0.2)(0.1)(9.5E-08) = 1.9E-09/ry

T_{23}PQE = (7)(0.1)(3.9E-08) = 2.7E-08/ry

The next step was to multiply the adjusted-case accident sequence frequencies by the containment failure probabilities presented in Table B.3 of NUREG/CR-2800 (U.S. NRC 1983c). The adjusted-case core melt frequencies for each accident sequence were then substituted into Table B.1 of NUREG/CR-2800 to calculate the adjusted-case total core melt frequency. A revised Table B.1 is presented in Tables A.1 and A.2. As shown, the frequencies of the nondominant accident sequences were also assumed to be affected by this STAT alternative. It was assumed that the percent change in core melt frequency for nondominant accident sequences is equivalent to the percent change in dominant accident sequence frequencies. The frequencies of the nondominant accident sequences were adjusted by multiplying the adjusted-case dominant accident sequence frequencies by the ratio of the base-case nondominant accident frequency to the base-case dominant accident frequency. The overall reduction in core melt frequency is 3.0E-06. It should be noted that this is a first-order approximation based on available data. More detailed analyses are needed to further refine this estimate.

TABLE A.1. Grand Gulf Dominant Accident Sequences and Frequencies for the Base Case (reactor-year^{-1})

Accident Sequence	BWR Release Category (based on WASH-1400) 1	2	3	4
T_1PQI	1.6E-08	1.6E-06		
T_{23}PQI	3.7E-08	3.7E-06		
T_1PQE			1.2E-07	1.2E-07
T_{23}PQE			2.7E-07	2.7E-07
SI	4.6E-08	4.6E-06		
T_1QW		6.2E-06		
T_{23}QW		1.2E-05		
T_{23}C		5.4E-06		
T_1QUV			9.5E-07	9.5E-07
Nondominant	1E-08		1E-07	3E-07
Total	1.1E-07	3.4E-05	1.4E-06	1.6E-06

Total Core Melt Frequency = 3.7E-05/ry

TABLE A.2. Grand Gulf Dominant Accident Sequencies and Frequencies for the Adjusted Case (reactor-year^{-1})

Accident Sequence	BWR Release Category 1	2	3	4
T_1PQI	1.6E-08	1.6E-06		
$T_{23}PQI$	3.7E-08	3.7E-06		
T_1PQE			9.5E-10	9.5E-10
$T_{23}PQE$			1.4E-08	1.4E-08
SI	4.6E-08	4.6E-06		
T_1QW		6.2E-06		
$T_{23}QW$		1.2E-05		
$T_{23}C$		5.4E-06		
T_1QUV			2.5E-08	2.5E-08
Nondominant	1E-08		3.0E-09	8.9E-09
Total	1.1E-07	3.4E-05	4.3E-08	4.9E-08

Total Core Melt Frequency = 3.4E-05/ry

STAT ALTERNATIVE 14:

USE MAIN CONDENSATE PUMP TO PROVIDE REACTOR COOLANT

The main feedwater (MFW) system supplies feedwater to the reactor vessel during normal operations. The system includes condensate pumps that draw suction from the main condenser hotwell. The flow is directed through a series of auxiliary condensers, a condensate cleanup system (demineralizers), feedwater heaters, and then through booster pumps. Flow may then be directed through additional feedwater heaters and then to the main feedwater pumps. From the main feedwater pumps, coolant is directed to the reactor vessel. The main feedwater and condensate systems are typically not available following a loss of offsite power. However, some plants use these systems in a high pressure coolant injection mode; these systems are referred to as the feedwater coolant injection (FWCI) system. Class 1E electric power is provided for the FWCI system. This issue only applies to the operating BWRs.

The sabotage scenario assumes that a loss-of-offsite-power transient occurs coincidentally with successful sabotage of all normal coolant makeup systems. These systems include the high pressure coolant injection systems (HPCI, HPCS, RCIC, FWCI) and low pressure coolant injection systems (LPCI, LPCS, and LPCI of the RHR system). The automatic depressurization system (ADS) cannot be activated automatically using the ADS actuation logic, but the control room operator can operate the safety relief valves using the individual valve control circuits. Thus, the reactor vessel can be depressurized, which makes it possible to use the main condensate pumps to restore core cooling. Suppression pool cooling is also needed, but it is assumed that the RHR system, which provides the suppression pool cooling function, has been sabotaged.

ASSUMPTIONS

This proposed STAT alternative would provide system connections necessary to use the condensate pumps for low pressure coolant makeup. This would include additional piping and valves to align the condensate pump suction with either the condensate storage tank or suppression pool and to align the discharge to the LPCS spray header. Electrical power must also be provided from a Class 1E source or from an alternative onsite source of Nonclass 1E power.

AFFECTED PARAMETERS

Using the condensate pumps as a source of low pressure coolant makeup is not modeled in WASH-1400 or the Grand Gulf RSSMAP. To estimate the impact of this STAT alternative on plant safety, the probabilities of high and low pressure coolant makeup system failure were adjusted to account for the additional flow path provided by the condensate system. The first step was to review the Grand Gulf LOCA and transient event trees and identify the accident sequences that include failure of the high and low pressure injection systems. The affected sequences are:

- T_1QUV: loss of offsite power followed by failure of the power conversion system (Q), the high pressure coolant systems (U), and low pressure coolant systems (V). The base-case frequency of this accident sequence is:

  T_1QUV = 1.9E-06/ry.

- T_1PQE: loss of offsite power followed by a stuck-open relief valve (P), which leads to a small LOCA. All emergency core cooling systems are unavailable (E). The base-case frequency of this sequence is:

  T_1PQE = 2.3E-07/ry.

- T_{23}PQE: transient other than loss of offsite power occurs followed by a stuck-open relief valve and failure of all emergency core cooling systems (E). The base-case frequency of this sequence is:

  T_{23}PQE = 5.4E-07/ry.

The parameters of concern here are V and E. The unavailabilities of these systems will be adjusted to account for the additional flow path provided by the main condensate system.

The Boolean equation used to model event V was:

V = ADS + LPCS * [(LPCIA * LPCIB) + (LPCIA * LPCIC) + (LPCIB * LPCIC)]

The final terms indicate that two out of three LPCI loops must operate for adequate core cooling. A base-case value of V can be calculated by substituting known values for the terms in the above equation. The following values were obtained from the Grand Gulf RSSMAP:

LPCS (T1)	= 3.5E-02	LPCIC (T1)	= 3.6E-02
LPCS (T23)	= 2.2E-02	LPCIA (T23)	= 2.8E-02
ADS	= 1.5E-03	LPCIB (T23)	= 2.8E-02
LPCIA (T1)	= 4.1E-02	LPCIC (T23)	= 2.3E-02
LPCIB (T1)	= 4.1E-02		

The base-case value of V for the T_1 sequence was determined to be 1.7E-03.

The Boolean equation for V was modified to account for the additional flow path provided by the main condensate system (MCS) as follows:

V = ADS + [MCS * LPCS * {(LPCIA * LPCIB) + (LPCIA * LPCIC) + (LPCIB * LPCIC)}]

It was assumed that the unavailability of the MCS is the same value as that used for the LPCS system. This is because the two systems would be similar and would also discharge coolant to the reactor vessel through the same core spray headers. The adjusted-case value of V for T_1 sequences then becomes 1.5E-03.

The adjusted-case frequency of accident sequence T_1QUV is the base-case frequency multiplied by the ratio of the adjusted-case $\bar{V}$ to the base-case V. This ratio is 1.5E-03/1.7E-03 or 0.88. The adjusted case frequency then becomes:

$$T_1QUV = 1.7E\text{-}06/ry$$

A similar procedure was followed to calculate the adjusted-case frequencies of the other two accident sequences. Event E, for small LOCAs, was modeled using the Boolean equation shown below:

E = (RCICS * HPCS * ADS) + (HPCS * RCICS * LPCS * 2-out-of-3 LPCI)

After substituting values for the parameters in the above equation and calculating E, it was found that the unavailability of E was dominated by the first term, which represents the unavailability of the high pressure systems and failure to depressurize the reactor vessel. This proposed STAT alternative would not significantly affect the value of E because it would not affect the first term. As a result, the frequencies of accident sequences T_1PQE and $T_{23}PQE$ would not be significantly affected.

The next step in the analysis was to multiply the adjusted-case frequency of the T_1QUV sequence by the containment failure probabilities given in NUREG/CR-2800. The adjusted-case accident frequencies were then substituted into Table 8.1 to calculate the adjusted-case core melt frequency. A revised Table B.1 is shown as Table A.3. As shown, the frequencies of the nondominant accident sequences were also assumed to be affected by this STAT alternative. It was assumed that the percent change in core melt frequency for nondominant accident sequences is equivalent to the percent change in dominant accident sequence frequencies. The frequencies of the nondominant accident sequences were adjusted by multiplying the adjusted-case dominant accident sequence frequency by the ratio of the base-case nondominant accident sequence frequency to the base-case dominant accident sequence frequency. The results are shown in Table A.3.

The overall reduction in core melt frequency that results from this proposed STAT alternative is the difference between the adjusted-case and base-case total core melt frequency. This is estimated to be 2E-07/ry.

TABLE A.3. Grand Gulf Dominant Accident Sequences and Frequencies (reactor-year^{-1})

Accident Sequence	BWR Release Category (based on WASH-1400)			
	1	2	3	4
T_1PQI	1.6E-08	1.6E-06		
T_{23}PQI	3.7E-08	3.7E-06		
T_1PQE			1.2E-07	1.2E-07
T_{23}PQE			2.7E-07	2.7E-07
SI	4.6E-08	4.6E-06		
T_1QW		6.2E-06		
T_{23}QW		1.2E-05		
T_{23}C		5.4E-06		
T_1QUV			8.5E-07	8.5E-07
Nondominant	1E-08		9.3E-08	2.8E-07
Total	1.1E-07	3.4E-05	1.3E-06	1.5E-06

Base-case core melt frequency = 3.71E-05/ry

Adjusted case core melt frequency = 3.69E-05/ry

Change = 2.0E-07/ry

STAT ALTERNATIVE 15:

CROSS-CONNECT SERVICE WATER WITH ESSENTIAL SERVICE WATER

The essential service water (ESW) system is used in a PWR to transfer heat from a component cooling water (CCW) system to the ultimate heat sink. Typically, this heat transfer occurs in a centralized heat exchanger that provides the cooling capability for several components. In a BWR, heat is transferred directly from the components that require cooling to the ESW system. The ESW system then transfers the heat to the ultimate heat sink. The ESW system is used during both normal operations and emergencies. A list of several important components cooled by the ESW systems at BWRs and PWRs is shown below.

BWR	PWR
Diesel generators (cooling system heat exchangers)	Reactor coolant pump coolers
HPCS pumps and room coolers	RHR or shutdown heat exchangers
LPCS pumps and room coolers	Control rod drive mechanism coolers
LPCI/RHR pumps, heat exchangers, and room coolers	Containment emergency fan coolers
RCIC room cooler	Diesel generator coolers
Containment spray/suppression pool cooling system pumps, heat exchangers, and room coolers	Room coolers (e.g., safety injection pump room, containment spray pump room, RHR pump room)
	RHR pump coolers
	LPSI and HPSI pump coolers
	Containment spray pump coolers

In the sabotage scenario associated with this STAT alternative, successful sabotage of the ESW system is assumed. This event is assumed to occur concurrently with a loss-of-offsite-power transient. The emergency diesel generators start up and operate to provide electric power to the Class 1E electrical system. If this occurs, the systems and components cooled by ESW would be operating without a heat sink and would begin to heat up. Component failure will occur unless flow in the ESW system can be restored. The STAT alternative would provide the capability to use the plant service water system (SWS), which is not a safety-related system, to provide cooling water flow to the components served by the ESW system. The nonsafety-related service water systems provide cooling water for nonsafety systems.

ASSUMPTIONS

This proposed STAT alternative could be implemented by providing cross-connections between the ESW system and the nonsafety service water system. It is assumed that the capability to rapidly restore ESW system flow will be provided by power-operated isolation valves in the ESW/nonsafety service water system cross-connection. Rapid realignment is needed to support operation of

the diesel generators, which would rapidly fail if cooling were not restored. It will also be necessary to restore electric power to the nonsafety service water system, which is not normally needed to operate under accident conditions.

AFFECTED PARAMETERS

Different approaches for PWR and BWR plants were used to estimate the reduction in core melt frequency associated with this STAT alternative. For PWRs, the ESW system is modeled in detail in NUREG/CR-2787 (Kolb et al. 1982) for ANO-1. Therefore, the effect on PWR core melt frequency can be estimated by assuming a percentage improvement in ESW system availability and calculating the effect on core melt frequency using the computer code. For BWRs, the ESW does not explicitly appear in the dominant cut sets for the dominant accident sequences. The approach to estimating the change in core melt frequency for BWRs will be described later.

The affected parameters for PWRs were identified by reviewing the ANO-1 PRA. The results of the review, which includes a list of dominant accident sequences and the ESW component failures which appear in the dominant cut sets, is shown below.

- $B(1.2)D_1$: Base-case frequency = 2.8E-06/ry

ESW Component Failures	Base-Case Unavailability
LF-SWS-S2	0.005

- $B(1.2)D_1C$: Base-case frequency = 4.4E-06/ry

ESW Component Failures	Base-Case Unavailability
LF-SWS-S1	0.005
LF-SWS-S2	0.005

- $B(4)H_1$: Base-case frequency = 1.4E-06/ry

ESW Component Failures	Base-Case Unavailability
LF-SWS-S2	0.005

- $T(D01)LD_{1YC}$: Base-case frequency = 3.1E-06/ry

ESW Component Failures	Base-Case Unavailability
LF-SWS-S1	0.005

- $B(1.66)H_1$: Base-case frequency = 1.2E-06/ry

  Dominant cut sets are the same as for sequence $B(4)H_1$.

The affected parameters are LF-SWS-S1 and LF-SWS-S2, which represent the pipe segments that contain the SWS pumps 4C and 4B, respectively.

Providing the cross-connection between the plant service water and ESW systems establishes an additional coolant flow path for safety-related components that require cooling. Thus, the proposed STAT alternative would increase the availability of LF-SWS-S1 and LF-SWS-S2 by an assumed factor of 10.

A list of the affected elements of the dominant cut sets is shown below. Also shown are the base-case and affected-case unavailabilities for each component.

Parameter	Base-Case Value	Adjusted-Case Value
LF-SWS-S1	0.005	0.0004
LF-SWS-S2	0.005	0.0004

The effect of these changes in parameter values was calculated using the ANO-1 computer code. The change in core melt frequency is 1.0E-08/ry.

For a BWR the affected elements of the Grand Gulf dominant cut sets are shown below. Also shown are the base-case and affected-case unavailabilities for each component. The affected parameters are SSA, SSB, and SSC, which represent the pipe segments that contain the SWS pumps A, 8, and C, respectively. Providing the cross-connection between the plant service water and the standby service water system (SSWS) establishes an additional coolant flow path for safety-related components that require cooling. Thus the proposed damage control measure would increase the availability of SSA, SSB, and SSC by an assumed factor of 10.

Parameter	Base-Case Value	Adjusted-Case Value
SSA	0.021	0.0021
SSB	0.021	0.0021
SSC	0.014	0.0014

The overall reduction in core melt frequency for this STAT alternative is the difference between the base-case and adjusted-case frequencies, or 2.4E-05/ry.

STAT ALTERNATIVE 16:

CROSS-CONNECT FIRE SYSTEM AND ESW SYSTEM

The essential service water (ESW) system in a BWR is used to transfer heat from the residual heat removal (RHR) heat exchangers to the ultimate heat sink during normal and emergency conditions. The ESW system is also used to remove heat directly from several components, including diesel generator cooling system and several safety-related pump and room coolers (e.g., LPCI, LPCS, RHR, RCIC, HPCI, and HPCS pump and room coolers). The ESW system typically consists of three independent trains with one train assigned to provide cooling to the high-pressure coolant systems after an accident. The other two trains supply cooling water to safety- and nonsafety-related components and will be in operation during normal plant conditions.

The sabotage scenario associated with this STAT alternative assumes that a loss-of-offsite-power transient occurs coincidentally with successful sabotage of the ESW pumps that supply cooling water to the suppression pool cooling or RHR heat exchangers (in most BWR plants, these are the same heat exchangers) and other components cooled by the ESW. The RCIC, HPCS, and HPCI systems operate to maintain coolant inventory. These systems maintain reactor coolant level and exhaust to the suppression pool. The heated water in the suppression pool is then pumped through the RHR heat exchangers, where the decay heat would be transferred to the ESW system and then to the ultimate heat sink. The RHR (or suppression pool cooling) system is operable, but a complete heat transfer path to the ultimate heat sink cannot be established because no coolant flow path to the secondary side of the RHR heat exchanger is available. Under these conditions, suppression pool temperature will continue to rise unless an alternative source of service water can be established. The proposed STAT alternative would use the plant fire water system as an alternative coolant supply for the secondary side of the RHR heat exchanger. This is similar to the "fix" proposed for STAT Alternative 15.

ASSUMPTIONS

It is assumed here that major fire water system design changes are implemented. The design changes would include increased pumping capabilities to provide both fire protection and alternative ESW services. It is also assumed that the fire protection system pumps will be supplied with Class 1E electric power or will be diesel-engine driven so they will be operable following a loss-of-offsite-power transient.

AFFECTED PARAMETERS

Using the fire protection system as an alternative coolant source for the ESW system effectively provides an additional coolant flow path to transfer heat from the RHR heat exchangers to the ultimate heat sink. This would increase the availability of the ESW system.

The alternative ESW coolant capabilities of this STAT alternative are similar to those of STAT Alternative 15, which uses the nonsafety plant service water system as an alternative source of ESW system cooling water. Use of the fire protection system to provide this capability would produce an equivalent change in core melt frequency because both fixes essentially add redundancy to the ESW pump system; i.e., both "fixes" add an additional ESW system train. As a result, the effect on core melt frequency for implementing this STAT alternative would be equivalent to the change in core melt frequency estimated for STAT Alternative 15. The reduction in core melt frequency is therefore estimated to be 2.4E-05/ry for a BWR, and 1.0E-08/ry for a PWR.

It should be noted that fires were not analyzed in the Grand Gulf (BWR) and ANO-1 (PWR) PRAs. Based on information in an unpublished NRC report titled Insights Gained from Probabilistic Risk Assessment, the contribution to core melt frequency from fires ranges from 25 percent to 40 percent of the total core melt frequency in the three plants analyzed. Without more detailed design information, it is not possible to estimate whether the availability of the overall fire protection system will be increased or decreased due to being cross-connected to the ESW system. Therefore for this analysis, no change in fire protection system availability is assumed.

STAT ALTERNATIVE 17:

USE ESW TO DIRECTLY COOL COMPONENTS COOLED BY CCW

The component cooling water (CCW) system in a PWR provides an intermediate heat transfer loop between several plant systems and components and the essential service water (ESW) system. The CCW system typically consists of CCW pumps to circulate cooling water to the components requiring cooling and CCW heat exchangers to transfer the heat from the CCW system to the ESW system. The ESW system then transfers the heat to the ultimate heat sink. A list of components that are typically cooled by the CCW system includes reactor coolant pumps, emergency diesel generators, a shutdown cooling heat exchanger, and several safety-related pump and room coolers.

In this sabotage scenario, it is assumed that a loss-of-offsite-power transient occurs, followed by a trip of the power conversion system. It is also assumed that the normal CCW pumps have been disabled by sabotage. Under these conditions, components cooled by the CCW system heat up because there is no flow in the CCW system. The most critical components are likely to be the diesel generators, if they are cooled by the CCW system (at some plants, the diesel generators are cooled directly by the ESW system). This proposed STAT alternative would provide cross-connections, valves, and pumping capability needed to align the ESW system to directly cool the components normally cooled by the CCW system.

ASSUMPTIONS

It is assumed that the ESW pumps are capable of providing sufficient pumping capabilities to serve as backup for the normal CCW system pumps. ESW system pumps with sufficient shutoff head to reach the upper portions of the plant would need to be installed. In addition, a cross-connection from the ESW system to the CCW system would be needed to permit rapid realignment of the systems, particularly if the diesel generators were cooled by the CCW system. It should be noted that at ANO-1, most safety-related components are cooled directly by the ESW system and a central CCW heat exchanger is not used. For the purposes of this assessment, it is assumed that a central heat exchanger is provided at ANO-1.

AFFECTED PARAMETERS

The overall effect of this STAT alternative is to increase the availability of the components that are cooled by the CCW system. This is analogous to saying that implementation of this "fix" increases the availability of cooling water to cool these components. As a result, the change in core melt frequency can be estimated by reducing the unavailability of the events in the ANO-1 PRA that involve failure of one or more components of the ESW system, which could cause ESW cooling water flow to be unavailable. This approach also minimizes the effect of the assumption that a central CCW heat exchanger is provided at ANO-1 because both the approach and the assumption

assume that the unavailability of the CCW heat exchanger is nondominant. The affected elements of the dominant minimal cut sets, as shown in the ANO-1 PRA, are:

LF-SWS-S1	LF-SWS-S5	LF-SWS-S82
LF-SWS-S2	LF-SWS-S14	LF-SWS-S83

The next step was to adjust the values of the above terms to reflect their increased availability. It is assumed that the unavailability of coolant used for cooling of components will increase by a factor of 10 as a result of this STAT alternative, which requires that operators perform several actions to reestablish coolant flow to the components. The above assumptions were applied in the PRA by adding ESW to the appropriate cut sets. To be conservative, it was assumed that the failure probability of ESW is 0.1. The operator role was also quantified by assuming that there is a 50 percent probability that the operator will fail to realign the system. The net effect is then to multiply base-case valves by 0.5/10, or 0.05. The affected parameters and their base-case and adjusted-case values are shown below.

Parameter	Base-Case Value	Adjusted-Case Value
LF-SWS-S1	0.005	0.00025
LF-SWS-S2	0.005	0.00025
LF-SWS-S5	0.01	0.0005
LF-SWS-S14	0.01	0.0005
LF-SWS-S82	0.023	0.0012
LF-SWS-S83	0.023	0.0012

These values were input to the ANO-1 PRA to determine the change in core melt frequency. The reduction in core melt frequency was estimated to be 1.7E-06/ry.

STAT ALTERNATIVE 18:

LOCAL PRESSURIZER AND STEAM GENERATOR WATER LEVEL INDICATION

Steam generator and pressurizer level indications provide information via sensors and transmitter units to safety- and nonsafety-related instrumentation and control systems, and serve as information sources for control room operations. The purpose of this STAT alternative is to provide local steam generator and pressurizer water level indication in the event that the normal level indication has been disabled through sabotage.

Under normal conditions the loss of offsite power (LOOP) requires the auxiliary feedwater system (AFWS) for core cooling and the charging system or high pressure safety injection (HPSI) system for core coolant inventory control. The steam generator level indications provide input to the reactor protection system (RPS) to initiate reactor trip on steam generator low level, to the AFS for automatic actuation, and to the safety-related display instrumentation in the control room. In addition, the safety-related logic systems provide input to nonsafety-related systems to initiate turbine trip, main feedwater pump trip, and feedwater valve closure in the event of a high steam generator water level condition. The pressurizer provides input to the RPS for high-pressurizer level trip and to control room instrumentation. This information may also be provided to nonsafety-related systems (e.g., pressurizer heater control system and chemical and volume control systems for automatic control of charging pumps and letdown line flow) (U.S. NRC 1982a).

It is important to note that there are typically three to six independent safety-related channels monitoring steam generator water levels. The RPS and AFW actuation logic both use coincidence logic to compare multiple channels and determine the need for actuation. Plants have upgraded power supplies so that each integrated control system (ICS) bus and non-nuclear instrumentation bus (NNI) has two separate power supplies each, coming from a different bus. This action was in response to a review of past transients, which identified nonredundant power supplies as vulnerable to single failures with resulting significant consequences. According to NUREG/CR-2787 (Kolb et al. 1982), power supply failure or malfunction to or from the ICS/NNI was the only event found which could "cause both loss of main and emergency feedwater flow. In addition, the ICS has shown a tendency to cause feedwater oscillations, which have led to high reactor coolant trips, low reactor coolant trips, actuation of engineered safety systems, loss of main feedwater and loss of emergency feedwater." Critical control room indications have been lost and resulting dryout, overfill, and depressurization of both steam generators have occurred (Kolb et al. 1982).

The postulated sabotage scenario suggests a loss of primary indications required for the operator to assess the adequacy of core cooling and coolant inventory. This scenario may entail disabled the station batteries, major instrument cable runs, or instrument cabinets. The fixes include the provision of level gauges inside containment; level gauges outside containment; or portable, self-powered, calibrated level instruments that can be connected to signal cables from selected level transmitters.

ASSUMPTIONS

The basic assumption is that system failures are caused by loss of steam generator and pressurizer level signal transmission and that resolution of this issue provides only monitoring capabilities which allow for some increased probability of recovery in the progression to core melt. It is assumed that resolution only affects recovery from loss of these systems (e.g., AFS and HPSI), and initial system failures are not affected. It is further assumed that the affected accident sequences include nondominant accident sequences with the T(PSC) initiator and dominant sequences with the T(LOP) initiator.

AFFECTED PARAMETERS

Recovery factors are assumed to be the affected parameters for this issue. It is assumed that they apply to recovery of the AFS and HPSI in sequences where the initiating events are total interruption of the power conversion system and loss of offsite power. Below are the affected accident sequences for the representative plant (ANO-1) with the base-case core melt frequencies, which include recovery factors based on credit taken for recovery prior to resolution of this issue:

Parameter	Base-Case Sequence Frequency w/ Recovery (/ry)
T(PCS)LD1	3.9E-07
T(PCS)LQ-D3	8.8E-07
T(LOP)LD1	3.8E-07
T(LOP)LD1C	2.5E-07
T(LOP)LD1YC	9.9E-06

The adjusted case includes the new recovery factor (X) and is based on the assumption that the operator recognizes and acts on the need to monitor local gauges, and the probability that the action is correct. The resolution does not provide a significant incentive to increase the probability of the first action. Therefore, the probability that the operator fails to act given the new local monitor is 80 percent. However, assuming that the operator acts (20 percent of the time), the high probability that operator actions will be correct is assumed (assume a failure probability of 40 percent). This means that the probability of nonrecovery due to resolution is 0.80 + (0.20 * 0.40) = 0.88. The factor X becomes an additional factor in each of the sequences:

Parameter	Base-Case Sequence Frequency w/ Recovery (/ry)
T(PCS)LD1X	3.43E-07
T(PCS)LQ-D3X	7.74E-07
T(LOP)LD1X	3.34E-07
T(LOP)LD1CX	2.20E-07
T(LOP)LD1YCX	8.71E-06

Applying these assumptions to the previous parameters results in a reduction in core melt frequency of 1.6E-06/ry.

STAT ALTERNATIVE 19:

LOCAL READOUTS FOR STEAM GENERATOR PRESSURE

The purpose of this proposed STAT alternative is to provide local readouts for steam generator pressure in the event that this indication is lost in the control room and at the emergency shutdown panel due to sabotage. Proposed methods for providing local indication of steam generator pressure include 1) replacing the main steam line sensor/transmitter with a unit that has a local readout, 2) providing a portable calibrated gauge that could be connected to a pressure sensing line (e.g., a blowdown valve), 3) providing a portable, calibrated pressure unit with a self-contained DC power supply and appropriate leads to connect to pressure sensor terminals in instrumentation cabinets or control boards, and 4) installing separate local pressure gauges with physical protection (U.S. NRC 1982a).

Steam generator pressure sensors and transmitters are located inside containment, with signal cables penetrating containment to provide the communication link with instrumentation systems (e.g., RPS, ESFAS), indicators, recorders, and a computer system. Other pressure sensors monitor main steam line pressure. These are located between containment and the main steam isolation valves (MSIVs) and provide a good indication of steam generator pressure.

Past experience has shown that loss of the integrated control system (ICS) and non-nuclear instrumentation (NNI) power has caused depressurization of steam generators, which has led to isolation of main and emergency feedwater flow to the steam generators. This has been attributed to the design of the steam generator isolation logic (Kolb et al. 1982).

The sabotage scenario assumes that offsite power is lost and that instrumentation systems that receive Class 1E power function normally except that all steam generator pressure and main steam line pressure indication on the steam generator side of the MSIVs has been disabled by sabotage action (U.S. NRC 1982a).

ASSUMPTIONS

It is assumed that a loss of offsite power exists and that the low steam generator signal actuates emergency feedwater (EFW) system and the emergency feedwater initiation and control (EFIC) system in the representative plant (ANO-1). The EFIC performs the function of steam generator isolation after depressurization and approach to overfill. Since the EFIC-related failures are only expected to cause failure of the power conversion system, they were not considered as individual initiating events. These failures were considered as part of the nondominant accident sequences with the T(PCS) initiators (Kolb et al. 1982). It is also assumed that installation of local pressure indicators does not in itself change the probability of system failures, although increased monitoring of system pressure could potentially avert failures. It is assumed

here that the addition of monitoring equipment would more likely provide monitoring capability for recovery from system failures.

AFFECTED PARAMETERS

Recovery factors are assumed to be the affected parameters for this sabotage issue. Potential recovery of the EFW and EFIC systems are considered. Initiators considered include loss of offsite power, causing transients, and loss of the power conversion system, causing transients and transient-induced LOCAs. The affected accident sequences for the representative plant with the base-case core melt frequencies, which include recovery factors based on credit taken for recovery actions prior to resolution of this issue, are:

Parameter	Base-Case Sequence Frequencies with Recovery (/ry)
T(PCS)LD1	3.9E-07
T(PCS)LQ-D3	8.8E-07
T(LOP)LD1	3.8E-07
T(LOP)LD1C	2.5E-07
T(LOP)LD1YC	9.9E-06

The adjusted case includes a new recovery factor (X) and is based on the assumption that the operator recognizes and acts on the need to recover plant conditions. The probability that the operator will fail to use the local monitoring gauges given an accident condition is assumed to be 80 percent. This assumes a probability of success of 20 percent. The probability that correct action is taken to avert core melt assumes that the appropriate human action is taken (assume a failure rate of 40 percent). The failure probability for X is 0.80 + (0.20 * 0.40) = 0.88. Therefore, X becomes an additional factor in each sequence, and the resulting adjusted-case sequence frequencies are:

Parameter	Adjusted-Case Sequence Frequencies with Recovery (/ry)
T(PCS)LD1X	3.43E-07
T(PCS)LQ-D3X	7.74E-07
T(LOP)LD1X	3.34E-07
T9LOP)LD1CX	2.20E-07
T(LOP)LD1YCX	8.71E-06

Applying these assumptions to above parameters results in a reduction in core melt frequency of about 1.6E-06/ry.

STAT ALTERNATIVE 20:

PROVIDE EMERGENCY AC POWER TO NONSAFETY-RELATED EQUIPMENT

This section addresses the use of plant emergency AC electrical systems to operate nonsafety systems that may be used to substitute for sabotaged safety systems. Specific system substitutions or realignments are considered in other STAT alternatives. For example, the essential service water system could be substituted for by the service water system, the fire water system, or the condensate system. Suppression pool feed-and-bleed cooling could be provided by the refueling water transfer system. However, these nonsafety systems generally cannot be connected to the plant Class 1E emergency AC power supply system. Since essentially all sabotage scenarios assume a coordinated offsite sabotage of incoming power sources, proposed modifications to the nonsafety systems required to allow their use in damage control must include provision of a source of AC electric power. This STAT alternative addresses modifications to allow their connection to the Class 1E power supply.

Because operation of the Class 1E emergency electrical power supply is essential to maintaining the plant in a safe shutdown condition, stringent design conditions are imposed upon this system and on any connections to non-Class 1E systems. In particular, two independent, separated, and redundant systems are required so that no single credible failure can prevent operation. During emergencies non-Class 1E loads must be automatically disconnected and prevented from automatic or manual connection until the transient is stabilized. The objective of these separation requirements is to create an independent Class 1E electrical system that can provide necessary power to safety related systems irrespective of faults in, or unavailability of, the nonCclass 1E system. This section addresses the potential effects of degradation of the reliability of the Class 1E system by modifications and interconnections required to allow the supply of electrical power to nonsafety systems as proposed in other STAT alternatives.

ASSUMPTIONS

Several STAT alternatives have been proposed which may require electrical power to be supplied to non-Class 1E systems. Descriptions of these measures are conceptual and lack engineering detail. Consequently, at best a general estimate of the effects of such interconnections can be obtained. It is assumed that the dominant effect on Class 1E system availability is the potential for operator error in manually disconnecting and connecting loads to a Class 1E bus (load shedding), which may lead to overloading and tripping the emergency diesel generator (EDG) supplying the bus. This effect is incorporated by increasing the probability of occurrence of a local fault in the EDG or associated support systems and control circuitry by a factor of 3.

It is assumed that only one of the EDGs is affected by the operator error. Due to the importance of the Class 1E system, it is assumed that emergency procedures directing circuit interconnections would prohibit disconnect/connect operations to more than one Class 1E bus at a time, and that they would prohibit

further such operations if they led to the trip of an EDG, until such time as the tripped circuit was recovered. It is, however, realized that by implementing this STAT alternative, the recovery of the power system is more likely. Therefore, the recovery factors C-14 and LOPNRL in ANO-1 and Grand Gulf, respectively, will then be reduced by a factor of 1/3.

AFFECTED PARAMETERS

ANO-1

For evaluation of the potential deleterious effects of interconnecting Class 1E and non-Class 1E systems in a PWR such as ANO-1, the parameter LF-AC-DG1 from ANO-1 is used. Its value is modified to reflect the assumed increase in probability of loss of EDG 1 and the Class 1E 4160 VAC bus A3, which it powers.

Parameter	Base-Case Value	Adjusted-Case Value
LF-AC-DG1	0.033	0.1
C-14	0.36	0.24

This STAT alternative is estimated to result in an increase in core melt frequency of about 1E-06/ry.

Grand Gulf

The Grand Gulf plant is used as representative of BWRs, affecting the variable Diesel1 and LOPNRL.

Parameter	Base-Case Value	Adjusted-Case Value
Diesel1	0.036	0.1
LOPNRL	0.1	0.067

Similar to ANO-1, this STAT alternative is estimated to result in an increase in core melt frequency of about 2.7E-06/ry.

STAT ALTERNATIVE 21:

PROVIDE CROSS-CONNECTION BETWEEN 125 V DC CLASS 1E AND NON-CLASS 1E POWER SYSTEMS

This STAT alternative would provide cross-connections to permit the non-Class 1E batteries to supply DC power to safety related systems when one or more Class 1E batteries are disabled. Tie circuits would be installed between 125 V DC busses in the Class 1E and non-Class 1E systems. Stringent controls would be imposed upon the bus tie circuits to maintain separation and independence of the Class 1E DC system. This includes the provision of removable disconnect links in each bus tie circuit and the provision of two circuit breakers in series located at different physical locations to minimize the likelihood of inadvertently or accidentally crosstying the circuits. Administrative controls over installation of the disconnect links would ensure that separation and independence of the Class 1E DC power system is maintained during all plant conditions when normal Class 1E power sources (battery and/or battery chargers) are available.

In the sabotage scenario a loss of offsite power is assumed to occur coincidentally with sabotage of one or more Class 1E batteries. At least one emergency diesel generator receives control power from an operable Class 1E DC supply and operates, providing Class 1E AC power to safety related systems.

ASSUMPTIONS AND AFFECTED PARAMETERS

It is assumed that the emergency diesel generator receiving control power from the inoperable Class 1E battery cannot be started without this power. Consequently, the coincident loss of offsite power and battery power result in loss of the associated Class 1E DC bus. It is therefore assumed that the effects of this transient may be estimated by adjusting the probabilities of loss and recovery of the 125 V DC Class 1E emergency safeguards busses D01 and D02 in the ANO-1 PRA.

The parameters T(D01) and T(D02) give the failure frequencies of busses D01 and D02. Loss of one of these busses is the initiating event for 5 of the 14 dominant accident sequences evaluated in the ANO-1 PRA. The ability to energize either of these busses from an alternative power source enhances the likelihood of recovery from such transients. Recovery requires correct operator action, including the physical installation of a removable disconnect link in the circuit. Installation must be prompt, within about 1 hour, to prevent core melt. It is assumed that the effects of DC bus failure can be remedied by disconnection of normal and battery power sources and connection of the appropriate non-Class 1E power supply. Incorporation of these effects into the analysis is accomplished by modifying the values of T(D01) and T(D02) to include an effective nonrecovery factor associated with completion of the bus tie circuit and removal of the fault at the bus.

It is assumed that there is roughly a 70 percent probability of an operator successfully completing the bus tie within the hour available to combat the transient. This is incorporated into the calculation by multiplying the values

of T(D01) and T(D02) by 0.3, the corresponding nonrecovery factor. For calculational simplicity, in the adjusted case this product is used in place of base-case values for these two parameters.

We recognize that this STAT alternative may also have detrimental effects. The ability to cross-connect Class 1E and non-Class 1E busses allows the opportunity for operator error and degradation of Class 1E bus independence by cross-connection during normal operation. This would increase the value of T(D01) and T(D02) above the base-case value, prior to multiplication by the nonrecovery factor of 0.3. If the increase were 50 percent and a nonrecovery factor of 0.2 were assumed, the adjusted-case value of T(D01) would be 0.3*T(D01), the same value assumed in the paragraph above. Since we cannot estimate more precisely, this value is assumed for this analysis.

Parameter	Base-Case Value	Adjusted-Case Value
T(D01)	0.018/ry	0.0054/ry
T(D02)	0.018/ry	0.0054/ry

Applying the above values to the ANO-1 PRA results in a reduction in core melt frequency of about 1.1E-05/ry.

STAT ALTERNATIVE 22:

PROVIDE MULTIPLE DC FEEDERS TO DESIGNATED DC POWERED COMPONENTS

This STAT alternative would provide multiple selectable feeders to designated DC powered components to allow them to be rapidly energized from an alternative feeder if power from the normal feeder source is lost. This feature is occasionally provided in nuclear power plants for certain equipment. Control circuits must be designed so that circuit breakers and/or transfer switches cannot automatically transfer loads between redundant power sources. This is to assure that no single interconnection failure can cause paralleling of Class 1E power supplies.

This STAT alternative is functionally similar to STAT Alternative 21 in that an alternative source of 125 V DC power is provided. In this case power is provided directly to selected components from an alternative Class 1E DC power supply bus, whereas in STAT Alternative 21 an alternative non-class 1E bus is connected to the normal power supply bus via bus tie circuits. In this case the selected components can be directly energized even if their normal supply bus is disabled.

In this sabotage scenario a loss of offsite power is assumed to occur coincidentally with sabotage of a Class 1E DC bus. At least one emergency diesel generator receives control power from an operable Class 1E DC supply and operates, providing Class 1E AC power to safety systems.

ASSUMPTIONS

The effect of supplying DC power by feeder lines is almost the same as that of reenergizing the disabled bus if all loads are energized. It is assumed that this is the case for this STAT alternative. Thus, by the use of transfer switches for the feeder lines to individual loads, DC power is reestablished to the loads as if the bus function had been recovered. Consequently, as was discussed for STAT Alternative 21, this effect can be incorporated into the calculation by modifying the probabilities of loss and recovery of the 125 V DC Class 1E emergency safeguards busses D01 and D02 in the ANO-1 PRA. The following discussion parallels that for Alternative 21 with one significant exception. Simultaneous loss of busses D01 and D02 is nonrecoverable for this alternative, since these busses are the only sources of Class 1E DC power. In Alternative 21 it was recoverable because use of an operable non-Class 1E bus was assumed.

As discussed under Alternative 21, it is assumed that the effects of energizing components normally supplied by either bus D01 or D02, by connecting them to the alternative bus by independent feeder lines, can be accomplished by modifying the values of T(D01) and T(D02) to include the effects of recovery. Specifically, adjusted-case values are obtained by multiplying base-case values by 0.3, an effective nonrecovery factor representing an approximate 70 percent likelihood of completing all transfer switching correctly. This value is the same as that used for Alternative 21.

The important difference between this case and Alternative 21 is in the nonrecoverability of the simultaneous loss of busses D01 and D02. In the ANO-1 PRA this is found in the cut sets T(D01)*LF-DC-D01 and T(D02)*LF-DC-D01. In these cut sets, for which the PRA already assumes a nonrecovery factor of 1.0, the adjusted-case values of T(D01) and T(D02) should be the same as those for the base case.

Parameter	Base-Case Value	Adjusted-Case Value
T(D01)*	0.018	0.0054
T(D02)*	0.018	0.0054
T(D01)**	0.018	0.018
T(D02)**	0.018	0.018

* Value used in all cut sets except T(D01)*LF-DC-D02 and T(D02)*LF-DC-D01.
** Value used only in the cut sets T(D01)*LF-DC-D02 and T(D02)*LF-DC-D01.

Applying the above values to the ANO-1 PRA results in a reduction in core melt frequency of about 7.2E-06/ry. It should be noted that this STAT alternative could not be modeled adequately in the representative BWR PRA. Therfore, it was assumed that the derived benefit from implementation of this alternative would be the same for both BWRs and PWRs.

STAT ALTERNATIVE 23:

PROVIDE AN ALTERNATE WATER SOURCE TO MAINTAIN COOLANT INVENTORY

The purpose of this STAT alternative is to provide alternative water sources to maintain reactor coolant inventory and to remove decay heat during hot shutdown. Normally, these functions are performed at high pressure in a PWR by the emergency feedwater system (EFS), which is also called the auxiliary feedwater system at some plants. The EFW system supplies water to the secondary side of the steam generators to remove decay heat from the reactor coolant system. The steam is then vented to the atmosphere. The normal water source for the EFW system is the condensate storage tank (CST). Other water sources are also typically available, such as the condenser hotwell, the service water system, fire protection system, or other auxiliary water supplies.

In the sabotage scenario, it is assumed that the normal sources of water for the EFS are disabled by sabotage. A coincident failure of offsite power causes the turbine to trip and the plant to shut down. Reactor core decay heat removal is being performed by the EFW system. If the shutdown cooling system (or residual heat removal system) is available, the EFS will be used to cool and depressurize the reactor coolant system to the point where the shutdown cooling system can be used. Sabotage actions may prevent this transition. Thus, the EFS must be used for long-term decay heat removal with the plant in hot shutdown. Since the EFW system is open-loop, this may increase the ultimate heat sink water requirements. For this STAT alternative, it is assumed that adequate water supplies are available onsite to permit long-term maintenance of a hot shutdown condition. A number of valves and cross-connections would be needed to permit realignment of the potential water sources to provide water to the EFS.

ASSUMPTIONS

This proposed STAT alternative could be implemented by providing interconnections to permit operators to rapidly realign the EFS pump suction when needed. The pumps used to supply water from the alternative sources are assumed to be available following loss of offsite power. In addition, the capabilities of these pumps are assumed to be compatible with the requirements of the pumps that are utilizing the alternate water source. Booster pumps may be needed but are not recommended because they present additional targets for sabotage actions. It is assumed that these "fixes" have been made and the plant is fully capable of providing alternate EFS water sources.

AFFECTED PARAMETERS

The ANO-1 PRA was reviewed to identify events involving the EFS. It is assumed that this STAT alternative will significantly reduce the unavailability of providing water to the EFS. This has been presented in the PRA by reducing the unavailability of LF-EFS by a factor of 10. The effect is similar to adding another term (alternative water source) to the appropriate cut sets and assuming a failure probability of 0.1 for that term:

Parameter	Base-Case Value	Adjusted-Case Value
LF-EFS-E22	3E-04	3E-05

The change in core melt frequency that would result from implementing this STAT alternative is the difference between the base-case and adjusted-case core melt frequencies; the reduction in core melt frequency is estimated to be 5E-07/ry.

STAT ALTERNATIVE 24:

PROVIDE A STANDBY NON-CLASS 1E COMBUSTION TURBINE GENERATOR

Nuclear power plants are provided with several systems that are capable of maintaining the plant in a safe shutdown condition. These systems can be categorized as either safety related or nonsafety related, depending on their importance to the plant's response to accident conditions. In general, safety-related systems and components must be designed to withstand credible accident conditions such as earthquakes and floods without failing. These systems are provided with redundant backup emergency AC power and are designed to operate after a loss of offsite power. Nonsafety systems are not designed to standards as stringent as those for safety systems but still may be undamaged and operable during emergency conditions. These systems and components are usually isolated during an accident and are not normally provided with backup electric power.

Two potential sabotage scenarios are considered for this STAT alternative. Both scenarios assume that a loss-of-offsite-power transient occurs and the main turbine trips on loss of load. This effectively eliminates that the sources of non-Class 1E power to plant systems. In the first sabotage scenario, it is assumed that successful sabotage of the safety-related systems required for safe shutdown has occurred. In addition, electric power to the nonsafety systems that could bring the plant to a safe shutdown is unavailable. In the second scenario, it is assumed that all emergency diesel generators have been sabotaged, preventing the operation of most safety-related systems. The nonsafety systems have not been sabotaged but are unavailable because of the loss of non-Class 1E power. In either scenario, if electric power could be restored to safety- or nonsafety-related systems, they could bring the plant to a safe shutdown condition. It should be noted that the plants are also provided with limited battery capacity that can be used to operate at least one train of the auxiliary feedwater system and the RCIC and HPCI systems independently of AC power for at least 2 hours. This STAT alternative proposes to provide an additional source of electric power using a combustion turbine generator.

ASSUMPTIONS

It is assumed here that a gas turbine generator will be provided as a backup source of AC power. The generator is assumed to be connected to the non-Class 1E power system via the existing distribution system. If the diesel generators are also unavailable, the gas turbine generator could be used to supply the Class 1E electric system from the startup bus using the existing distribution system. It is further assumed that if electric power can be restored, the plant can be brought to safe shutdown.

AFFECTED PARAMETERS

For BWRs, the approach to calculating the change in core melt frequency was to increase the availability of the diesel generators to account for the additional AC power source provided by the gas turbine generator. The factor used to determine

the increased reliability was established by first calculating the base-case unavailability of all three emergency power system trains (EPS-1, EPS-2, and EPS-3), given that they are called on to activate. The simultaneous unavailability of all three trains can be approximated by multiplying the independent unavailabilities of each train. The following values are from Appendix B of the Grand Gulf PRA:

EPS-1 = 6.7E-02 EPS-2 = 6.7E-02 EPS-3 = 5.5E-02

The resulting value for the simultaneous unavailability of all three EPS trains is then 2.5E-04.

The results of the Grand Gulf PRA indicate that failure of Diesel Generator 1 contributes over 50 percent of the event EPS-1 unavailability. Thus, (EPS-1) = 2DIESEL1. If it is assumed that the same is true for events EPS-2 and EPS-3, then (EPS-2) = 2DIESEL2 and (EPS-3) = 2DIESEL3. As a result, another form for the Boolean equation describing the failure of the emergency power system (assuming independent trains) is:

Unavailability of backup AC power (base case) = 2DIESEL1 * 2DIESEL2 * 2DIESEL3

= $8(DIESEL1)^3$

= 3.7E-04

The adjusted-case Boolean equation would include an additional term for the unavailability of the combustion turbine generator. This equation would take the form:

Unavailability of backup AC power (adjusted case) = (EPS-1) * (EPS-2) * (EPS-3) * (CTG)

where CTG is the unavailability of the combustion turbine generator system. The unavailability of the CTG itself is assumed here to be equivalent to the unavailability of a diesel generator (CTG unavailability = DIESEL1 = 0.036/demand). Again, assuming that 50 percent of the unavailability of the EPS trains is due to faults in the diesel generators, the Boolean equation can be rewritten:

Unavailability of backup power (adjusted case) = (2DIESEL1) * (2DIESEL2) * (2DIESEL3) * (2DIESEL1)

= $16DIESEL1^4$

= 2.7E-05

The adjusted-case unavailability of backup AC power is approximately 93 percent lower than the base case. This increase in reliability as a result of providing a CTG is assumed to be analogous to increasing by 60 percent the reliability of the three existing diesel generators. The adjusted-case values for these cut-set elements become:

DIESEL1 = DIESEL2 = DIESEL3 = 0.0025

The adjusted-case values were input to the Grand Gulf computer code with the following result:

Change in core melt frequency = 6.8E-06/ry.

A similar approach was used to evaluate the reduction in core melt frequency for implementing this STAT alternative at PWRs. First, the ANO-1 PRA was reviewed to identify elements of dominant cut sets that involve failure of the emergency AC power system. The unavailability values for these parameters were then reduced by 93 percent to determine the adjusted-case values. The cut-set elements and their base-case and adjusted-case values are shown below.

Parameter	Base-Case Value	Adjusted-Case Value
LF-AC-DG1	3.3E-02	2.3E-02
LF-AC-DG2	3.3E-02	2.3E-02

These values were input to the ANO-1 computer code with the following result:

Change in core melt frequency = 7.8E-07/ry.

STAT ALTERNATIVE 25:

PROVIDE THE CAPABILITY TO PLACE AN EMERGENCY DIESEL GENERATOR IN SERVICE WITHOUT DC POWER

In this sabotage scenario, it is assumed that a loss-of-offsite-power transient occurs coincidentally with successful sabotage of the DC power supply for one or more emergency diesel generators. This would create a station blackout condition. Under these conditions and if all feedwater were lost, a PWR core would be uncovered to its midplane in about 2 hours. Additional time would be gained if the turbine-driven auxiliary feedwater (AFW) system (typically designed to be operable on DC power alone) was operable and decay heat could be removed via the steam generators. In a BWR, these conditions could lead to the core being uncovered to its midplane in about 1.4 hours. Adequate core coolant inventory could be maintained by the reactor core isolation cooling (RCIC) or high pressure coolant injection (HPCI) systems, which are typically designed to be operable on DC power alone. For both types of plants, AC power would eventually be needed for the operation of long-term decay heat removal systems (e.g., RHR or suppression pool cooling in a BWR, and a charging pump for reactor coolant makeup in a PWR).

This proposed STAT alternative provides a local/manual capability to start up and operate one or more diesel generators without DC power. This would involve a number of design changes to the diesel generators, including the following:

- Provide a system to mechanically drive the diesel generator cooling water system without dependence on any equipment outside the diesel generator building. One example is a system of V-belts and pulleys connected to the diesel engine output shaft. The V-belts and pulleys would be connected to an overhead rotating shaft that turns another set of V-belts and pulleys that are connected to diesel cooling water system fans. This would reduce the dependency of diesel generator cooling on the service water system.

- Provide a manual handwheel or lever on the air-start solenoid valves to permit local/manual startup of the diesel engine.

- Develop a means to ensure that sufficient residual magnetism is present in the generator to "flash" the generator field to begin generating voltage. This could be done by decreasing the diesel generator test interval from 30 days to 15 days.

Plant operators would also need to receive additional training on the procedures for local/manual startup, operation, and control of the diesel generators.

ASSUMPTIONS

It is assumed here that this STAT alternative increases the availability of the emergency diesel generators. It is further assumed that the existence of sufficient residual magnetism in the generator can be ensured by decreasing the diesel generator test interval to 15 days. It is also assumed that the diesel engine cooling system can be operated without the service water system in a manner

similar to that described above. It is assumed that all operations regarding the startup and control of the diesel generators can be performed within the diesel generator building.

AFFECTED PARAMETERS

The approach to evaluating the reduction in core melt frequency for this STAT alternative was to identify potentially affected parameters of the dominant cut sets, adjust the base-case values for the affected parameters, and input the adjusted-case values into the computer codes. It is assumed that the alternative will increase the reliability of the diesel generators to start, or alternatively, will reduce the probability that the diesel generators fail to start. As a result, the parameters affected by this STAT alternative are failures of the diesel generators themselves. These parameters are:

PWR	BWR
LF-AC-DG1	DIESEL1
LF-AC-DG2	DIESEL2
	DIESEL3

The ANO-1 PRA contains an expansion of events LF-AC-DG1 and LF-AC-DG2. It is assumed that this STAT alternative increases the probability that the diesel generators will start by 50 percent (or alternatively, reduces the unavailability due to failure to start by 50 percent). The proposed "fix" also increases the unavailability due to maintenance and repair and due to test. Since it is assumed that the test interval is doubled, it is also assumed that these unavailabilities will double. The expansion of event LF-AC-DG1 into its component failures and the base-case and adjusted-case values for this parameter are shown in Table A.4. As shown, the adjusted-case value for LF-AC-DG1 (and for LF-AC-DG2) is 0.0237/demand.

The Grand Gulf PRA also contains an expansion of events DIESEL1, DIESEL2, and DIESEL3. It is assumed that similar changes can be made to these parameters as were made to the ANO-1 (PWR) parameters; i.e., a 50 percent increase in reliability of the diesel generators to start and a 100 percent increase in unavailability due to test and maintenance. The expansion of this event is shown below.

DIESEL1 = DIESEL2 = DIESEL3	Base-Case	Adjusted-Case
Failure to Start	0.030	0.015
Maintenance	0.0064	0.0128
	0.036	0.028

The adjusted-case values for the affected parameters were then input to the ANO-1 and Grand Gulf computer codes to calculate the reduction in core melt frequency. The reduction in core melt frequencies of ANO-1 and Grand Gulf PRA are estimated to be 4.0E-07/ry and 2.0E-06/ry, respectively.

The CMF values are believed to represent the upper bound of benefit that would be obtainable due to implementation of this STAT alternative. This is because to be effective, the STAT alternative would require loss of offsite power (LOOP), loss of DC power supply, loss of DG, loss of steam-driven AFW pumps, loss of ultimate heat sink and other safety systems (depending upon the plant design). The frequency of the first two terms, LOOP and loss of DC power supply, is approximately 2E-05/ry. Combining this with the probability of the remaining terms would lower this contributor by 2 to 3 orders of magnitude. Also, the ability to start the diesels without DC power would lower the value by another 1 to 2 orders of magnitude. Thus, the difference in the CMF before and after is intuitively on the order of 1E-07/ry to 1E-08/ry. It was decided to use the upper-bound estimates for the evaluation of this STAT alternative to be consistent with the approach taken on others.

TABLE A.4. Expansion of Event LF-AC-DG1 (composite failures)

LF-AC-DG1: Local fault of diesel generator 1 [fails HPIS (P36) A and B pumps, RBCS (SF1) A and B cooler fans, RBSI A pump (P35A), and EFS electric pump (P7B)].

Component Type	Subevent Description	Subevent Unavailability	
		Base Case	Adjusted Case
Diesel generator (DG1)	Failure to start	2.5E-02	1.3E-02
	Failure to run, given start	7.8E-04	7.8E-04
	1 of 5 shorts to power in time delay relays	5E-05	5E-05
	Maintenance, repair of DG1	1.5E-03	3.0E-03
	Unavailability of DG1 due to test	1.2E-04	1E-03
Output circuit breaker for DG1 (308)	Failure to mechanically transfer	1E-03	1E-03
	Circuit breaker control circuit:		
	(a) Failure of 1 of 5 contacts	5.4E-04	5.4E-04
	(b) Failure of 2 relays to energize	2E-04	2E-04
	Maintenance, repair of CB308	4E-06	4E-06
Tie breaker from A1 to A3 (309)	Failure to mechanically open	1E-03	1E-03

TABLE A.4. (Contd)

Component Type	Subevent Description	Subevent Unavailability Base Case	Subevent Unavailability Adjusted Case
(A) 1 of 3 circuit breaker UV control circuits (309-A31)	(a) Failure of 1 of 2 relays to energize	2E-04	2E-04
	(b) Failure of 1 of		
[ANDed with (B) and (C) below]	(c) Open circuit in cable	1.1E-03	1.1E-03
(B) 1 of 3 circuit breaker UV control circuits (309-A32)	(a) 1 of 2 relays not energized	2E-04	2E-04
	(b) Failure of 1 of 2 contacts	2.2E-04	2.2E-04
[ANDed with (A) above and (C) below]	(c) Open circuit in cable	1.1E-03	1.1E-03
(C) 1 of 3 circuit breaker UV control circuit (309-B5)	(a) 1 of 2 relays not energized	2E-04	2E-04
	(b) Failure of 1 of 4 contacts	4.3E-04	4.3E-04
[ANDed with (A) and (B) above]	(c) Open circuit in cable	1.1E-03	1.1E-03
Circuit breaker (D114)	Overload surge protection malfunction	2.4E-05	2.4E-05
Cable (D114)	Open circuit	7.2E-05	7.2E-05
Bus (D114)	Open circuit	7.2E-05	7.2E-05
Motor-driven fuel pump for DG1 (P16A)	Failure to start	1E-03	1E-03
	Failure to run, given start	7.2E-04	7.2E-04
	Circuit breaker overload surge protection malfunction (5114)	2.4E-05	2.4E-05
	Open circuit in cable	7.2E-05	7.2E-05
		0.033	0.022

ASSUMPTIONS FOR CALCULATION OF SABOTAGE AND TAMPERING CMF REDUCTIONS

This section describes the assumptions used in calculating the CMF reductions for the 25 STAT alternatives. Chapter 3 describes the use of these assumptions and results.

STAT Alternative 1: Three 100 Percent Trains

Three 100 percent independent safety trains are proposed for the mitigation and prevention of tampering and sabotage acts. The present arrangement in plants is to have two independent safety trains, from sensors; through logic circuitry; through engineered safeguards actuation; to the paths for safety injection, containment isolation/spray, and emergency power generation.

Tampering

Review of historical data related to tampering acts in DOE facilities and commercial nuclear power plants indicates that previous acts of tampering have occurred in no more than two plant locations. Addition of a third 100 percent independent safety train should eliminate the opportunity for this type of tampering. Given the number of systems involved, this STAT alternative was rated high for opportunity reduction. The systems would also have greater availability given an attack. This was judged as a significant contribution for this parameter. Finally, due to the reduced chance of tampering leading to system failures, the STAT alternative was judged to affect the motivation for committing tampering acts. Given the many alternative targets, however, the effect on this parameter was believed to be moderate.

Quantification of these assumptions is described in Chapter 3. This issue was assumed to have the maximum potential tampering CMF reduction of 50 percent. To quantify the effectiveness of adding a third totally independent safety train in terms of reduction in core melt frequency, the ANO-1 and Grand Gulf vital area study (see Appendix B) and PRA were used. The reductions in core melt frequency for ANO-1 and Grand Gulf are estimated to be 2E-05/ry and 2E-06/ry, respectively.

Sabotage With Tampering

The addition of a third 100 percent safety train is believed to impact tampering-induced equipment failure combinations that lead to core melt. The third safety train will not, however, reduce the vulnerability of the plant to initiation of accidents.

This STAT alternative, based on results of the vital area studies, would have no impact on single-location cut sets. It does, however, have high potential to reduce the number of two-location cut sets. Systems that are targets for tampering would have greater reliability. The alternative also would increase the reliability of systems other than the target system. Using the approach described above, STAT Alternative 1 was assigned an effectiveness of 10 percent. Applying the results of Appendix B analyses and the Grand Gulf and ANO-1 PRA yields a reduction in core melt frequency of about 2E-05/ry for Grand Gulf and ANO-1.

STAT Alternative 2: Two Additional Bunkered AFW Pumps--For PWRs
Two Additional RCIC Pumps--For BWRs

This alternative would add two additional bunkered AFW and RCIC pumps. In present designs, there are typically three auxiliary feed pumps: two that are electric motor driven and one that is steam driven. The plumbing is assumed to be cross-connected in such a way that any one motor-driven pump can fail and the other pump can carry the load.

Tampering

It was assumed that plant vulnerability to tampering is not drastically affected by adding additional reactor core isolation coooling (RCIC) or auxiliary feedwater (AFW) pumps, given the existing three trains. This alternative was rated as having a modest impact on reducing tampering opportunity due to decreased reliance on the control room. The systems that are affected by STAT Alternative 2 are already quite diverse. Thus, these systems would be only minimally affected by additional trains. However, the independence of the bunkered concept was felt to moderately improve diversity. No impact on tampering motivation was perceived due to the single system orientation of the modifications. These assumptions resulted in an estimate of a 5 percent reduction in tampering CMF. Based upon analyses of Grand Gulf and ANO-1 PRAs, this translates to a reduction in core melt frequency of 2E-6/ry for PWRs and 7E-7/ry for BWRs.

Sabotage With Tampering

Addition of two independent and bunkered AFW pumps and RCIC pumps significantly reduces the threat of disabling an AFW system and an RCIC system from a single location. Given the number of accidents where these systems play a role, there would also be a significant reduction in the number of two-location sabotage targets and significant improvement in the AFW and RCIC system reliability as backups to other tampering targets. No reduction in the frequency of sabotage attempts was anticipated. Based on this rationale, it is believed that the sabotage threat could be reduced by up to 50 percent. From the ANO-1 and Grand Gulf PRAs, this translates to a reduction in core melt frequency of 1E-04/ry.

STAT Alternative 3: A Passive Steam Condenser for PWRs

This issue was defined to affect only releases of material. No effects were considered for the reduction of CMF due to sabotage or tampering.

STAT Alternative 4: SNUPPS Design with Complete Separation

This alternative was not treated due to the lack of an applicable PRA. Sabotage vulnerabilities may not be appreciably different from other PWRs. Tampering vulnerability is unknown.

STAT Alternative 5: Implementation of the Two Man Rule

Implementing the two man rule in the vital areas is proposed to reduce tampering and sabotage with tampering CMF.

Tampering

The two man rule has been implemented in military installations for many years. However, data on the effectiveness of this measure is not available. Simple binomial distribution of the available data on the number of postulated "pairs" per year in the plant and the overall frequency of tampering can be used to calculate reductions in the tampering frequency of about 70 percent. This calculation, however, assumes that 125 random "pairings" are made every day. However, these pairs are not together in all parts of the plant.

Assuming that the two man rule will only be implemented in the important areas, it is reasonable to postulate that the protected areas will become a more attractive target for the individuals with tampering intent. The analysis of the vital area study also revealed that a system can be disabled from many locations, and some of these locations are in the protected areas. Therefore, protection of part of the system in important areas will not stop a determined individual from tampering with the exposed system in the protected area.

Due to the increased chance of discovery by the second worker, the STAT alternative was judged to moderately reduce the motivation for committing tampering acts.

Quantification of these assumptions resulted in assigning STAT Alternative 5 a potential tampering reduction effectiveness of 10 percent. To quantify the effectiveness of implementing the two man rule in terms of reduction in core melt frequency, the ANO-1 and Grand Gulf vital area studies and PRAs were used. The reductions in core melt frequency for ANO-1 and Grand Gulf are estimated to be 3E-06/ry and 3E-07/ry, respectively.

Sabotage With Tampering

Similar to the previous STAT analysis, implementing the two man rule is believed not to have a direct impact in preventing or mitigating sabotage attempts. The control room is likely to be unaffected since some aspects of the two man rule are in effect under other rules. However, since sabotage with tampering requires initiation of an accident accompanied with loss of mitigation (safety) systems, it is perceived the two man rule could play a role in reducing the number and severity of tampered systems in locations far from the control room. This was interpreted as reducing the number of two-location cut sets.

This STAT alternative would have little impact on increasing the reliability of the backup systems. A reduction in the frequency of sabotage attempts is anticipated. Based on this rationale, it is believed that the sabotage threat is reduced by about 5 percent. From the ANO-1 and Grand Gulf PRAs, this translates to a reduction in core melt frequency of about 1E-05/ry.

STAT Alternative 6: Installation of TV Cameras in Vital Areas

TV cameras are proposed in vital areas for the purpose of reducing and preventing tampering and sabotage acts.

Tampering

Similar to the arguments presented in the analysis of the two man rule (STAT Alternative 5) and based on the review of data available on effectiveness of TV cameras in industrial installations against shoplifting/theft and other types of crimes, it is believed that a modest improvement in reduction of tampering acts is possible. However, since it is proposed that the TV cameras will only be installed in vital areas, it is reasonable to postulate that the protected areas will become a more attractive target for individuals with tampering intent. Tampering threat analysis of the Grand Gulf and ANO-1 PRAs reveal that the loss of systems in protected areas presents an equal or higher contribution to CMF than loss of systems in important areas. Based on this rationale, it is believed that this STAT alternative does not reduce the opportunity significantly.

No improvement in the availability of the mitigation systems is foreseen due to implementation of this STAT alternative. A modest improvement in the reduction of motivation is, however, possible. This was attributed to fear of discovery.

Based on above rationale, it is believed that this STAT alternative would be less effective than STAT Alternative 5. A reduction in tampering threat frequency of about 5 percent is assumed due to installation of TV cameras. Applying this to the ANO-1 and Grand Gulf vital area studies and PRAs yield a core melt frequency reduction of about 2E-06/ry for ANO-1 and 2E-07/ry for Grand Gulf.

Sabotage With Tampering

This STAT alternative is believed not to have any impact on reducing the number of single- and two-location cut sets due to the resolution available for monitoring staff with legitimate access. No increase in the availability of the backup systems is possible due to implementation of this alternative. It is, however, believed that installation of TV cameras has a modest impact on reduction of sabotage attempts. This is due to the greater chance of detection from TV surveillance. A reduction in sabotage threat of about 1 percent was assigned to this STAT alternative. Applying this assumption to the ANO-1 and Grand Gulf PRAs yields a core melt frequency reduction of about 2E-06/ry.

STAT Alternative 7: Manual/Local Operation of BWR Safety Relief Valves

Manual/local operation of BWR safety relief valves is proposed for the purpose of reducing and preventing tampering and sabotage acts. All LWRs are provided with some means of relieving the reactor coolant system pressure to avoid overpressurizing the system. This capability is provided by pressure relief valves located in the main steam lines. These valves can be operated automatically or manually from the control room. The proposed design alternative provides for local operation of the relief valves, in case the control room has been sabotaged.

Tampering

The local operation of the relief valves could be beneficial if the operation of these valves is made impossible from the control room. However, local operation of the relief valves in a place other than the "super- protected" control room could make the second location an attractive target. Opening the valves inadvertently could lead to LOCA initiation.

A moderate improvement in the availability of the mitigating systems is believed to be possible due to STAT Alternative 7. No improvement on reducing the tampering opportunity or motivation is foreseen due to implementation of this alternative. Based on this rationale, a reduction in tampering threat of about 5 percent was assigned to STAT Alternative 7. Applying this assumption to the Grand Gulf vital area study and PRA yields a reduction in core melt frequency of about 2E-07/ry.

Sabotage With Tampering

Providing manual/local operation of relief valves results in an additional location where sabotage from the control room could be mitigated. Therefore, this STAT alternative reduces the single-location cut set and increases the two-location cut sets.

No increase in the availability of the backup systems is assumed to be possible due to this STAT alternative. A moderate increase in system availability is, however, postulated since this alternative allows for local/manual operation of the relief valves. Based on this rationale, a reduction in sabotage threat of 5 percent was postulated. Applying this to the Grand Gulf PRA yields a core melt frequency reduction of about 1E-05/ry.

STAT Alternative 8: Feed-and-Bleed Operation of Suppression Pool

Feed-and-bleed operation of supression pool could be provided for the purpose of reducing, mitigating, and/or preventing tampering and sabotage acts. STAT Alternative 8 would supply cooling to the suppression pool using a feed-and-bleed technique in the event that suppression pool cooling systems are disabled.

Tampering

This STAT alternative calls for several alternative means of providing coolant makeup source for feed-and-bleed operation of the suppression pool in case the residual heat removal (RHR) cooling mode is disabled. These alternative sources include suppression pool makeup using 1) the high pressure coolant injection (HPCI) or high pressure core spray (HPCS) system, 2) the refueling water transfer system, and 3) the service water system (SWS) cross-connect to the RHR system.

Review of generic accident progression event trees indicates that the sources mentioned above are relied upon to mitigate series of accidents and transients to avoid core melt or core damage. Therefore, it is believed that if a source such as the HPCI is used to replace the function of the RHR cooling mode of the suppression pool, it will jeopardize the availability of the HPCI when it is called upon to perform its function toward the advanced stages of the accident.

No improvement on reduction of tampering opportunity or motivation is foreseen due to implementation of this STAT alternative.

A modest increase in the availability of the system is assumed due to alternative means of cooling. Based on this rationale, it is believed that this STAT alternative does not reduce the tampering threat significantly. A reduction in tampering threat of about 1 percent is postulated. Applying this assumption to the Grand Gulf vital area study and PRA yields a reduction in core melt frequency of about 3E-07/ry.

Sabotage With Tampering

This STAT alternative is believed to address one of the most important issues related to plant safety. The reason is that many vital mitigating systems such as the decay heat removal system, the core spray injection system, and the reactor core isolation cooling system are affected by the suppression pool. It is believed that this alternative has a significant impact on the availability of the backup mitigating systems. A moderate improvement in systems availability is believed to be possible due to implementation of this alternative.

No impact on single- or two-location cut sets is foreseen due to implementation of this alternative. Based on this rationale, it is believed that this STAT alternative would not reduce the sabotage threat greatly. Therefore, a reduction in sabotage CMF of about 1 percent was postulated. Applying the above assumption to the Grand Gulf PRA yields a core melt frequency reduction of about 2E-06/ry.

STAT Alternative 9: Use of Safety Injection Pumps to Supply Water to Steam Generators

Safety injection pumps are proposed to supply water to steam generators for reduction, mitigation, and/or prevention of tampering and sabotage acts. This alternative would supply water to the steam generators using the safety injection pumps in the event that the auxiliary feedwater system is disabled.

Tampering

Implementation of STAT Alternative 9 was assumed to have a significant impact on the availability of the backup mitigating systems due to improvements in emergency feedwater capabilities. No reduction in tampering opportunity or motivation is foreseen due to implementation of this alternative. Based on this rationale, it is believed that this alternative would not reduce the tampering threat more than 1 percent. Applying this assumption to the ANO-1 vital area study and PRA yields a reduction in core melt frequency of about 3E-08/ry.

Sabotage With Tampering

Two-location cut set analysis of the ANO-1 indicates that acts are possible that initiate an accident and failure of both the AFW system and the high pressure injection pumps. Therefore, it is believed that the availability of

the system and the backup systems is not significantly affected by this alternative. No reduction of the single- or two-location cut sets would be achieved under this alternative. Based on this rationale, it is believed that this alternative does not reduce the sabotage threat. Therefore, the reduction in core melt frequency is zero.

STAT Alternative 10: Provide Spring Loaded Safety Valves for Venting SGs

This STAT alternative was determined to have no impact on reducing the sabotage and tampering threats because of the number of actions needed to require the use of these valves. Therefore, no core melt frequency reduction was postulated due to implementation of this alternative.

STAT Alternative 11: Use of Fire Water as Source of Cooling RHR Heat Exchangers

Due to similarities in function between this alternative and STAT Alternative 16, only Alternative 16 was analyzed.

STAT Alternative 12: Connect SI Pumps in Series to Raise Discharge Pressure

Due to similarities in function between this alternative and STAT Alternative 9, only Alternative 9 was analyzed.

STAT Alternative 13: Use Control Rod Drive Hydraulic System to Supply Reactor Coolant Makeup in a BWR

The control rod drive hydraulic system (CRDHS) supplies reactor coolant makeup in the event that high pressure injection systems are disabled. This alternative is applicable to BWRs. The CRDHS supplies pressurized water to operate and cool the control rod drive mechanisms. The water used for these functions is ultimately discharged into the reactor vessel and provides a backup source of water in an emergency.

Tampering

The purpose of this STAT alternative is to provide post-accident reactor coolant makeup using the CRDHS in the event that other high pressure injection systems are inoperable.

The BWR high pressure injection systems include the reactor core isolation cooling (RCIC) system, the high pressure core spray (HPCS) system, the high pressure coolant injection (HPCI) system, or the feedwater coolant injection (FWCI) system. The availability of any of these systems would negate the need for considering this STAT alternative.

Review of the Grand Gulf vital area study shows that to disable all high pressure injection systems, it is necessary to cause damage in more than two rooms. As before, based on historical data, all of the previous tampering acts have occurred in more than two rooms.

However, under the existing design, it requires a three-location cut set to disable all mitigation systems. This suggests that based on historical data, addition of one more backup system is not necessary. Therefore, the availability of the mitigating systems would not be affected by this alternative.

Furthermore, no reduction in tampering opportunity or motivation is postulated due to STAT Alternative 13. Based on this rationale, it is believed that this alternative does not have any effect on the reduction of tampering threat. Therefore, the reduction in core melt frequency is zero.

Sabotage With Tampering

A successful sabotage scenario would require loss of all high pressure injection systems. This is because if any of the high pressure injection systems function, the need for this alternative is negated and the plant has the capability to mitigate the accident.

This alternative does not reduce the number of single-location cut sets. It does, however, reduce the number of two-location cut sets through the creation of four-location cut sets. The availability of the backup systems is also increased in case of a sabotage event. A moderate improvement in system availability is also postulated due to implementation of this alternative.

Based on above rationale, it is believed that this alternative has a moderate impact on the reduction of sabotage threat. A reduction in sabotage threat of about 5 percent was postulated. Applying this assumption to the Grand Gulf PRA yields a reduction in core melt frequency of about 1E-05/ry.

STAT Alternative 14: Use Main Condenser Pumps to Provide Reactor Coolant Makeup

Main condensate pumps are proposed to supply water in the event that the normal reactor coolant makeup systems are disabled. This STAT alternative is applicable to BWRs.

Tampering

Loss of all reactor coolant makeup sources would require the loss of main feedwater pumps, loss of all high pressure injection systems, loss of the CRDHS, and loss of all low pressure injection systems. Therefore, this STAT alternative does significantly improve the availability of the mitigating systems.

Furthermore, no reduction in tampering threat or opportunity is foreseen due to implementation of this STAT alternative. Based on this rationale, it is believed that no reduction in tampering threat is achieved by implementing this alternative. Therefore, the reduction in core melt frequency is zero.

Sabotage With Tampering

A successful sabotage scenario would require loss of all high pressure and low pressure coolant makeup sources.

As mentioned above, to lose all reactor coolant makeup would require loss of main feedwater pumps, loss of high pressure coolant injection systems (e.g., RCIC, HPCS, HPCI, FWCI), loss of the CRDHS, and loss of the low pressure coolant injection systems (LPCS, LPCI, and LPCI of the RHR system). This assumes adequate capability and redundancy to provide coolant makeup in the event that normal feedwater is lost. Therefore, implementation of this alternative would have little additional improvement in two-location cut sets. No improvement would be achieved for single-location cut sets since all of these systems can still be disabled from the control room.

Implementation of STAT Alternative 14 would improve the availability of the backup systems to some degree. It was also believed that this alternative does not reduce the sabotage threat significantly. Therefore, a reduction in sabotage threat of about 1 percent is postulated. Applying above assumption to the Grand Gulf PRA yields a reduction in core melt frequency of about 2E-06/ry.

STAT Alternative 15: Cross-Connect Service Water With Essential Service Water (ESW)

Cross-connections between the service water and the essential service water system are proposed for STAT Alternative 15. This alternative is applicable to both BWRs and PWRs. Its purpose is to provide cross-connection in BWR and PWR plants for heat removal from the safety-related components and systems in the event that the ESW pumps are disabled.

Tampering

The PWR ESW system is used to transfer heat from component cooling water to the ultimate heat sink during normal operations and emergencies. The system typically consists of two independent trains. The systems serviced by ESW system include diesel generators (DGs), HPSI, LPSI, the component cooling system (CCS), and a variety of other safety- and nonsafety-related systems.

The BWR ESW system is used to transfer heat directly from the components such as DGs, HPCS or HPCI, LPCS, RCIC, and numerous other safety- and nonsafety-related systems. The system typically consists of three independent trains or divisions.

The STAT alternative calls for cross-connecting the plant service water system to the ESW system to restore cooling water flow to components and systems in the event that the ESW pumps are disabled. Therefore, implementation of this alternative could have a moderate impact on the availability of the mitigation systems.

No reduction in tampering opportunity or motivation is foreseen due to implementation of this alternative. Based on the above rationale, it was believed that this alternative would not have a large impact on reduction of tampering threat. Therefore, a reduction in tampering threat threat of about 1 percent is postulated. Applying the above assumptions to the ANO-1 and Grand Gulf vital area studies and PRAs yields a reduction in core melt frequency of about 3E-07/ry for ANO-1 and 3E-08/ry for Grand Gulf.

Sabotage With Tampering

The PWRs and BWRs have at least two independent trains for the ESW system. Therefore, by using the alternative service water systems as another means of cooling the systems and components, it was assumed that there would be a reduction in the number of two-location cut sets.

There may be a moderate increase in the availability of the backup systems due to the support role of the ESW. Single-location cut sets are not affected by this alternative. Based on this rationale, it was believed that this alternative would have a moderate impact on the reduction of sabotage threat.
A reduction of 1 percent was postulated. Applying this assumption to the ANO-1 and Grand Gulf PRAs yields in a reduction in core melt frequency of about 2E-06/ry.

STAT Alternative 16: Cross-Connect Fire Water System and ESW

Cross-connections between the fire water system and the essential service water system are proposed by this alternative. This alternative is applicable to both BWRs and PWRs. Its purpose is to provide cross-connection between the fire water system and the ESW system in BWR and PWR plants to provide for heat removal from the safety-related components and systems in the event that the ESW pumps are disabled.

Tampering

The PWR ESW system is used to transfer heat from a component cooling water to the ultimate heat sink during normal operations and emergencies. The system typically consists of two independent trains. The systems serviced by ESW system include DGs, HPSI, LPSI, CCS, and a variety of other safety- and nonsafety-related systems.

The BWR ESW system is used to transfer heat directly from the components such as DGs, HPCS or HPCI, LPCS, RCIC, and numerous other safety- and nonsafety-related systems. The system typically consists of three independent trains or divisions.

This STAT alternative calls for cross-connection of the ESW system and the fire water system to cool the systems and components. One problem with this alternative is the capacity of the fire water system. The fire water system runout flow rate is approximately 50 percent of the flow rate of a single ESW pump. In case of tampering with the power system, only the diesel-engine- driven fire water pump will be available. This diesel-engine-driven pump can provide approximately 15 to 25 percent of the flow rate of a single ESW pump. This low flow rate in the ESW system would not be adequate to support the operation of a single ESW loop. Therefore, there is no significant increase in the availability of the mitigating systems.

One other problem related to the cross-connection of the fire water system and the ESW system is the plant's vulnerability to an actual fire. Since the fire water system is tied up performing other functions, it cannot perform its fire fighting function. This alone could be a temptation to start a fire. Therefore, the tampering motivation may actually be increased.

No reduction in tampering opportunity is foreseen due to implementation of this STAT alternative. Based on this rationale, it is believed that this alternative does not reduce the tampering threat greatly. A 1 percent reduction in tampering threat was postulated. Applying the above assumptions to the ANO-1 and Grand Gulf vital area studies and PRAs yields a reduction in core melt frequency of about 3E-07/ry for ANO-1 and 3E-08/ry for Grand Gulf.

Sabotage With Tampering

As mentioned above, the PWRs and BWRs have at least two independent trains of the ESW system. Therefore, using the fire water system as another means of cooling the systems and components reduces the number of two-location cut sets. This STAT alternative does not have any impact on the single-location cut sets and it is also believed that it does not have a significant impact on improving the availability of the backup systems. This is due to many reasons. The most important is the low flow rate provided by the fire water system. Also, a fire can be initiated when the fire water system is not available. Only limited time is available to restore ESW flow if that system provides direct diesel generator cooling. The diesel generator cooling should be established 5 minutes following startup.

Based on the above discussion and without substantial upgrade of the fire water system, it is unlikely that the fire water system could serve as an effective replacement for the ESW pumps. Therefore, it is believed that no reduction in sabotage threat is achieved due to this STAT alternative, and the core melt frequency reduction is zero.

STAT Alternative 17: Use ESW to Directly Cool Components Cooled by CCW

Due to functional similarities between this alternative and STAT Alternative 15, only Alternative 15 was analyzed.

STAT Alternatives 18 And 19: Local Readouts for Pressurizer, SG Level Indication, and SG Pressure

Local readouts for pressurizer, steam generator level indication, and pressure are proposed for the reduction, mitigation, and/or prevention of tampering and sabotage acts. These alternatives are combined in this analysis due to their similarities in function. Steam generator and pressurizer level indications provide information via sensors and transmitter units to safety- and nonsafety-related instrumentation and control systems, and serve as information sources for control room and remote operations. The purpose of these alternatives is to provide local steam generator and pressurizer water and pressure (for steam generators) level indication in the event that the normal level indication has been disabled.

Tampering

PWR plants might have two, three, or four steam generators, but only one pressurizer. Steam generator and pressurizer level indications are derived from differential pressure sensor/transmitter units located inside containment. Signal cables are then connected to a variety of safety- and nonsafety-related instrumentation and control systems.

There are typically three to six independent safety-related channels monitoring steam generator water level. Based on NUREG/CR-2585 (U.S. NRC 1982a), rapidly disabling all steam generator and pressurizer level indications would not be accomplished by tampering the sensor/transmitter units inside containment. The specific tampering attempt may entail disabling the station batteries (Class 1E and non-Class 1E), major instrument cable runs, or instrument cabinets. Such actions will likely affect more systems than just level instrumentation.

Sabotage With Tampering

Providing local readouts for the steam generator and pressurizer level indications is believed to improve manual recovery outside the control room. Thus, providing for local steam generator and pressurizer readouts reduces the single-location cut sets (control room). It does not, however, have any impact on the two-location cut sets. It is believed that the availability of backup systems is improved due to availability of data, so the recovery chances are higher.

Based on this rationale, it is believed that the sabotage threat is minimally affected by these STAT alternatives. A 1 percent reduction in sabotage threat was postulated. Applying this assumption to the ANO-1 PRA yields a reduction in core melt frequency of about 2E-06/ry.

STAT Alternative 20: Provide Emergency AC Power to Nonsafety-Related Equipment

Due to the similarities between this alternative and STAT Alternative 21, only Alternative 21 was analyzed.

STAT Alternative 21: Provide Cross-Connection between Class 1E/Non-Class 1E

Cross-connections between the Class 1E and non-Class 1E DC power systems are proposed. The purpose of this STAT alternative is to permit the non-Class 1E batteries to supply power to safety-related systems when one or more Class 1E batteries are disabled.

Tampering

The main purpose of the non-Class 1E DC batteries would be to restore DC power to the Class 1E load group to start the diesel generators. Review of the vital area studies indicate that the batteries are located in more than two locations. For example, in the Grand Gulf plant there are three distinct battery rooms. Therefore, based on historical data, it is believed that the batteries will survive a tampering attempt.

Two-location cut set analysis of the ANO-1 and Grand Gulf vital area studies also shows that the diesel generators can be disabled via two locations. Due to this vulnerability, it is believed that cross-connecting the non-Class 1E batteries with Class-1E batteries to start the diesel generators will not have a significant impact on increasing the diesel generator's availability, since the diesel generators can be still disabled via two locations.

No reduction in tampering opportunity or motivation is foreseen due to implementation of this alternative. It is believed that STAT Alternative 21 would not have any effect on tampering. Therefore, the reduction in core melt frequency was assumed to be zero.

Sabotage With Tampering

As mentioned before, two-location cut set analysis of the ANO-1 and Grand Gulf vital area studies has shown that the diesel generators can be disabled via two locations. Therefore, even providing another means of starting a diesel generator following loss of its normal DC supply would not be effective if the diesel generators have been attacked directly.

Therefore, no improvement in the availability of the backup systems is foreseen. By providing for alternative means of starting the diesel generators, there is a reduction in the number of two-location cut sets. No effect in the single-location cut sets is foreseen. Based on the above rationale, it is believed that this alternative would not have a large impact on sabotage threats. A reduction in sabotage threat of 1 percent was postulated. Applying this assumption to the ANO-1 and Grand Gulf PRAs yields a reduction in core melt frequency of about 2E-06/ry.

STAT Alternative 22: Provide Multiple DC Feeders to DC Powered Components

Due to functional similarities between this alternative and STAT Alternative 25, only Alternative 25 was analyzed.

STAT Alternative 23: Provide an Alternate Water Source to Maintain Coolant Inventory

An alternative water source is proposed to maintain reactor coolant inventory and to remove decay heat during hot shutdown in the event that the usual sources of water have been disabled. This alternative is applicable to PWRs.

Tampering

Decay heat removal in a PWR is accomplished at high pressure by the auxiliary feedwater system and at low pressure by the residual heat removal system. The main objectives of this STAT alternative are similar to those of Alternatives 2 and 9. Alternative 2 calls for addition of two additional bunkered AFW pumps, and Alternative 9 also calls for use of safety injection pumps to supply water to steam generators. As evident, these measures are calling for alternate means of maintaining coolant inventory and providing the long term decay heat removal in the event that usual coolant sources are not available.

Review of the ANO-1 vital area study shows that the AFW system cannot be disabled via two locations. It is believed that providing an alternative means of reactor coolant makeup does not affect the availability of the mitigation systems. No reduction in tampering opportunity or motivation is foreseen due to implementation of this STAT alternative. Thus, it is believed that this STAT alternative would not have any impact on reducing tampering threat. Therefore, the reduction in core melt frequency is zero.

Sabotage With Tampering

Review of the ANO-1 vital area study shows that the diesel generators and Class 1E load group can be disabled via two locations. In this case, the pumps needed to supply the water from an alternative source will not start. Therefore, there is no impact on two-location cut sets.

The ANO-1 study also shows that sabotage of the target identified in Appendix B will disable the pumps needed for the AFW and HPI systems. The interconnecting piping system can also be disabled via damage caused in two locations. Therefore, the impact of this alternative on availability of backup systems is minimal. There is also no impact on the single-location cut sets. Based on this rationale, it is believed that this STAT alternative has no impact on sabotage threat. Therefore, the reduction in core melt frequency is zero.

STAT Alternative 24: Provide a Standby Non-Class 1E Combustion Turbine Generator

A standby non-Class 1E combustion turbine generator is proposed that could supply power to the station startup bus for distribution to designated equipment and systems when offsite power is not available. This alternative is applicable to both PWRs and BWRs.

NUREG/CR-2585 (U.S. NRC 1982a) considers this alternative to be applicable to two types of sabotage scenarios. The first one involves the sabotage of safety-related systems and the unavailability of nonsafety-related systems due to loss of non-Class 1E AC power. The second scenario involves unavailability of all diesel generators and unavailability of nonsafety systems due to loss of non-Class 1E AC power.

Tampering

Addition of a standby combustion turbine generator provides redundancy of the onsite emergency power source. This alternative therefore increases the availability of the mitigation systems and also reduces the opportunity for an effective tampering act. There is no impact on tampering motivation. Based on this rationale it was believed that this alternative has a moderate impact on tampering threat. A reduction in tampering threat of about 5 percent was postulated. Applying the above assumptions to the ANO-1 and Grand Gulf vital area studies and PRAs yields a reduction in core melt frequency of about 2E-07/ry and 2E-07/ry, respectively.

Sabotage With Tampering

Review of the ANO-1 and Grand Gulf vital area studies shows that to disable all existing diesel generators, it is necessary to cause damage in two locations. Therefore, disabling all emergency power falls into the two-location cut set category. Providing a standby combustion generator for emergency power is like adding another location that has to be tampered with to disable emergency power. Adoption of this alternative complicates actions necessary to prevent effective plant response to an accident initiation. Availability of a standby combustion turbine generator would permit the use of some nonsafety-related systems for accident mitigation for approximately 30 minutes following loss of offsite power. This STAT alternative provides a

diverse onsite power source that could restore power to safety-related and nonsafety-related systems following a sabotage scenario involving loss of offsite power and all diesel generators. Therefore, there is a moderate improvement in the availability of backup systems.

There would be no reduction in single-location cut sets. Based on above reasoning, it is believed that this STAT alternatives makes a moderate impact on sabotage threat. A reduction in sabotage threat of 1 percent was postulated. Applying this assumption to the ANO-1 and Grand Gulf PRAs yields a reduction in core melt frequency of about 2E-06/ry.

STAT Alternative 25: Provide Capability to Place an Emergency Diesel Generator in Service Without DC Power

It is proposed to provide the capability to place an emergency diesel generator in operation, supplying its normal Class-1E load group when DC is not available to the diesel generator control or auxiliary system or to the diesel generator auxiliary system.

This alternative calls for a variety of means to place a diesel generator in service without DC power. These means include use of STAT Alternative 21 to establish a DC bus tie to reenergize the affected DC load groups or to re-establish DC power to diesel auxiliaries by switching them to an alternate DC power source (STAT Alternative 22), or to manually start up the diesel generators without AC or DC power.

Tampering

The basic objectives of this STAT alternative and STAT Alternative 21 are the same. Both call for alternative means of starting the diesel generators. However, two-location cut set analysis of the ANO-1 and Grand Gulf vital area studies shows that the diesel generators can be disabled via two locations. Due to this rationale, it is believed that even providing for other means of starting up the diesel generators will not be effective.

Therefore, it is believed that this STAT alternative does not impact the availability of the mitigation systems. Tampering opportunity or motivation is also unaffected. Based on this rationale, it was assumed that this STAT alternative has no impact on tampering threat. Therefore, the reduction in core melt frequency is zero.

Sabotage With Tampering

As mentioned before, two-location cut set analysis of the ANO-1 and Grand Gulf vital area studies has shown that the diesel generators can be disabled via two rooms. Therefore, providing another means of starting a diesel generator following loss of its normal DC supply would not be enough if the diesel generators have been disabled.

Therefore, there is no impact on the two-location cut sets. This STAT alternative also has no impact on the single-location cut sets. Furthermore, it is believed that providing for diesel generator startup without DC power has a minimal impact on the availability of the backup systems. Considering the above rationale, it is believed that STAT Alternative 25 would have no impact on sabotage threat. Therefore, the reduction in core melt frequency was assumed to be zero.

NUREG/CR-4462
PNL-5690
RG, RS, R1

DISTRIBUTION

No. of Copies

OFFSITE

U.S. Nuclear Regulatory Commission
Division of Technical Information
& Document Control
7920 Norfolk Avenue
Bethesda, MD 20014

P. Ting
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

12 Office of Nuclear Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

R. M. Bernero
W. Minners
O. D. Parr
L. S. Rubenstein
A. W. Serkiz
A. Singh (5)
T. P. Speis
J. S. Wermiel

R. H. Gramann
Office of Nuclear Materials
Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

2 Human Affairs Research Centers
4000 N.E. 41st Street
Seattle, WA 98105

T. D. Overcast
W. R. Rankin

No. of Copies

ONSITE

50 Pacific Northwest Laboratory

W. B. Andrews (33)
P. M. Daling
B. A. Fecht
B. F. Gore
M. F. Mullen
T. B. Powers
R. E. Rhoads
R. E. Schreiber
R. J. Sorenson
A. S. Tabatabai
J. J. Tawil
Publishing Coordination (2)
Technical Information (5)

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1 REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG/CR-4462
PNL-5690

2 TITLE AND SUBTITLE
A Ranking of Sabotage/Tampering Avoidance Technology Alternatives

3 LEAVE BLANK

4 DATE REPORT COMPLETED
MONTH: November YEAR: 1985

5 AUTHOR(S)
WB Andrews, AS Tabatabai, TB Powers, PM Daling, BA Fecht, BF Gore, TD Overcast, WR Rankin, RE Schreiber, JJ Tawil

6 DATE REPORT ISSUED
MONTH: January YEAR: 1986

7 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Pacific Northwest Laboratory
P.O. Box 999
Richland, Washington 99352

8 PROJECT/TASK/WORK UNIT NUMBER

9 FIN OR GRANT NUMBER
NRC FIN B2548

10 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Systems Integration
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555

11a TYPE OF REPORT

b. PERIOD COVERED (Inclusive dates)
May 1984 - November 1985

12 SUPPLEMENTARY NOTES

13 ABSTRACT (200 words or less)

Pacific Northwest Laboratory conducted a study to evaluate alternatives to the design and operation of nuclear power plants, emphasizing a reduction of their vulnerability to sabotage. Estimates of core melt accident frequency during normal operations and from sabotage/tampering events were used to rank the alternatives. Core melt frequency for normal operations was estimated using sensitivity analysis of results of probabilistic risk assessments. Core melt frequency for sabotage/tampering was estimated by developing a model based on probabilistic risk analyses, historic data, engineering judgment, and safeguards analyses of plant locations where core melt events could be initiated. Results indicate the most effective alternatives focus on large areas of the plant, increase safety system redundancy, and reduce reliance on single locations for mitigation of transients. Less effective options focus on specific areas of the plant, reduce reliance on some plant areas for safe shutdown, and focus on less vulnerable targets.

14 DOCUMENT ANALYSIS - a KEYWORDS/DESCRIPTORS
Sabotage, Tampering, Safeguards, Probabilistic Risk Assessment, Insider, Core Melt Frequency, Prioritization, Design Criteria

b IDENTIFIERS/OPEN ENDED TERMS

15 AVAILABILITY STATEMENT
Unlimited

16 SECURITY CLASSIFICATION
(This page) Unclassified
(This report)

17 NUMBER OF PAGES

18 PRICE