NUREG/CR-6141
BNL-NUREG-52398

Handbook of Methods for Risk-Based Analyses of Technical Specifications

Prepared by
P. K. Samanta, I. S. Kim/BNL
T. Mankamo/AO
W. E. Vesely/SAIC

Brookhaven National Laboratory

Avaplan Oy

Science Applications International Corporation

Prepared for
U.S. Nuclear Regulatory Commission

NUREG/CR-6141
BNL-NUREG-52398

Handbook of Methods for Risk-Based Analyses of Technical Specifications

Manuscript Completed: November 1994
Date Published: December 1994

Prepared by
P. K. Samanta, I. S. Kim/Brookhaven National Laboratory
T. Mankamo/Avaplan Oy
W. E. Vesely/Science Applications International Coporation

Brookhaven National Laboratory
Upton, NY 11973-5000

Avaplan Oy
Itainen rantatie 17
FIN-02230
Espoo, Finland

Science Applications International Corporation
655 Metro Place South
Suite 745
Dublin, OH 43017

Prepared for
Division of Systems Research
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
NRC Job Code A3230

ABSTRACT

Technical Specifications (TS) requirements for nuclear power plants define the Limiting Conditions for Operation (LCOs) and Surveillance Requirements (SRs) to assure safety during operation. In general, these requirements are based on deterministic analysis and engineering judgments. Experiences with plant operation indicate that some elements of the requirements are unnecessarily restrictive, while a few may not be conducive to safety. Improving these requirements involves many considerations and is facilitated by the availability of plant-specific Probabilistic Safety Assessments (PSAs) and development of related methods for analyses.

Using risk- and reliability-based methods to improve TS requirements has gained wide interest because they can:

- quantitatively evaluate the risk impact, and justify changes in these requirements based on objective risk arguments; and
- provide a defensible basis for these requirements for regulatory applications.

The United States Nuclear Regulatory Commission (USNRC) Office of Research has sponsored research to develop systematic risk-based methods to improve various aspects of TS requirements. This handbook summarizes these risk-based methods.

The scope of the handbook includes reliability- and risk-based methods for evaluating allowed outage times (AOTs), scheduled or preventive maintenances, action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals (STIs), and management of plant configurations resulting from outages of systems, or components. For each topic, the handbook summarizes analytic methods with data needs, outlines the insights to be gained, lists additional references, and gives examples of evaluations.

TABLE OF CONTENTS

TABLE OF CONTENTS

FOREWORD

This handbook summarizes the results of research to develop methods for analyzing changes in facility Technical Specification (TS) requirements that are amenable to risk impact analysis (i.e., estimating the impact of TS changes on core-damage frequency or probability). These TS changes primarily involve allowed outage times (AOTs), surveillance test intervals (STIs), and action statements. The handbook can be used as a reference document to assist the NRC staff in reviewing licensees' risk-based analyses submitted as part of the bases for proposed changes in facility Technical Specifications.

A separate report documenting a detailed TS review and evaluation procedure (NUREG/CR-6172) is also being completed to give the NRC staff an integrated procedure for evaluating risk-based TS-change analyses and results that licensees may submit in future as part of the bases for proposed changes in the originally approved facility TS.

These two reports provide complementary information on TS evaluations. The handbook summarizes analysis methods and equations; the procedural outline describes a technical evaluation procedure for approval of proposed TS changes. The reports do not imply regulatory requirements. The reports summarize information learned from research and case evaluations.

ACKNOWLEDGEMENTS

We express our sincere appreciation and thanks to Carl Johnson, Jr. of United States Nuclear Regulatory Commission (USNRC), Technical Monitor for the project, for conceiving the concept of this handbook, and then diligently and patiently working with us in every step during its development. He also technically guided the research on risk-based methods for analyzing Technical Specification which made this handbook possible.

We also acknowledge Frank Coffman, Mark Reinhart, and Millard Wohl of USNRC whose valuable comments and insights we often used during the preparation of the handbook. We thank the reviewers of the handbook who provided many useful comments, improving both its content and presentation.

Gerald Andre', Westinghouse Electric Corporation
Lennart Carlsson, Swedish Nuclear Inspectorate
Erul Chelliah, USNRC
Andy Dykes, PLG, Inc.
John Flack, USNRC
Robert Hall, Brookhaven National Laboratory
James Higgins, Brookhaven National Laboratory
Joel Kramer, USNRC
Steven Mays, USNRC
Sonia Orlando Gibelli, Brazilian Regulatory Authority
Frank Rahn, Electric Power Research Institute
Curtiss Smith, Idaho National Engineering Laboratory
Herschel Specter, New York Power Authority
Jussi Vaurio, Loviisa Nuclear Power Plant, Finland
James Wing, USNRC

We also thank the technical editor, Avril Woodhead, for editing different versions of the handbook.

Finally, we express our appreciation for Donna Storan who patiently typed many versions of the handbook, took upon herself the preparation of the manuscript and did an excellent job. Kathleen Nasta was generous in helping prepare the manuscript as we often called upon her.

ABBREVIATIONS

AOT	Allowed Outage Time
AR	Action Requirement
BNL	Brookhaven National Laboratory
BWR	Boiling Water Reactor
CCF	Common-Cause Failure
CDF	Core Damage Frequency
CDP	Core Damage Probability
CM	Corrective Maintenance
CO	Continued Power Operation
CRD	Control Rod Drive
CT	Completion Time
EDG	Emergency Diesel Generator
EESD	Extended Event Sequence Diagram
EFW	Emergency Feedwater
EHV	Emergency Heating & Ventilation
EPRI	Electric Power Research Institute
ESW	Emergency Service Water
FSAR	Final Safety Analysis Report
HPCI	High Pressure Cooling Injection
IAEA	International Atomic Energy Agency
IPE	Individual Plant Examination
LCO	Limiting Condition for Operation
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOSP	Loss of Off-Site Power
LP&SD	Low Power and Shutdown
LPI	Low Pressure Injection
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PM	Preventive Maintenance
POS	Plant Operational State
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RCIC	Reactor Core Isolation Cooling
RHR	Residual Heat Removal
SAIC	Science Applications International Corporation
SBO	Station Black Out
SD	Shutdown
SNL	Sandia National Laboratories
SR	Surveillance Requirement

STD	Shutdown Transient Diagram
STI	Surveillance Test Interval
STS	Standard Technical Specification
SW	Service Water
TDP	Turbine Driven Pump
TS	Technical Specification

GLOSSARY

The terms defined here are somewhat unique to the risk-based analyses of TS and to this handbook. No attempt is made to cover the typical terms used in a PSA; rather, familiarity with such terms is assumed.

Allowed Outage Time (AOT): Allowed outage time, part of a limiting condition for operation (LCO), defines the time within which the equipment, specified in the relevant condition of the LCO, should be restored to operable status. Standard Technical Specifications (STSs) now use the term, completion time, which has a broader meaning than AOT, also defining the time for other required actions, such as verifying the status of other equipment, or changing plant modes (see "downtime").

AOT Risk Contribution: An AOT risk contribution is the risk contribution associated with an AOT. When a component is controlled by an AOT, two AOT risk contributions can be evaluated: a single-event AOT risk contribution and a yearly AOT risk contribution. (See "single-event AOT risk contribution," and "yearly AOT risk contribution.")

Conditional Core-Damage Frequency (CDF): The conditional CDF is the CDF conditional upon some event; in this handbook, typically it is the outage of equipment. It is calculated by re-running the PSA code after setting the unavailabilities of those basic events associated with the inoperable equipment equal to "True," and also adjusting the parameters of common-cause failures models, as appropriate, to represent the inoperable equipment.

Configuration Risk: Configuration risk refers to the risk associated with a specific configuration of the plant. A configuration usually refers to the status of a plant where multiple components are simultaneously down. (See "downed-configuration.")

Core-Damage Probability (CDP): The CDP represents the probability of core-damage occurring. We approximate core-damage probability by multiplying core-damage frequency by a time period. The CDP sometimes is called cumulative CDP because it is accumulated over time.

Corrective Maintenance: The actions needed to restore the operability of failed or degraded equipment within acceptable limits. These actions include repairs or replacement for failed equipment and maintenance actions for those degradations where immediate corrective actions are preferred.

Downed-Configuration: Multiple components which are simultaneously down is called a downed-configuration, or simply a configuration. In other words, it represents the status of plant components. If a component is operational, it is up; otherwise, it is down.

Downtime: The amount of time a component is down. If the component is controlled by an AOT, then this time is limited by the AOT for the component. The average duration of the component downtime is called the average downtime, and the average frequency of occurrence is called the average downtime frequency.

Downtime Effect of Maintenance: When a component is taken out-of-service for maintenance, it is associated with a certain downtime and its corresponding risk. The risk resulting from this inoperability of the component during the downtime is called downtime effect of maintenance.

Fault-Exposure Time: The time during which equipment is subject to failures (strictly, standby time-related failures) while on standby.

Limiting Condition for Operation (LCO): The LCOs impose limitations on plant operation by requiring the status of inoperable equipment to be restored within a specific time (i.e., the AOT). In Technical Specifications developed recently, such as Standard Technical Specifications (STSs), surveillance requirements also are included as part of LCOs.

Maintenance: Maintenance includes those actions that mitigate degradation of equipment, or restore the design function of failed equipment to an acceptable level. In the context of PSA models, maintenance includes both corrective and preventive maintenance.

Plant Operational State (POS): Plant operational states define the unique conditions as plant goes through different phases during shutdown operations, such as midloop operation or refueling.

Preventive Maintenance: The actions that detect, preclude, or mitigate degradation of a functional component to sustain or extend its useful life by controlling degradation and failures at an acceptable level.

Reliability Effect of Maintenance: Maintenance on a component may improve its reliability. Such an improvement due to maintenance is called the reliability effect of the maintenance.

Repair: The actions taken to restore failed equipment to operable status.

Rolling Maintenance Schedule: This involves planned, fixed-frequency maintenance of a group of components where a predefined set of components is allowed to be taken out-of-service for scheduled preventive maintenance. Typically, such schedules are defined for a fixed period, e.g., 12 weeks, and then repeated at the end of the period, i.e., every 12 weeks.

Running Start on Maintenance: A running start on maintenance refers to starting maintenance on a certain component (e.g. diesel generator) at power just before entering a scheduled refueling outage of the plant.

Single-Event AOT Risk Contribution: The single-event AOT risk contribution is the risk contribution from a given occurrence of the AOT. In terms of core damage, the single-event AOT risk contribution is the probability of core damage occurring during the AOT. The value is obtained by multiplying the increase in the core-damage frequency by the AOT.

Surveillance Requirements: Surveillance requirements are included in Technical Specifications as part of the LCO requirements. These requirements define those surveillances (or tests) which should be conducted, along with their frequencies.

Surveillance Test Interval (STI): The surveillance test interval is the period between consecutive tests, defined in terms of frequencies in the surveillance requirements of Technical Specifications. For example, if once per 31 days is defined, then the STI or the surveillance frequency is 31 days.

Test-Caused Risk: The test-caused risk represents those risk contributions that are due to the adverse effects of testing, such as errors causing plant transients, or wearout of the equipment due to testing.

Test-Limited Risk: The test-limited risk represents the risk contribution that can be limited by the test, by controlling the fault-exposure time. If tests are conducted more frequently (i.e., decreasing test interval), then the test-limited risk will be correspondingly reduced because then, the tests reduce the risk from potential failures between tests. The test-limited risk sometimes used to be called test-detected risk, emphasizing that this risk is directly related to the detection of failures by testing.

STI Risk Contribution: The STI risk contribution is the risk contribution associated with a surveillance test interval. This risk contribution includes the test-limited risk, arising from the possibility that a component may fail between tests, and test-caused risk, representing those contributions that are caused by the adverse effects of testing itself (see "test-limited risk" and "test-caused risk").

Yearly AOT Risk Contribution: The yearly AOT risk contribution is the average yearly risk contribution from the AOT, accounting for the average yearly frequency of the AOT. It is the frequency of core-damage occurring per year due to the average number of AOT occurrences per year. The value is estimated as the product of the single AOT risk contribution and the average yearly frequency of the AOT, namely the yearly frequency of how often the plant will enter the LCO associated with the AOT.

1. INTRODUCTION

Technical Specifications (TSs) for nuclear power plants (NPPs) define limits and conditions to assure that the plant is operated in a manner that is consistent with the analyses and evaluations in the plant's Safety Analysis Report. Under current NRC regulations (10 CFR 50.36), TSs are required as part of the Final Safety Analysis Report (FSAR) for each application for a licensee to operate a facility, and are incorporated into licenses authorizing its operation. Older NPPs have TSs that were developed specifically for that plant, while newer ones have plant-specific TSs based on the NRC-developed Standard Technical Specifications (STSs).

Technical Specification (TS) requirements for a plant include the Limiting Conditions for Operation (LCOs) and Surveillance Requirements (SRs) to assure safety during operation. These requirements originally were based on deterministic analyses and engineering judgments. However, experiences with plant operation indicate that some elements of the requirements may be unnecessarily restrictive, and a few may not be conducive to safety. As potential improvements or changes in these requirements are made, the NRC receives submittals from licensees proposing to modify certain aspects of TS requirements. This handbook is intended to aid NRC staff in reviewing these submittals using a risk perspective.

Risk-Based Analyses of TS

A broad spectrum of assessments and experiences are used in evaluating changes to TSs that involve deterministic analyses, knowledge of lessons learned from previous changes, engineering judgments, and risk implications of the change. The probabilistic safety assessment (PSA) of a NPP provides a tool for quantitatively assessing the risk contributions of TS requirements and the risk impact of a change. Such an evaluation is called Risk-Based Analyses of TS. It also is called a PSA-Based Analysis of TS because of the use of PSA models and methods. Assessing the risk impact of a change can be useful input for analyzing, reviewing, and accepting the change. Thus, with the availability of plant-specific PSAs, there is growing interest in using them to address changes to TS.

The objective of the handbook is to summarize risk-based methods for analyzing various aspects of the TSs. The primary focus is to assist NRC staff in reviewing risk-based analyses submitted by licensees to support proposed changes in TS requirements. Therefore, for the types of TS requirements amenable to risk assessment, the handbook summarizes analysis methods including:

- the issues to be considered,
- the methods and steps involved in the analysis, and
- illustrative examples and insights for evaluating changes to the TS requirements.

Analyses and Considerations in Changing TSs and the Role of the Handbook

The TSs of a nuclear power plant encompass a broad spectrum of requirements covering various aspects of plant operation. Because of differences in the types of requirements, the methods needed to analyze them differ. The availability of a plant-specific PSA allows many of the requirements within LCOs and SRs to be addressed consistently, based on their risk implications.

Within those TS requirements that can be so addressed, there are differences in the details of the analyses and the calculations needed. The methods presented in this handbook discuss such differences and, at the same time, unify the underlying concepts, applications, and usage of the methods. Bringing together in a single document those methods that apply to many of the TS requirements can enhance consistency in the application and its review, and can facilitate their use to improve a TS.

The handbook addresses permanent changes in the TS; however, the methods also can be used for analyzing one-time exemptions. We focus on active components (e.g., pumps, valves, instruments) in nuclear power plants. In other words, the types of components that are currently modeled in a PSA. In principle, the methods generally are applicable for analyzing TSs associated with other types of equipment or conditions, e.g., passive components (such as pipes, cables), and external events (requirements in response to fires, floods, wind conditions). However, the details involved in such usage can be different and are not delineated here.

We also focus on the analyses of TS requirements during power operation of the plant, although there also are TS requirements when the plant is shut down. In principle, the methods discussed here can be applied to shutdown periods using the corresponding PSA-model for the shutdown stages. However, the specific conditions

and parameters for shutdown analyses vary because different activities and requirements then should be taken into consideration.

Although this handbook focusses on PSA-based methods to analyze the risk impact of TS requirements, it is important to recognize that many other considerations go into a TS change, which we do not cover; for example, the considerations relating to occupational exposure and to the cost burden associated with changing TS requirements. However, a cost/benefit analysis might include the risk-analysis methods described in this handbook.

Organization of the Handbook

The handbook is organized in terms of the types of the requirements in the TS, and the associated PSA-based methods for analyzing the requirement.

Chapter 2, TS Risk Measures and PSA-Based Quantification, describes the general concepts associated with the risk-based measures used in TS analysis, and is relevant for all the applications presented. Separate chapters, numbers 3 to 8, are devoted to aspects of the requirement with its specific applications and analysis needs. These chapters are written so that readers can proceed directly to the one covering their topic of interest.

Three of the chapters directly relate to LCOs. LCOs include Allowed Outage Times (AOTs) and Action Requirements (ARs). The AOTs are used to undertake both corrective and preventive (or unscheduled and scheduled) maintenances. We first discuss the method for analyzing AOTs in Chapter 3, focussing on corrective maintenances, and then, in Chapter 4, expand on the methods to analyze preventive maintenances (PMs). In some cases, an AOT change may be desired to carry out certain PMs during power operation, and accordingly, the methods in Chapters 3 and 4 may need to be considered together. Action requirements (ARs) involving plant shutdown are discussed later in Chapter 7. The methods for analyzing ARs are more complex, involving analyses of risk associated with shutting down the plant, and may require including additional surveillance tests. Hence, this chapter follows the chapters on SRs. Use of the information in Chapter 7 is helped by knowledge of the methods given in Chapters 3 and 5.

Methods related to SRs are discussed in Chapters 5 and 6, both of which address surveillance frequency (or surveillance test intervals); Chapter 5 also discusses surveillance test strategy. The reason for these two separate chapters is that for many SRs the adverse effects are minimal so that these requirements can be analyzed adequately with the methods presented in Chapter 5. Only in selected cases will Chapter 6 be used where methods for addressing the adverse effects of testing are discussed.

Chapter 8, Managing Plant Configurations, discusses a concept and the approaches to an alternate way of implementing TS requirements where PSA-based methods are used more directly. This approach has the potential to shape the future TSs. Although selected portions relating to AOTs may be more appealing than others, this approach integrates AOTs, SRs, and ARs.

Two appendices are included. In Appendix A, the attributes of PSAs for TS applications are discussed. Appendix B provides details for evaluating conditional core-damage frequency (CDF) using PSA models. Each of the chapters is described below.

Chapter 2. TS Risk Measures and PSA-Based Quantification: Aspects relating to quantification of risk impacts are discussed, using the PSA models that generally apply to the methods in the handbook.

Chapter 3. Allowed Outage Time (AOT): This includes methods for evaluating AOT requirements and discusses the risk impacts of changes to single or multiple AOT requirements.

Chapter 4. Preventive Maintenance: TS LCOs have been specified so that, after a failure is detected, the equipment can be repaired during power operation of the reactor. However, these LCOs also are used for preventive maintenance during power operation. Risk-based analyses of preventive maintenance and scheduling of such maintenance are discussed.

Chapter 5. Surveillance Test Interval: This includes methods for evaluating the frequency of surveillance tests (or the surveillance test interval) and for considering the test strategy (e.g., staggered testing, sequential testing) in analyzing the test interval.

Chapter 6. Adverse Effects of Surveillance Testing: Some surveillances may be associated with adverse effects, e.g., test-caused transients or degradation. This chapter discusses methods to evaluate surveillance test intervals for these surveillance tests.

Chapter 7. Action Statements Requiring Shutdown: This chapter particularly addresses those systems which are needed for shutting the plant down. The risk of shutting the plant down when these systems fail can be substantial. We discuss methods for comparing the risk of continued operation versus shutdown to evaluate LCO requirements.

Chapter 8. **Management of Plant Configuration:** The risk from simultaneous outages of multiple components can be much larger than from single-component outages. TSs forbid outages of redundant trains within a safety system, but many other combinations of component outages can pose significant risk. In seeking TS changes and in controlling operational risk, these configurations may need to be analyzed. Risk-based analyses for outage configurations are discussed.

Use of the Handbook

The handbook is expected to have several uses:

a) The handbook is intended to aid in NRC reviews of risk-based analyses of TS requirements submitted by the licensees.

b) Licensees may find the handbook useful in preparing submittals to NRC proposing changes to their existing TSs, or in analyzing newly designed plants,

c) Licensees may find that individual Plant Evaluations (IPEs) can be used with the methods in this handbook to analyze TS requirements, and,

d) The methods discussed can enhance consistency in the analysis and in the review.

2. TS RISK MEASURES AND PSA-BASED QUANTIFICATIONS

In this chapter, we briefly discuss some of the concepts associated with analyzing the risk impact of TS requirements, particularly those aspects relating to the risk measures and their quantification using probabilistic safety assessment (PSA) models applicable to the methods presented in the later chapters. These discussions are not repeated elsewhere in the handbook unless a different viewpoint is applicable for a specific discussion.

We discuss the following aspects relating to risk-based methods for analyses of TS:

1. Different Risk Measures and Different Level of Analyses
2. Time-Dependent Versus Time-Averaged Analyses
3. Uncertainty and Sensitivity Analyses

2.1 Risk Measures and Levels of Analyses

When risks associated with TSs are to be evaluated, one has to decide on the risk measure to use and the level of analysis to carry out. The risk measures which can be used include:

Distribution of Early and Latent Fatalities
Frequency of Radioactive Release
Core Damage Frequency
Safety Function Unavailability
System Unavailability

The level of analysis involves the depth and detail to which contributors are modeled. The analysis may be carried out at a system, subsystem (or train), or component level.

In a system-level analysis, systems are modeled as black boxes. In a subsystem or a train-level analysis, the modeling resolution is down to the train level, and in a component-level analysis, models are taken to the component level.

Risk Measures

The applicable risk measure which is selected should be consistent with the basic function of the components whose TSs are being evaluated. Risk measures associated with accident frequencies should be calculated when evaluating components whose functions are to prevent accidents. The components involved in accident prevention, for example, include those in systems whose functions are involved in reactivity control, reactor coolant system integrity, core heat removal, and reactor coolant system pressure relief. Risk measures associated with accident prevention include the core damage frequency and unavailabilities of the associated safety functions and systems.

Risk measures measuring accident consequences should be assessed when evaluating components whose functions are to mitigate consequences of accidents. Such components, for example, include those in systems whose functions are involved in containment pressure suppression, containment integrity and fission product control. Risk measures associated with accident mitigation include complementary cumulative distributions of early and latent fatalities versus frequency, frequencies of radioactive release versus release category, and unavailabilities of safety functions and systems which are involved in mitigating the consequences of accidents.

Some components can be involved both in preventing and mitigating accidents. Prime examples are components in support systems, such as electric power systems, which provide support to systems involved in accident prevention and also to systems involved in mitigation. For these multi-functional components, both types of risk measures can be evaluated.

The risk measure to use for a given set of components should encompass all the hardware dependencies and functional dependencies among the components. For a set of components in a frontline system which is involved in only accident prevention and which provides no support to other systems, the system's unavailability at least needs to be evaluated. Function unavailability needs to be evaluated if the components are in more than one system but are involved in a common function, such as in emergency core-cooling. The core-damage frequency

should be evaluated if there is potential for more extensive hardware or functional interactions among the components.

Even though system or function unavailabilities can be evaluated if the components are self-contained in the system or function, it is a good strategy to evaluate the risk measure at a plant level, such as evaluating the core-damage frequency for components involved in accident prevention, and also the release frequencies (or containment failure probability) for components involved in accident consequence mitigation. Evaluating the risk at a plant level assures that all the interactions of components are included, and provides greater flexibility in identifying approaches to optimize resource requirements.

In this handbook, the methods are discussed in terms of the core-damage frequency, but as outlined above, corresponding measures can be defined directly. We use the term "risk," since the measures also imply early or latent fatalities, but we consider evaluations using core-damage frequency. The available PSA models and computer codes can conveniently calculate core-damage frequency.

Level of Analysis

For any risk measure, the level for analysis should be sufficiently detailed to accurately model the contributions being evaluated. For technical specifications which address component requirements, this means that component level modeling is required, i.e., the modeling should identify the individual components addressed by the TSs and their associated risk contributions. This generally means modeling to the individual pump, valve, and circuit-breaker. Even if the TSs address system requirements, component-level modeling usually is necessary to evaluate the system's risk contribution.

For certain TS risk evaluations, train-level modeling is adequate. For example, it is adequate for evaluating AOT risk contributions and configuration risks where the entire train goes down when a component in the train fail. Even for these situations, it is better to model to the component level since strategies for controlling the risks are focused at the component level, e.g., on the components being down.

2.2 Time-Dependent Versus Time-Averaged Analyses

In this handbook, the formulas for the risk contributions generally are applied using time-averaged risk calculations for analyzing the effects of testing; however, time-dependent analysis also is useful.

In using time-averaged calculations, the detailed time-dependent or instantaneous unavailability profiles of the components are not calculated, but instead,

the time-averaged unavailability and failure probability values are used in the formulas which are given. This is the usual practice in most PSA evaluations. Even for the formulas which are given to evaluate the risk impacts of configurations of components being down, the time-averaged unavailabilities of the other components generally are used.

The formulas given in the different chapters can be translated to time-dependent formulas by using time-dependent unavailabilities and time-dependent failure probabilities in place of the time-averaged values. This approach produces time-dependent risk contributions and risk impacts which can have uses for certain types of applications.

The following section summarizes the evaluations of time-dependent unavailabilities versus time-averaged unavailabilities. The section after discusses specific applications where time-dependent evaluations can provide important additional information.

Time-Dependent Versus Time-Averaged Unavailabilities

The figure below illustrates the standard sawtooth pattern for the time-dependent unavailability of a component between surveillance tests having an interval T and assuming a constant failure rate for the components.

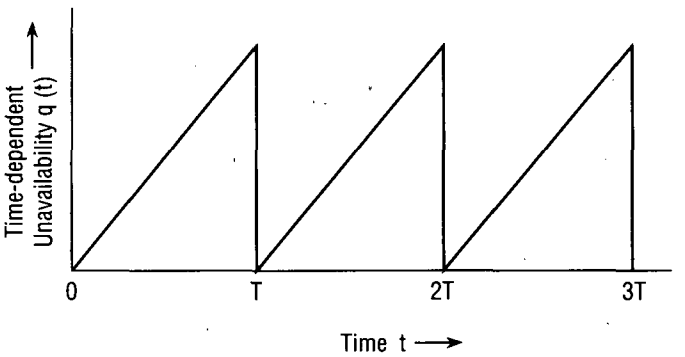

Figure 2.1 Time-dependent unavailability for a tested component

The figure assumes negligible downtime for test and repair, negligible test inefficiencies, and that, at the end of a test, the component unavailability is zero. The time-dependent component unavailability q(t) then rises according to the formula

$$q(t) = 1 - e^{-\lambda t}$$

$$\cong \lambda t \qquad (\lambda t < 0.1)$$

where λ is the component failure rate and t is the time since the last test. The time-dependent component unavailability is given by the above formula for t up to the test interval T, i.e. for $0 \leq t \leq T$. The time-dependent unavailability then is reduced to zero after the test assuming that it was effective test and that all failures are described by the failure rate λ. The time-dependent unavailability then repeats its behavior for the next test interval.

The time-averaged component unavailability q is determined by averaging q(t) over a test interval

$$q = \frac{1}{T}\int_0^T q(t)dt$$

$$= 1 - \frac{1}{\lambda T}(1 - e^{-\lambda T})$$

or

$$q \cong \frac{1}{2}\lambda T \qquad (\lambda T < 0.1).$$

The last formula is the first order approximation used in PSAs and in the formulas given in this handbook. Additional contributions for repair time and test downtime are added to q if these are non-negligible.

Time-Dependent Applications

Evaluations of time-dependent unavailability can provide important information in certain applications; this handbook discusses such time-dependent evaluations for specific applications. Those situations in which time-dependent modeling can be useful include:

More detailed evaluations of configuration risk impacts to account for when available components were last tested

More detailed evaluations of the effects of carrying out a test before repair or maintenance to account for the times of last tests

Evaluations of the effects of time-dependent unavailability resulting from test-caused wearout of a component

More detailed evaluations of the risk effects of scheduling component tests when the tests are not simple staggered or sequential ones.

For these types of applications, time-dependent evaluations can supplement the time-averaged evaluations if the benefits are deemed to be potentially significant.

2.3 Uncertainty and Sensitivity Analyses

Uncertainties in risk-based evaluations of TS due to data uncertainties can be assessed using standard uncertainty analysis techniques. Together, sensitivity analysis and uncertainty analysis can help to evaluate the robustness of insights and conclusions based on risk analysis.

In this handbook, the methods discussed and the evaluations involved can be used to carry out uncertainty analyses. However, we have presented many examples using point estimates of the risk measure, e.g., core-damage frequency. The methods for uncertainty analyses are not separately discussed as they do not differ from standard PSA uncertainty evaluations. (See, for example, Appendix C.6 of NUREG-1489, "A Review of NRC Staff Uses of Probabilistic Risk Analysis," PRA Working Group, 1994.)

Uncertainties in TS risk results due to data uncertainties could be evaluated using these uncertainty analysis techniques. Even though point values may be used in the intermediate calculations and in calculating individual risk contributions, it is a good strategy, at a minimum, to calculate the uncertainties for the final risk contributions for the set of proposed TS changes. The uncertainty calculations will help to assure that the conclusions are not affected by the uncertainties. If they do, then means for dealing with the uncertainties need to be identified. Sensitivity analysis is useful to understand the effects of assumptions which have little data or information to justify them. Sensitivity analyses are discussed separately for many applications.

3. ALLOWED OUTAGE TIME (AOT)

Basic Concepts

Allowed Outage Time (AOT): When a component goes down, there generally is a risk increase due to loss of function of the component. The AOT specifies the period in which the component can be down to restore its operation.

AOT Risk Contributions: For a given AOT, the risk contribution is calculated by multiplying the risk impact (CDF increase) by the AOT. There are two risk contributions, single-event and yearly, corresponding to the two risk impacts.

Control of the AOT Risk Contributions: The single-event AOT risk contribution is the contribution when the AOT is activated. The yearly AOT risk contribution is the average contribution from expected occurrences of the AOT. Both need to be controlled.

Risk-Based AOT: A risk-based AOT assures that the single event and yearly AOT risk contributions are acceptable.

Risk Impact of a Downed Component: The PSA calculates the risk impact of the component being down by calculating the resulting increase in core damage frequency (CDF) which results.

Single-Event Versus Yearly Risk Impacts: The single-event risk impact of a downed component is the increase in CDP assuming that the component is down. The yearly risk impact is the increase in CDF including the frequency of the component going down in a year.

Chapter Outline

List of Symbols

d downtime associated with an AOT

f downtime frequency or the average yearly frequency of occurrences of the AOT

R_1 the increased risk level, e.g., increased CDF, when the component is known to be down or unavailable

R_o the reduced risk level, e.g., reduced CDF, when the component is not down, i.e., down unavailability is zero

ΔR the increase in the conditional risk level, e.g., increase in CDF, given the component is down

r single-event AOT risk

R_y yearly AOT risk

3.1 Current Practices and Issues

Allowed outage times (AOTs) are defined as part of the limiting conditions for operation (LCOs) in TS for nuclear power plants. The AOT defines the time for which a component or a train in a safety system can remain inoperable before an action is required, which typically is plant shutdown. An AOT is used to repair or replace a failed or a degraded component, and sometimes, also to carry out scheduled maintenances. In Standard Technical Specification (STS), an AOT is called a completion time (CT), which has a somewhat broader meaning. We will use the term

AOT in its traditional sense as defined above, because the term completion time is not widely used yet.

The intent of an AOT is to provide adequate time to repair a failed component without incurring undue risk because of loss of function of the component. A long AOT implies a relatively larger risk to be incurred, but a shorter AOT may result in inadequate repair and/or unnecessary plant shutdown, both of which have risk implications. These requirements are defined largely based on engineering judgments. Experience with plant operation indicates that changes in some of them may be desirable.

A change in an AOT, for example , an increase in an AOT, may be desired to provide adequate time for repair/maintenance, to avoid unnecessary plant shutdown, or to obtain operational flexibility whereby increased attention may be focussed on risk-significant aspects. In certain cases, a decrease in an AOT may be required because of the large associated risk contribution. PSAs provide a systematic tool to address the risk contributions associated with an AOT, and to judge any change that may be desired. This chapter discusses risk-based analyses of AOTs, the steps in conducting the analyses, and gives example applications.

3.2 Overview of the Risk Contributions Associated with an AOT

During an AOT, the risk level generally increases because of the loss of function of the component.[1] The increase in risk level is the cause of the AOT risk contribution, as shown in Figure 3.1. Whenever a component goes down, there is an associated AOT risk contribution that needs to be controlled. The AOT risk contribution depends upon the specific risk measure which is focused on. For components in a safety system whose function is to prevent core damage, the most relevant risk measure is the core-damage frequency. For components in a safety system whose function is to mitigate the consequences of an accident, the most relevant measure is the frequency of severe consequence accidents, or the associated consequence-related risk. As a surrogate for core-damage frequency, the unavailability of the safety function or of the system can be selected as the important risk measure, provided that all contributions associated with the AOT, as discussed above, are included. Instead of the severe-accident frequency for a mitigating system, the unavailability of its safety function can be selected as the risk measure, again provided that all contributions associated with the AOT are included.

---

[1]For certain components, e.g. logic actuation components in a shutdown system, the risk level decreases when a component is brought down because other components are reconfigured. We shall focus on the more usual situation, where the risk level increases when the component goes down.

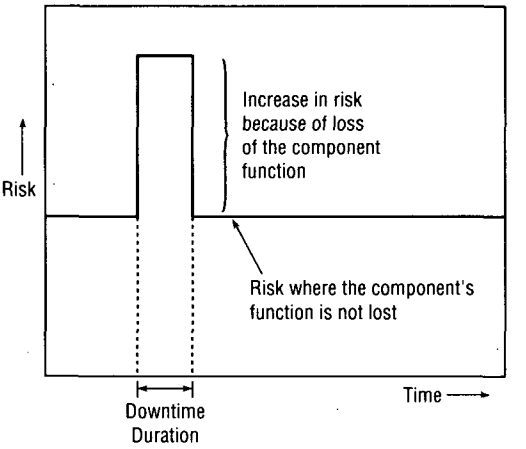

Figure 3.1 The risk contribution associated with an AOT

3.2.1 Definition of the Two Types of Risk Contributions Associated with an AOT

There are two types of AOT risks associated with the increase in risk level caused by a component going down, the *single-event AOT risk,* and the *yearly AOT risk contribution.* The single-event AOT risk is the risk associated with a given occurrence of the AOT. The yearly AOT risk contribution is the average yearly risk contribution from the AOT, accounting for its average yearly frequency. Thus, the single-event AOT risk is the conditional risk contribution, given the occurrence of the downtime. The yearly AOT risk contribution is the unconditional risk contribution, averaged over the expected number of occurrences of the downtime in a year. As discussed later, the average yearly AOT risk is product of the frequency of downtime occurrence and the single-event AOT risk. The single-event AOT risk and the yearly AOT risk contribution have different units; the former is the risk per downtime event, and the latter is the risk contribution per year. For example, in terms of a core-damage occurrence, the single-event AOT risk is the *probability* of a core damage occurring during the period the component is down. The yearly AOT risk contribution is the frequency of core damage occurring per year due to the average number of downtime occurrences per year. Since the AOT is initiated when the downtime event occurs, the single-event AOT risk needs to be controlled to control the risk for the given downtime event. Since the average yearly AOT risk contribution contributes to the average yearly risk, the yearly AOT risk contribution

also needs to be controlled. Hence, both contributions must be evaluated when specific AOTs are evaluated, or are proposed for modification.

3.2.2 Interaction of the Risk Contributions from Several AOTs

The single-event AOT risks from several AOTs do not generally interact nor do they accumulate to give a total contribution because the single AOT risks are conditional risks per event, and the downtime events for the different AOTs are different events. The only time that single-event AOT risks need to be simultaneously considered is when multiple components can be down at the same time, constituting the same event. Such a case is termed a downed-configuration, or simply a configuration. The risk contribution associated with a configuration is termed the configuration risk, and is evaluated separately as a multiple component downtime. Conducting maintenance on several components is a principal cause for potentially high configuration risks; then, the downtimes need to be scheduled so that the downtimes of critical components do not overlap. The focus here is evaluating single downtime occurrences.[2]

Yearly AOT risk contributions from several AOTs can interact and need to be accumulated to give the total yearly contribution from all the AOTs being considered. When the AOTs do not interact, i.e. when the downed components are not in the same minimal cutset, then the yearly AOT risk contribution from several AOTs is the sum of the individual yearly AOT risk contributions. When the AOTs do interact, i.e. when two or more of the downed components are in the same minimal cutset, then interaction of the AOT risk contributions need to be considered. The quantification of the single-event AOT risk and yearly AOT risk contributions is discussed subsequently.

3.2.3 The AOT Risk Contribution Calculated in the Usual PSA

The usual PSA only calculates the average yearly AOT risk contribution because the PSA calculates the yearly risk, e.g. the CDF, and the yearly AOT risk contribution is what contributes to the yearly risk. However, from the viewpoint of technical specifications, an AOT is activated when a given downtime event occurs. Thus, the AOT in technical specifications is a conditional requirement, conditional on the component going down; hence, the conditional risk contribution, which is the single-event AOT risk, needs to be assessed. The PSA can be analyzed simply to

---

[2]We note that all the equations to be presented for a component are applicable for a configuration, with proper interpretations. Configuration risks are separately discussed later in Chapter 8.

obtain the single-event AOT risk using standard PSA codes, as the next sections describe (Vesely, NUREG/CR-5425, 1989; Samanta et al., NUREG/CR-5200, 1988).

3.2.4 Basic Formula for the Single-event AOT Risk in Terms of the Contributing Factors

Let

ΔR = the increase in conditional risk level, given that the component is down

d = the downtime associated with the AOT, and

r = the single-event AOT risk

then

$$r = \Delta R \cdot d. \tag{3.1}$$

Thus, to calculate the single-event AOT risk, r, from basic factors, the associated increase in risk level ΔR and the associated downtime d is needed. Both the single-event AOT risk and the yearly AOT risk contribution, as well as the basic contributing factors, can be calculated from the PSA using standard PSA codes. Subsequent sections describe the PSA calculations which are involved in determining the AOT risk contributions and the increase in risk level.

3.2.5 Basic Formula for the Yearly AOT Risk Contribution in Terms of the Contributing Factors

The yearly AOT risk contribution is the product of the single-event AOT risk and the frequency of occurrence of the AOT.

Let

r = the single-event AOT risk

f = the average yearly frequency of occurrences of the AOT or the downtime frequency

and,

R_y = the yearly AOT risk contribution.

then

$$R_y = f \cdot r$$

Now, the single-event AOT risk r is

$$r = \Delta R \cdot d$$

hence

$$R_y = f \cdot \Delta R \cdot d, \tag{3.2}$$

where ΔR is the increase in risk level associated with the AOT, and d is the downtime associated with the AOT. Thus, the yearly average AOT risk contribution differs from the single-event AOT risk in that the former involves the extra factor of the average yearly downtime frequency, f. The downtime frequency, f, needs to be in units of per year for the risk R_y to be in units of per year. If the average yearly frequency, f, is greater than 1, then the numerical value of the average yearly AOT risk contribution is larger than the single-event AOT risk. If f is smaller than 1, then the numerical value of the average yearly AOT risk contribution is smaller than the single-event AOT risk. However, again we note that the single-event AOT risk is for a given downtime event, and the average yearly AOT risk contribution is the average contribution for a given year. The larger of these two measures should be used to select allowed outage times for technical specifications.

3.2.6 Using the PSA to Determine the Single-event AOT Risk and the Yearly AOT Risk

The PSA can be used to calculate the increase in risk level ΔR which is the key factor in determining the single-event AOT risk and the yearly AOT risk contribution.

Let

R_1 = the increased risk level when the component is known to be down or unavailable,

and,

R_0 = the reduced risk level when the component is known to be up or available.

The risk level can be the level of core-damage frequency, severe accident frequency, an expected consequence level, or even a system unavailability level. We shall focus on the core-damage frequency (CDF) as previously discussed. R_1 is the increased risk level, e.g. CDF, with the component assumed down, or equivalently, the component unavailability equal to 1. R_0 is the reduced CDF with the component assumed up, i.e. the component unavailability equal to zero. In terms of R_1 and R_0, the increase ΔR in risk level associated with the AOT then is

$$\Delta R = R_1 - R_0.$$

Using the above expression, the single-event AOT risk and the yearly AOT risk can be expressed as,

$$\begin{aligned} r &= \text{single-event AOT risk} \\ &= (R_1 - R_0) \cdot d \end{aligned} \tag{3.3}$$

and,

$$\begin{aligned} R_y &= \text{yearly AOT risk contribution} \\ &= f \cdot r \\ &= f \cdot (R_1 - R_0) \cdot d. \end{aligned} \tag{3.4}$$

R_1 can be calculated by setting the component-down event to a true state in the PSA. Similarly, R_0 can be calculated by setting the component-down event to a false state in the PSA. The component down event in the PSA is the event describing that the component is down for a repair or maintenance. If the component-down event is included in the existing minimal cutsets then these minimal cutsets can be used to determine R_1 and R_0 provided the minimal cutsets sufficiently cover the contribution of the down event. The existing minimal cutsets are sufficient if those containing the down event are not all near the truncation limit, i.e., are not all within a factor of 10 of the truncation limit. Alternatively, the minimal cutsets are sufficient if those containing the down event have a non-negligible contribution, i.e., have a contribution greater than or equal to 1%. If the existing minimal cutsets are sufficient, then the increased risk level R_1 can be determined by setting the component-down unavailability to 1 and deleting larger minimal cutsets which contain smaller minimal cutsets (i.e. are absorbed by the smaller minimal cutsets). If there are any minimal cutsets containing complementary events, then they also need to be removed if they are inconsistent with the component being down. The reduced risk level R_0 can be determined analogously by setting the down unavailability to zero.

If the component-down event is not contained in the existing minimal cutsets, or if there is question on the coverage of the existing minimal cutsets, then the minimal cutsets will need to be regenerated. R_1 is determined by setting the down-component event in the PSA models to a true state. The truncation limit of the minimal cutset can be reduced by at least a factor of 10 to give added assurance of sufficient coverage. The minimal cutsets which are generated subsequently then can be used to determine R_0 by setting the down unavailability at zero.

Contributions from common-cause failures need special attention when calculating the increased risk level R_1. If the component is down because of a failure, then the common-cause contributions involving the component need to be divided by the probability of the component being down due to failure since the component is given to be down. If the component is down because of being brought down for maintenance, then the common cause failure contributions involving the component need to be modified to remove the component and to only include failures of the remaining components (also see Appendix B).

If other components are reconfigured while the component is down, then these reconfigurations can be incorporated in estimating R_1 or ΔR, using the PSA. If other components are tested before repair or if maintenance is carried out on the downed components, then the conduct of these tests and their outcomes also can be modeled. If other components are more frequently tested when the component is down for the AOT, then this increased frequency of testing also can be incorporated. These modeling details are sometimes neglected in the PSA because of their apparently small contribution. However, when isolating the AOT risk contributions and in justifying modified AOTs, these details can become significant.

3.2.7 Obtaining the AOT Risk Contributions from the PSA Minimal Cutsets When it is Appropriate

As indicated, a PSA computes the yearly AOT risk contribution to the yearly core-damage frequency (CDF). Basically, the yearly AOT risk contribution is the sum of the minimal cutset contributions containing the component downed unavailability (typically, for maintenance), q_m,

$$q_m = f \cdot d$$

where f is the downtime frequency and d is the downtime associated with the AOT. The downtime, d, usually is estimated as an average downtime associated with the AOT. If the minimal cutsets sufficiently cover the downed unavailability, those which contain the downed unavailability q_m can be summed to give the yearly AOT risk contribution R_y. The previous section described the checks needed to assure that the

existing minimal cutsets sufficiently cover the downed component unavailability contribution so that they do not need to be regenerated.

To obtain the single-event AOT risk from the yearly AOT risk contribution, we can use the relationship between the single-event AOT risk, r, and the yearly AOT risk contribution, R_y:

$$R_y = f \cdot r$$

or

$$r = \frac{R_y}{f} \tag{3.5}$$

Thus, to obtain the single-event AOT risk r, the yearly AOT risk contribution R_y is divided by the downtime frequency, f, used in the PSA. The downtime frequency, f, must be expressed in units of per year to obtain the correct units for the AOT risk.

3.2.8 Consideration in Defining the Downtime Associated with an AOT

A final point should be made about the downtime value used to calculate the AOT risk contributions. In calculating the single-event AOT risk or the yearly AOT risk contribution, the downtime, d, associated with the AOT needs to be defined. As one alternative, the downtime can be defined to be the maximum downtime allowed, as specified by the AOT. Alternatively, the downtime can be defined to be the average downtime, based on an assessment of past history. Both downtimes should be used for comprehensive evaluations to show the range of AOT risks which can occur. If there is a large disparity between the two, the assumption that only a small fraction of the AOT will be used needs to be justified with data from experience.

When AOT risk contributions are being evaluated for a proposed extended AOT, then, usually, past data are not available for estimating average downtime. Conservatively, the average downtime can be assumed to proportionally increase with the increase in the proposed AOT for downtimes associated with corrective (or unscheduled) maintenances. For preventive (or scheduled) maintenances, the downtime assumed can be representative of plant practices, e.g., one half of the AOT.

3.3 Conducting AOT Risk Evaluations

3.3.1 The Steps Involved in a Systematic AOT Evaluation Process

A systematic evaluation should be carried out of the risks associated with either existing or proposed AOTs. The steps below represent such a process. To accomplish each step, the appropriate analysis described in the previous methodology sections must be conducted. These steps are listed below, and then the analysis involved in each is described briefly in the following pages.

Steps Involved in Systematic AOT Risk Evaluations

1. Identify the AOTs to be evaluated for their risk contributions.

2. For a given or proposed AOT to be evaluated, then determine the single-event AOT risk and yearly AOT risk contribution for each.

3. If multiple AOTs are evaluated, determine the overall yearly AOT risk contribution from all the proposed AOTs.

4. If not already carried out, check the AOT risk contributions, re-evaluating the PSA with the proposed AOTs.

5. Perform sensitivity evaluations or uncertainty evaluations to address the issues and uncertainties associated with the AOT risks.

6. If an AOT is to be defined to satisfy given risk criteria, then demonstrate that the criteria are satisfied.

7. Document the AOT risk evaluations, giving the associated risks, sensitivity results, and uncertainty results.

Step 1. Identify the AOTs to be Evaluated for Their Contributions

The first step is to identify the AOTs whose risk contributions are to be evaluated. The AOTs can be a set which are being considered for modification. Alternatively, the objective may simply be to evaluate existing AOTs for their single-event AOT risks and their yearly AOT risk contributions. The existing AOTs which then are prime candidates for additional attention are those having relatively high risks, and those which are prime candidates for relaxation are those having negligibly low risk.

Step 2. If a Given or Proposed AOT is to be Evaluated for its Risks, then Determine the Single-event AOT Risk and the Yearly AOT Risk Contribution for the AOT

For comprehensive risk evaluations, the single-event AOT risk and the yearly AOT risk contribution needs to be determined for every AOT evaluated. From the previous presentations of AOT risk methodology, if

r = the single-event AOT risk

and,

R_y = the yearly AOT risk contribution

then, in terms of the basic contributing factors

$$r = \Delta R \cdot d$$

and,

$$R_y = f \cdot \Delta R \cdot d$$

where

ΔR = the increase in risk level

d = the downtime associated with the AOT

and,

f = the downtime frequency.

The options for defining d are

$d = \bar{d}$ = the mean downtime under the AOT
$d = d_{max}$ = the maximum allowed downtime under the AOT.

Both values can be used for comprehensive evaluations.

Step 3. If Several AOTs are Evaluated, Determine the Overall Yearly Risk Contribution From All the AOTs

As described in the methodology, the yearly AOT risk contributions from several AOTs accumulate to give a total risk contribution. The single-event AOT risks do not accumulate because they are conditional, depending upon different given events. Thus, if several AOTs are proposed or are evaluated, the overall yearly AOT risk contribution needs to be evaluated. If the AOTs are all in different minimal cutsets, then there are no interactions among them, and the individual yearly AOT risk contributions are additive. If two or more of the AOT components appear in the same minimal cutset (i.e. the downed unavailabilities of two or more components appear in the same minimal cutset), then interactions among the yearly AOT risk contributions need to be evaluated. The interaction among the yearly AOT risk contributions can be accounted for by substituting the corresponding downtimes and the frequency of the downtime to replace the maintenance downtime unavailabilities for the relevant components in the PSA and then re-calculating the results.

Step 4. If Not Already Done, then Check the AOT Risk Contributions by Evaluating the PSA with the Proposed AOTs

If modified AOTs are being proposed, then the yearly AOT risk contributions need to be checked by substituting the proposed AOTs in the PSA and re-calculating the results. If this has been done previously, it need not be repeated. Checking is particularly applicable when the AOTs are determined to satisfy given criteria and the risk contributions have not yet been checked.

Step 5. Perform Sensitivity Evaluations or Uncertainty Evaluations to Address the Issues and Uncertainties Associated with the AOT Risks

The following uncertainties and sensitivities which specifically affect the AOT contribution need to be assessed:

1. The effect on the AOT risk contribution of using the mean downtime versus the maximum AOT,

2. The effect of assumptions and lack of data on estimates of the mean downtime used to calculate the AOT risks,

3. The effects of any component reconfigurations and additional tests or checks on the AOT risks,

4. The effects of common-cause failure contributions to the AOT risks,

5. The effects of human-error contributions and recovery probabilities to the AOT risks,

6. The effects of general PSA uncertainties in terms of plausible ranges for the AOT risk contributions.

Step 6. If an AOT is to be Defined to Satisfy Given Risk Criteria, then Demonstrate that the Criteria are Satisfied

Instead of proposing AOT values and then evaluating their risk contributions, AOT values can be defined to satisfy given risk criteria. Such a criteria-determined AOT is obtained by setting the single-event risk, r, and the yearly downtime risk contribution, R_y, to be less than or equal to given acceptable values r_c and R_c, respectively

$$r \leq r_c$$

$$R_y \leq R_c.$$

Substituting the basic contributing factor expressions for r and R gives

$$\Delta R \cdot d \leq r_c$$

$$f \cdot \Delta R \cdot d \leq R_c$$

or

$$d \leq \frac{r_c}{\Delta R}$$

$$d \leq \frac{R_c}{\Delta R \cdot f}$$

The above constraints can be written more concisely as:

$$d \leq \min \left[\frac{r_c}{\Delta R}, \frac{R_c}{\Delta R \cdot f} \right] \qquad (3.6)$$

where "min" determines the minimum of the arguments. The maximum, d, which satisfies the risk constraints is determined by setting the inequality " $\leq$ " to an equality " $=$ ".

When implementing the above criteria for several AOT values, then additional considerations are needed. Because the yearly AOT risk contributions accumulate, if several AOTs are being evaluated, then R_C should account for the multiple AOT contributions (for example, for each AOT the contribution R_C/n can be used where n is the number of AOTs being determined).

Step 7. Document the Evaluations and Prepare a Summary Table of the Results

The AOT risk evaluations which were carried out in the previous steps should be fully documented. The calculations should be presented in a format which can be auditable, and be clearly traceable to the data and assumptions used. The results and associated calculations presented should include the following:

1. For each AOT, the single-event AOT risk and the yearly AOT risk contribution,

2. The total yearly AOT risk contribution from all the AOTs evaluated,

3. The single-event risk and yearly AOT risk contribution using the total AOT as the downtime,

4. A description of the basis and data used to determine the average downtimes used to calculate the AOT risks,

5. A discussion of the basis for the values used for the downtime frequencies in determining the yearly AOT risk contributions,

6. Preventive Maintenance (PM) risk contributions, as applicable, considering the PM schedules to be used, if AOT modification is being sought to conduct PM during power operation (discussion in Chapter 4),

7. Estimations of the uncertainties associated with the AOT risk contributions, which need not involve formal uncertainty propagations, but can be based on the PSA results and considerations of the factors involved in the AOT risks,

and,

8. A discussion of the sensitivities associated with the AOT risks due to common-cause failures, human errors, and other factors which can cause the AOT risks to vary.

3.3.2 Data Needs for AOT Analyses

The following are the special data needs for AOT analyses, in addition to the data collected as part of a PSA:

- Distribution of repair times of components: this is needed to judge whether adequate AOT is being provided to complete a repair. This distribution also can be used to estimate the expected risk for a given AOT. The distribution of repair time may shift when an AOT is being changed. However, information about such an influence on the distribution is not expected to be available when the AOT modification is being studied.

- Frequency of downtime: the frequency of downtime for a component may be a factor of 3 to 10 times higher than the failure frequency. Since AOTs can be used for maintenance, the frequency of maintenance should be incorporated in estimating the downtime frequency.

- Schedule for performing PM: maintenance scheduling used by the plant, defining the situations when multiple equipment or system trains may be taken down for PM. These schedules are important to assure that high risks from components being simultaneously down do not occur.

- Restoration probabilities for components in PM: during a component outage for PM, if a component is requested to function, it may be possible in certain situations to restore it within a reasonable time. If bounding evaluations show that early restoration is unlikely, then the component will be considered fully unavailable. If detailed evaluations of restoration possibilities are to be performed, then data defining restoration probabilities should be obtained.

3.4 Examples of Evaluations of AOT Risk Contributions

3.4.1 Introduction

In the following sections, examples are given of evaluations of AOT risk contributions. These risk contributions are AOT core-damage frequency (CDF) contributions, both single-event AOT risks and yearly AOT contributions. The results are taken from NUREG/CR-5200, "Evaluations of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant" published as part of the NRC research program on risk-based technical specifications.

The objective of the calculations in NUREG/CR-5200 was to determine the CDF contributions associated with present AOTs at this particular plant using the plant's PSA. The calculations demonstrated the sizes of AOT CDF contributions and also, how such calculations could be used to prioritize AOTs. The AOTs with the highest CDF contributions, for either single-event AOT risks or yearly AOT risk contributions, would be the focus for risk control; those with the lowest contributions would be candidates for relaxation.

The next section has an example of the calculated AOT risk contributions and their contributing factors, as determined from the plant's PSA. The results are discussed in terms of methodology which was described. The section after the next one shows examples of tables which can be constructed to tabulate the AOT risk contributions, not only for present AOTs but for proposed modified ones. The tables would be supplemented by sensitivity or uncertainty analyses and discussions of data and assumptions involved, which are particularly important to define the bases for proposed AOTs.

3.4.2 Calculation of the Single-event AOT Risk and Yearly AOT Risk Contribution

The example below presents values for the AOT CDF contributions and their contributing factors determined from the plant PSA, and given in NUREG/CR-5200.

Component: High Pressure Injection (HPI) Pump 36C
AOT (d): 60 hr
Downtime Frequency (f): 3.1×10^{-5} per hour
Increase in CDF (ΔR): 2.7×10^{-3} per year
Single event CD Probability (r): 1.9×10^{-5}
Yearly CDF Contribution (R_y): 5.0×10^{-6} per year

The component is a particular pump and the AOT is the allowed downtime as specified by the technical specifications. The increase in CDF per year is the

increase in the conditional CDF when the HPI pump is down. To obtain the single-event AOT risk at the core-damage frequency level, the increase in CDF is multiplied by the AOT of 60 hrs. The AOT needs to be transformed to units of years (60 hours x 1/8760 hours per year = 6.8×10^{-3} years). The average downtime also can be used for assessment, in which case the average downtime instead of the AOT would be used. The average downtime chosen would need to be justified from plant experience. The sum of the minimal cutset contributions, as calculated in the PSA, used the average downtime associated with the AOT which is less than the total AOT of 60 hours. Consequently, the minimal cutset contributions can be multiplied by the ratio of the total AOT to the average downtime to obtain the same result.

The yearly AOT CDF contribution is calculated by multiplying the single-event AOT risk by the downtime frequency. To do this, the downtime frequency of 3.1×10^{-5} per hour needs to be transformed to units of per year (3.1×10^{-5} per hour x 8760 hours per year = 2.7×10^{-1} per year). We note that, in this case, the yearly CDF contribution is significantly less than the single CDF contribution since the downtime frequency is less than 1. The downtime frequency used in this example (and in NUREG/CR-5200) is for corrective maintenances needed for failures of the component; maintenances for degradation of the component or scheduled preventive maintenances are not included. The AOT risk measures discussed here also should include these other types of maintenances. Risk-based analyses of these types of maintenances are discussed in the following chapter.

3.4.3 Tables of AOT Risk Contributions

Tables 3.1 and 3.2 illustrate how the calculated single-event AOT risk and the yearly AOT risk contributions can be presented in tabular form to summarize the pertinent risk information. Table 3.1 presents the AOT risks for the components in the High Pressure Injection (HPI) system, and Table 3.2 for the components in the Low Pressure Injection (LPI) system. Similar tables also can be constructed using the average downtime instead of the total AOT. The results, which are taken from NUREG/CR-5200, show the large variation in present AOT risk contributions and the potentials for improvement.

3.5 Risk Strategies Involving AOT Risks

3.5.1 Introduction

It is desirable to focus attention on the AOTs with the highest risk contribution and to redirect unnecessary attention away from AOTs of negligible risk contribution. Various strategies can be employed in proposing modifications to AOTs using risk considerations; one is that the proposed AOT modifications result in no net increase in risk.

Table 3.1 AOT Risks at the CDF Level for the High Pressure Injection (HPI) System

Component	AOT (hr)	Downtime Frequency f (per hr)	Increase in Conditional CDF, ΔR (per year)	Single-event AOT Risk (CD Probability) r	Yearly AOT CDF Contribution R_y (per year)
HPI Pump 36C	60	3.1E-5	2.74E-3	1.88E-5	5.1E-6
HPI Pump 36B	60	3.1E-5	1.50E-5	1.03E-7	2.8E-8
HPI Pump 36A	60	3.1E-5	5.00E-6	3.43E-8	9.3E-9
HPI MOV 1227	60	4.0E-7	3.00E-5	2.06E-7	7.2E-10
HPI MOV 1228	60	4.0E-7	3.00E-5	2.06E-7	7.2E-10
HPI MOV 1219	60	4.0E-7	1.20E-5	8.22E-8	2.9E-10
HPI MOV 1220	60	4.0E-7	1.20E-5	8.22E-8	2.9E-10

Table 3.2 AOT Risks at the CDF Level for the Low Pressure Injection (LPI) System

Component	AOT (hr)	Downtime Frequency f (per hr)	Increase in Conditional CDF, ΔR (per year)	Single-event AOT Risk (CD Probability) r	Yearly AOT CDF Contribution R_y (per year)
LPI Pump 34B	60	3.1E-5	5.10E-5	3.49E-7	9.5E-8
LPI Pump 34A	60	3.1E-5	5.00E-5	3.43E-7	9.3E-8
LPI MOV 1406	60	4.0E-7	7.90E-5	5.41E-7	1.9E-9
LPI MOV 1405	60	4.0E-7	7.20E-5	4.93E-7	1.7E-9
LPI MOV 1428	60	4.0E-7	5.00E-5	3.43E-7	1.2E-9
LPI MOV 1429	60	4.0E-7	5.00E-5	3.43E-7	1.2E-9
LPI MOV 1400	60	4.0E-7	6.00E-6	4.11E-8	1.4E-10
LPI MOV 1401	60	4.0E-7	5.00E-6	3.43E-8	1.2E-10

To accomplish this, a risk-reduction strategy can be considered. Also, increases in risk due to AOT relaxations can be compensated for by decreases in risk due to risk-reduction actions. These actions may involve tightening AOTs on other components, or others, such as testing a redundant train before beginning the AOT. Also, they can involve carrying out a maintenance or quality assurance. However, in some case, certain options may not be applicable from engineering considerations. In general, the AOTs and the action defined should make engineering sense and not be based on numerical manipulation.

Since the increase in risk associated with an AOT relaxation can be very small, particularly if the AOTs are of negligible importance, the actions to reduce risk do not necessarily need to entail significant resources. Furthermore, for small changes in risk, the risk reduction does not need to be accurately quantified. In some cases, quantification may not be necessary and a qualitative description may suffice. The following sections describe strategies which can be considered in achieving a net reduction in risk or no net increase from one or more AOT modifications.

3.5.2 Reducing the Risk Increase Associated with the AOT by Testing Redundant Components Before the AOT

To reduce the single event risk and yearly risk contribution associated with an AOT, the first question that can be asked is whether the associated increase in risk level can be reduced. From the previous methodology sections, both the single-event risk r and the yearly risk contribution R_y are proportional to the increase in risk level ΔR caused by the downed component. The equations for the single-event AOT risk, r, and the yearly AOT risk contribution, R_y, are, again,

$$r = \Delta R \cdot d$$

and,

$$R = f \cdot \Delta R \cdot d$$

$$= f \cdot d \cdot (R_1 - R_0)$$

Both of these risks can be reduced for a given proposed downtime d if R_1 can be reduced. Even if there is a longer proposed downtime, the AOT risk contributions can be reduced if R_1 can be reduced, thereby lessening the risk-impact of the downed component.

To reduce the increased risk level R_I, the unavailability of one or more of the other components in the contributing minimal cutsets needs to be reduced.[3] One of the most direct ways to achieve this is to test the component to determine if it is operational. If the test effectively assesses the failure mode identified in the PSA and there is negligible downtime associated with the test, then the unavailability is reduced and the contribution of the minimal cutsets containing the tested component is reduced.

One must assure that there is no significant downtime associated with the test, comparable to the AOT downtime d, otherwise the test will not effectively reduce the unavailability. If the component's unavailability is due to a faulty configuration, then a simple test or check often can effectively reduce its unavailability. For example, stroke-testing a valve from the plant control room to determine if it is operable is an effective test with negligible downtime. Even if only a partial test is conducted, the unavailability of the tested component can be reduced by some factor which can reduce the increased risk level R_I.

After the test is conducted, the unavailability of the tested component will increase with time according to the formula $1 - \exp(-\lambda t) \cong \lambda t$, where λ is the component's failure rate and t is the time from test. This effect generally will be small and can be ignored if the AOT downtime is small, for example, less than one week. The smallness of the unavailability can be checked by calculating $(1/2)\lambda d$ which is the average unavailability of the tested component during the downtime, d. If the contribution is non-negligible, then it should be included in the evaluation.

There will be a residual unavailability of the tested component due to a cyclic or per-demand contribution to the component's failure rate that will cause the unavailability of the tested component to not be zero after the test, but instead, be some residual value ρ. After time t, the unavailability then will be approximately $\rho + \lambda t$. This residual contribution can be neglected as a first approximation and sensitivities can be performed on the effects of various values for the residual unavailability.

---

[3]The increased contribution to risk level also is proportional to the frequency of initiating events in each minimal cutset, although this frequency usually cannot be reduced.

3.5.3 Reducing the Risk Increase Associated with the AOT by Reducing Other Component Unavailabilities

As an extension of the strategies in the previous section, the increased risk level associated with the downed component can be decreased by more generally reducing the unavailability of one or more components in the same minimal cutset as the downed component. Some examples include decreasing the test interval which results in earlier detection of failure so reducing the unavailability, reducing the downtime, improving the component so it has a lower failure rate, reducing common-cause failure probabilities, reducing human-error probabilities, and carrying out more effective tests and maintenances. Accomplishing these results does not need to involve significant resources, but can involve improving existing activities to focus on the important contributors to the increased risk level. The actions should be commensurate with the risk. If the AOT risk contribution is small, then minor improvements will be sufficient to counter the small contribution. Qualitative evaluations may be reasonable.

4. PREVENTIVE MAINTENANCE

Basic Concepts

Downtime Effect of Maintenance: When a component is taken out-of-service for maintenance, it is associated with certain downtime and its corresponding risk. The risk resulting from this inoperability of the component during the downtime is called the downtime effect of maintenance.

Maintenance Schedule: It is the schedule followed to conduct PM. In such a schedule, multiple components, implicitly allowed by TS, may be taken out-of-service at a time, e.g., in a rolling maintenance schedule.

Preventive Maintenance: The action that detects, precludes or mitigates degradation of a functional component to sustain or extend its useful life by controlling degradations and failures at an acceptable level.

Risk-Based Maintenance Scheduling (power operation vs. shutdown): In risk-based maintenance scheduling, the downtime effect of maintenance is assessed (sometimes comparing the effects during power operation vs. shutdown) to decide when maintenance should be scheduled.

Risk Impact of Maintenance Schedule: The incremental risk, e.g., increase in the CDF, associated with a maintenance schedule where multiple components may be taken out-of-service at a time and at a pre-defined frequency.

Chapter Outline

List of Symbols

d_{PM}	downtime associated with a PM
f_{PM}	frequency of PM
r_{PM}	single PM risk contribution (similar to single event AOT risk contribution r)
ΔR	the increase in the conditional risk level, i.e., increase in the CDF, when the component is down for PM
R_{PM}	yearly PM risk contribution (similar to the yearly AOT risk contribution R_y)
$R_1(P,Wn)$	CDF when the components scheduled for PM during week n are taken out-of-service (for power operation of the plant)
$R_1(P)$	CDF at power, when the component is taken down for maintenance
$R_1(POSn)$	CDF in a given operational state during shutdown, when the component is taken down for maintenance
$r_{PM}(SD)$	risk incurred, e.g., estimated in terms of CDP, to perform the PM by shutting the plant down
$r_{PM}(PO)$	risk incurred, e.g., estimated in terms of CDP, to perform the PM while the plant is at power

4.1 Current Practices and Issues

Components in safety systems of nuclear power plants require preventive maintenance (PM) to assure their reliability. These maintenances are performed both during power operation and shutdown, but traditionally, the bulk of them are carried out during shutdown. However, because of the longer fuel cycles and the desire to reduce the plant's shutdown outages, increasing amounts of PM are being scheduled during power operation. The following are the two dominant effects of PM:

a) Improving the components' reliability, resulting in a decrease in the plant's risk level in the long run, called the reliability effect.

b) Increasing the plant's risk level due to loss of function for the duration of the PM, called the downtime effect.

The PMs are performed using the LCO requirements defined in the plant TS (i.e., the AOTs discussed in Chapter 3). These requirements originally were intended for repairing failures, but are used to voluntarily declare an equipment inoperable to perform a PM. Thus, the duration of the PM is limited by the AOT, and also, LCO requirements are followed, limiting simultaneous outages of redundant trains in a system.

The practice of PM at power is widespread in nuclear facilities; however, the implementation approaches vary from one plant to another. Some nuclear power plants carry out PM as needed, based on the results of routine surveillance tests of the components. Others follow a rolling maintenance schedule, where each week a predefined group of components is permitted to be taken out-of-service for PM. This type of PM schedule is defined for a fixed period, e.g., 12 weeks, and is repeated at the end of the period, i.e., every 12 weeks.

The following are some of the common features associated with PM practices:

a) multiple components, implicitly allowed by TS, being taken out of service at a time,

b) repeated entry into LCO to perform PM, resulting in large equipment downtimes,

c) significant portion of the power-operation period may be spent in the LCO condition to carry out PM, e.g., in a rolling maintenance schedule.

The following are the risk implications of such practices during power operation:

a) CDF impact of simultaneous outages of multiple components can be significant,

b) the plant CDF can be higher than the assumed value (calculated in a PSA) due to the PM schedules being used,

c) the contribution to CDF due to PM downtimes can be a significant contribution to the risk of the plant.

Scheduling PM involves many considerations relating to the risk implications discussed above, cost-benefit issues aiming at reduction of plant operation and maintenance costs, and maintenance needs in increasing the plant's capacity. Considering these interacting issues, PM schedules are decided which may include both power and shutdown operation periods. Shifting the PM burden from power to shutdown operation and vice-versa has corresponding concerns since the risk implication of PM during shutdown is not necessarily negligible.

Such risk, particularly during the early stages of a shutdown, can be comparable to that during power operation, and shifting the PM burden to periods of shutdown may not necessarily be desirable. A large PM burden during shutdown also increases the refueling outage period for the plant and can be costly. Table 4.1 summarizes the potential problems to be considered if preventive maintenance is scheduled during power operation versus shutdown.

In this chapter, our focus is primarily on addressing the methods relating to the analyses of risk implications of PMs. If AOTs are used during power operation to conduct the PMs, such evaluations form a part of the AOT evaluation.

4.2 Applications of Risk-Based Analyses of PM

Currently, PSA models include the contributions from maintenance downtime, but the beneficial impact of maintenance, i.e., the improvement in reliability due to PM, is not separated out. In general, PSA models can be used to assess the impact of component downtimes due to a PM. The PSA applications to evaluate PM are focussed on assessing this risk impact of PM downtimes, and seeking alternatives to the PM plan to minimize the impact. Three types of applications can be considered:

a) Assessing the risk impact of PM for individual components,

b) Evaluating PM schedules, e.g., rolling maintenance schedules to be implemented, and analyzing available alternatives,

c) Deciding between scheduling a PM during power operation versus shutdown, based on analyses of risk impacts.

Table 4.1 Potential Problems to be Considered if PM is Scheduled During Power Operation Versus Plant Shutdown

PM DURING POWER OPERATION	
Potential Problems to be Considered	**Insights**
Repeated use of LCO to perform PM; increased component unavailability	Monitor unavailability due to PM. If its duration and frequency during power operation are excessive, set limit on both during power operation
Multiple components may be simultaneously down for PM	Control PM schedules to assure that risk implications are acceptable
Unreliable failure history; failures may be masked because of PM before testing	Interpretation of surveillance test data when PM is performed prior to testing may be different from data for tests without a prior PM
Uncertainty that PM can be completed, and component returned to service	Schedule during specified shutdown period
PM DURING PLANT SHUTDOWN	
Potential Problems to be Considered	**Insights**
Risk impact is significant during certain shutdown periods	Avoid long-duration PM during specified shutdown activities (e.g., initial phases of shutdown); perform PM during certain low-risk shutdown periods
Outage Duration of plants can be lengthened if the burden of PM during shutdown period is increased	Allow some PM activity during power operation (the PM scheduled during power operation should be such that it does not imply "running start" on maintenance)
Unreliable component during power operation	Optimize PM program between power operation and shutdown; certain PM during power operation may improve the components' reliability

4.3 Method for Analyzing Risk Impact of Maintenance

A. Risk Impact of PM on a Single Component

The risk contributions associated with the PM of a component is similar to that associated with AOTs (discussed in Chapter 3). Here, we review the basic formulas applicable to PMs and discuss the differences with the AOT risk measures.

When a component is taken out-of-service or made unavailable for a PM, the risk contribution of a single PM is given by:

$$r_{PM} = \Delta R \cdot d_{PM} \tag{4.1}$$

Where

ΔR = increase in the CDF when the component is down,
d_{PM} = downtime associated with the PM,
r_{PM} = single-event PM risk contribution (for a component).

Similarly, the yearly PM risk contribution is given by:

$$R_{PM} = f_{PM} \cdot \Delta R \cdot d_{PM} \tag{4.2}$$

Where

f_{PM} = yearly frequency of PM on the component,
R_{PM} = yearly PM risk contribution (for the component).

Differences with AOT Risk Measures

The differences with AOT risk measures relate to the interpretation of the parameters and in their estimations.

The downtime due to a PM, d_{PM}, is usually precisely known compared to d, downtime associated with a corrective maintenance (CM). In other words, since PM typically is a planned activity, uncertainty in d_{PM} is minimal, whereas d associated with a CM could have significant uncertainty.

The frequency of PM, f_{PM}, also may be precisely known. In some cases, PM activities are scheduled at fixed intervals, e.g., in a rolling maintenance schedule, where f_{PM} may have no direct relation to the failure rate of the component.

The increase in risk level, ΔR, when the component is down is similar to the AOT analysis, but can differ slightly (see Section 3.2.6 and Appendix B for calculation of ΔR). For conservative calculations, which are adequate in many applications, the same value can be used. The primary difference is in modeling the common-cause failure (CCF) contribution of the redundant components when ΔR is calculated. The base-case PSA may include a CCF contribution for the CCF of the component being taken down for PM and the redundant components in the system. When one of the components is taken down for PM, and, as part of the PM procedure, the redundant component is successfully tested before starting the PM, then the CCF term is negligible; this reduces the value for ΔR. However, the PSA model is applicable if the components' statuses are not known when a PM is being carried out.

B. Risk Impact of Maintenance Schedules

The maintenance schedule of a plant may involve multiple components being taken out-of-service simultaneously. Such a schedule may be predefined and may involve different groups of equipment being taken out-of-service at different times. For example, in a 12-week rolling-maintenance schedule, the set of equipment that may be taken out-of-service every week to perform PM is predefined, and is repeated every 12 weeks.

PSA-based analyses of maintenance schedules involve assessing their average impact on the CDF when such schedules are followed. These measures can be used to obtain the CDF impact of the PM schedule and compare alternatives for controlling the adverse effects due to PM downtime.

Assuming that the schedule is repeated every n-weeks, let us define

$R_1(P,W1)$ = CDF when the components scheduled for PM during week 1 are taken out-of-service

$R_1(P,W2)$ = CDF when the components scheduled for PM during week 2 are taken out-of-service

.
.
.

$R_1(P,Wn)$ = CDF when the components scheduled for PM during week n are taken out-of-service

These calculated CDFs can be plotted to obtain the CDF level due to the particular maintenance schedule. The average CDF due to the maintenance schedule can be estimated if the actual duration of maintenance in each week is known.

Otherwise, a bounding estimate can be obtained, assuming that the components are unavailable during the entire week; this is a conservative value, since, in many cases, PM requires only a fraction of the allotted week. Also, the component may not be scheduled for maintenance every n weeks when PM is permitted. These bounding evaluations are adequate for comparing alternate maintenance schedules.

C. Scheduling Maintenance Between Power Operation Versus Shutdown

Another aspect of maintenance scheduling is to decide whether the maintenance is to be carried out during power operation or at plant shutdown. In general, the assumption is that the risk impact of a component being out-of-service for maintenance is lower at shutdown than during power operation. However, this may not be valid for all components for all stages of plant shutdown. An assessment of the risk impacts during power operation and shutdown stages can provide useful insights. In comparing the risk impacts during these two periods, it should be kept in mind that the uncertainties associated with the corresponding PSA models are different; the uncertainties in the estimates for the shutdown periods can be considerably higher.

When PSA for both power operation and shutdown periods are available, then the risk impact of maintenance can be used in judging when preventive maintenance should be scheduled or avoided. Consider the maintenance for a single safety-system component. We now include P for power operation and POSn for plant operational state n during shutdown in our notation to distinguish among different times during plant operation.

The following measures are to be calculated:

$R_1(P)$ = CDF at power when the component is taken down for maintenance, calculated using the PSA model for power operation.

$R_1(POSn)$ = CDF in a given plant operational state (POS) during shutdown when the component is taken down for maintenance, calculated using the Shutdown PSA Model.

$R_1(POSn)$ may involve several separate calculations depending on the POSs defined in the shutdown PSA and the times when the maintenance can be carried out.

In principle, to minimize the risk impact of a maintenance, it can be carried out when the risk of taking the component out-of-service is the lowest. However, the scheduling PM involves different situations, requiring different considerations in comparing the alternatives of scheduling at power versus shutdown. Two different situations are:

a) routine scheduling of PM at a fixed frequency: in such a schedule, the components' PM schedules are clearly defined and are carried out irrespective of their performance or of the conditions, e.g., changing a filter in a component every six months.

b) PM needed when a degraded condition is detected for a component: in such scheduling, a PM need is defined when, based on test or inspection of the component, it is judged that PM is needed. Otherwise, the component may experience a failure soon, implying that the condition of the component is degraded. For example, changing a filter is recommended when it is judged that the filter is sufficiently clogged and may cause a component to fail.

A risk comparison for these two situations are discussed below.

For choosing an appropriate time (shutdown or power operation) for a fixed frequency PM, the conditional CDFs during these times can be directly compared, i.e., if

$$R_1(POSr) = \text{Min}\ \{R_1(P), R_1(POS1),\ldots,R_1(POSn)\} \quad (4.3)$$

then POSr is the preferred time for scheduling the PM.

When PM needs to be performed frequently, e.g., more than once a year, then the risk contribution due to the PM can be assessed as defined in Section A above. In that case, there may be no choice to scheduling the PM at power and effort should be focussed on controlling the risk contributions.

In the other situation, e.g., when a component is degraded, a decision must to be made between shutting down a plant or staying at power to carry out the PM required. If the risk of doing the maintenance at power is judged small, then the PM can be scheduled during power operation without further analyses. If a shutdown is decided, then the risk due to the PM, r_{PM} (SD), consists of two parts:

= (risk due to transition from power operation to shutdown) +
(risk from the component unavailability for the duration of the PM in the preferred shutdown POS)

For example, assuming that the preferred POS is POS4, the risk incurred to perform the maintenance by shutting the plant down is given by:

$$r_{PM}(SD) = R_0(POS1) \cdot t_1 + R_0(POS2) \cdot t_2 + R_0(POS3) \cdot t_3 + R_1(POS4) \cdot d_{PM} \quad (4.4)$$

where

$R_0(POSn)$ = CDF when transmitting through POSn
t_k = time in POSk
d_{PM} = PM duration

$R_1(POS4)$ = conditional CDF at POS4 when the component is down for maintenance.

On the other hand, if the decision were made to perform the PM at power, then the risk incurred would be given by the single PM contribution defined in Section A, and the corresponding risk of power operation for the comparable period. Here, the focus is on evaluating the risk to be compared with the corresponding risk to be incurred if shutdown was decided.

$$r_{PM}(PO) = R_1(P) \cdot d_{PM} + R_0(P) \cdot (t_1 + t_2 + t_3) \quad (4.5)$$

where

$r_{PM}(PO)$ = core-damage probability contribution for performing PM during power operation

$R_0(P)$ = CDF at power, when the component is not down for maintenance

$R_0(P) \cdot (t_1 + t_2 + t_3)$ = core-damage probability for the period $(t_1 + t_2 + t_3)$ when the component is not down for maintenance.

A comparison of $r_{PM}(PO)$ and $r_{PM}(SD)$ provides useful insights for carrying out the PM at power or for shutting the plant down to perform the PM.

4.4 Example Applications

In this section, we present three examples explaining the types of analyses discussed above.

4.4.1 Risk Impact for a Single Component

Consider that plant personnel want to perform PM twice a year on the turbine-driven pump (TDP) of the reactor core isolation cooling (RCIC) system during power operation. Assume that each PM takes 3 days, and the component is unavailable for this duration. To evaluate the risk impact of this PM plan for the component, the following PSA-based measures are to be calculated using the PSA.

Base-Case PSA Average CDF = 2×10^{-6}/yr.
CDF when RCIC-TDP is down for PM (R_1) = 2.5×10^{-5}/yr.
CDF when RCIC-TDP maintenance unavailability is zero (R_0) = 1.8×10^{-6}/yr.

The single PM risk contribution can be calculated as:

$$r_{PM} = (2.5 \times 10^{-5} - 1.8 \times 10^{-6})/\text{yr.} \cdot (3/365)\text{yr.}$$
$$= 1.9 \times 10^{-7}$$

The yearly PM contribution for the pump is calculated as:

$$R_{PM} = 2 \cdot (1.9 \times 10^{-7})$$
$$= 3.8 \times 10^{-7}$$

Here, the single and the yearly PM contributions are calculated using R_1 and R_0, but the estimated values would have been comparable if the base-case CDF was used instead of R_0. This is because R_1 is significantly larger than the base case CDF, which is comparable to R_0. In such cases, the base-case CDF can be used and an additional CDF calculation avoided.

The new average CDF of the plant, including this planned PM, can be estimated as the sum of the base-case CDF and the yearly PM contribution, i.e.,

$$= 2 \times 10^{-6} + 3.8 \times 10^{-7}$$
$$= 2.4 \times 10^{-6}/\text{yr.}$$

In other words, the changed CDF when the planned PM for the pump, in effect, will be 2.4×10^{-6}/yr.

4.4.2 Risk Impact of Maintenance Schedules During Power Operation

Many nuclear plants follow a fixed-frequency maintenance schedule where multiple equipment may be taken out-of-service at the same time. As mentioned earlier, the risk impact, i.e., the increase in CDF, can be particularly sensitive to this situation, even though the CDF impact of taking out each equipment separately is small. In planning this schedule, the intent is to avoid simultaneous outages of multiple components that can cause a large increase in the CDF.

An example analysis of a 12-week rolling maintenance schedule is shown in Table 4.2. Here, care is taken to avoid taking down redundant equipment during the same week, i.e., the maintenances of division-A and division-B batteries are performed during different weeks. Still, during certain weeks, multiple risk-significant equipment may be taken out-of-service simultaneously. For example,

Table 4.2 Example of a Rolling Maintenance Schedule

Week 1	Div. 1	Week 7	Div. 3
	Battery & DC Distribution (A)†		Condensate Booster (A)
	EDG (A)		Condensate (A)*
	Low Pressure Core Spray		Plant Service Air (A)
	EDG Room Ventilation (A)		
	Switchgear Heat Removal (A)*		
		Week 8	Non-Div.
			Fire Water (A)
Week 2	Div. 2		Instrument Air
	Battery & DC Distribution (B)		Plant Service Water (B)
	EDG (B)		
	Residual Heat Removal (C)		
	DG Room Ventilation (B)	Week 9	Div. 1
	Switchgear Heat Removal (B)*		Component Cooling (A)
			Condensate Booster (A)*
			Condensate (A)*
Week 3	Div. 3		RHR (A)
	Battery & DC Distribution (C)		Shutdown SW (A)
	EDG (C)		
	High Pressure Core Spray		
	EDG Room Ventilation (C)	Week 10	Div. 2
	Switchgear Heat Removal (C)*		Condensate Booster (B)*
	Plant Service Water (C)		Condensate (B)*
			Control Rod Drive (B)
			Shutdown SW (B)
Week 4	Non-Div.		Auxiliary Bldg HVAC (A)
	Control Rod (A)		Plant Service Water (A)
	Standby Liquid Control (B)		
		Week 11	Div. 3
Week 5	Div. 1		Shutdown Service Water (3)
	Condensate Booster (C)*		Auxiliary Bldg HVAC (B)
	Component Cooling (C)		
	Condensate (C)*		
	Standby Liquid Control (A)	Week 12	Non-Div.
	Containment Building HVAC		Fire Water (B)
			RCIC
			Supply Pool Makeup
Week 6	Div. 2		
	Component Cooling (B)		
	Residual Heat Removal (B)		

†A,B,C, respectively signify components in Division A,B,C.
*Not modeled in the PSA used.

during the first and second week, batteries in one division, one EDG, and additional equipment are maintained. As is done in this schedule, when a component of the support system, e.g., service water pump for the emergency diesel generator (EDG), and the component being supported, i.e., in this case, the EDG, are maintained together, then the CDF impact is minimized.

Figure 4.1 shows the CDF risk profile of this maintenance schedule, calculated incorporating the simultaneous outages of multiple components, as defined in the schedule. This figure conservatively assumes the same CDF level for the entire week, implying that the components scheduled for maintenance are unavailable for the entire week. This is a bounding assumption, because typically, maintenances or inspections are completed much faster, whereby the high risk level will remain only for a portion of the week.

To demonstrate how simultaneous maintenance of redundant components can significantly affect the CDF, we present the risk profile where the schedule is slightly altered. Here, the maintenance of the ventilation fan for EDG C is performed in the 2nd week, along with the maintenance of EDG B and its ventilation fan. Figure 4.2 shows an order of magnitude jump in CDF during the 2nd week. This type of analysis will assure that such peaks in CDF are avoided.

In addition to controlling any CDF peaks, the increase in the average CDF of the plant can be determined. Here, the average CDF is obtained by averaging the CDF over 12 weeks, which is repeated every 12 weeks. For Figure 4.1, the upper value of the average CDF due to the maintenance schedule is

$$= \frac{\sum_{i=1}^{12} R_1(P,WKi)}{12}$$

$$= 1.7 \times 10^{-5}/\text{yr.}$$

In the bounding case, the average plant CDF due to the PM schedule will increase by about an order of magnitude.

To control this CDF impact, three alternatives can be assessed:

a) rearrange the distribution of PM for components among the weeks,

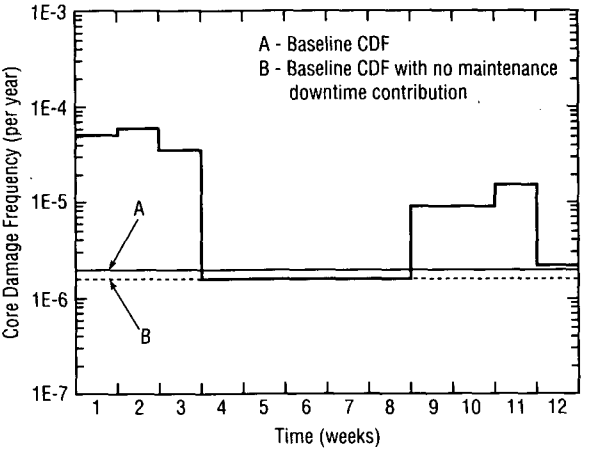

Figure 4.1 Core-damage frequency levels in an example of a rolling maintenance schedule. (Note: multiple components are assumed to remain unavailable for the entire week: a bounding scenario)

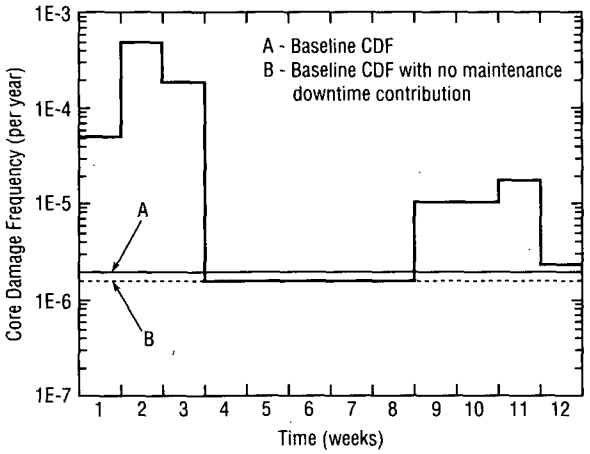

Figure 4.2 Change in core-damage frequency level due to an undesirable change in the example of a rolling maintenance schedule

b) when feasible, without increasing maintenance errors, consider completing the maintenance faster where the CDF impact is large,

c) consider reducing the frequency of maintenance, e.g., reduce EDG maintenance from once every 12 weeks to once every 24 weeks, if such changes will not reduce the component's reliability.

Alternative b) and c) already may take place in a normal use of rolling maintenance schedule; however, based on this type of analysis, the need for these changes can be identified and assured.

Considering that the best possible distribution of components was made across the weeks to control the risk peaks, the risk profile can be used to identify specific alternatives. One alternative is to assure that during the first three weeks when the CDF peaks are highest, the maintenances are completed within two days: this will reduce the average CDF to 7.8×10^{-6}/yr., approximately a factor of 2 reduction. In another alternative, the frequency of the components maintained during the first three weeks is reduced from once every 12 weeks to once every 24 weeks, then the average CDF falls to 5×10^{-6}/yr., about a factor of 3 reduction.

4.4.3 Scheduling Maintenance During Power Operation Versus Shutdown

An example analysis of the risk impact of emergency diesel generator (EDG) maintenance during power operation and shutdown is discussed to decide on a strategy for scheduling routine maintenances. This type of analysis requires both full power and shutdown PSAs.

For full-power operation with an EDG in maintenance, a single conditional CDF is calculated using the corresponding full-power PSA. The shutdown periods are divided into several plant operational states (POSs), each represented by the respective PSA model which is used to calculate the CDF. The pressurized water reactor (PWR) low power and shutdown (LP&SD) model defines 15 POSs, using the Surry plant as an example, whereas the boiling water reactor (BWR) model defines 7 POSs, using the Grand Gulf plant as an example. The impact of EDG maintenance differs from one POS to another. Accordingly, the effect of EDG maintenance on CDF is calculated for each POSs using the respective CDF model.

We compare the conditional CDF, given EDG is in maintenance between power operation and shutdown periods, and among the shutdown POSs to identify the periods when the risk impact of maintenance is minimal.

Analysis for a PWR

The risk-impact of EDG maintenance during power operation and shutdown periods was assessed using the corresponding PSA models for the Surry plant, a PWR (Samanta et al., NUREG/CR-5994, 1994). The emergency power system, as modeled in the PSA, takes credit for the third EDG that can be cross-connected.

The risk impact of EDG maintenance (in terms of conditional CDF) was evaluated for full-power operation, and also, for different POSs 4 through 12, during a shutdown (Figure 4.3). These POSs were chosen because EDGs are maintained during them. The base-line CDF for each of the POSs also is shown. The risk of EDG maintenance during early stages of cold shutdown (POS 4, 5), and midloop operations (POS 6, 10) is relatively high; it is low during POSs 8 and 12, i.e., during refueling, and when the reactor coolant system (RCS) is filled after refueling.

Table 4.3 compares the risk of EDG maintenance during full-power operation versus different shutdown POSs. Because of the earlier stage of development of the shutdown PSA and the different uncertainties involved, the conditional CDFs calculated with full-power PSA and shutdown PSA are not directly compared. Accordingly, the CDFs are categorized as high (H), medium (M), and low (L). The results show that the CDF impact of EDG maintenances during periods of shutdown can be comparable to that during power operation.

Analysis for a BWR

The conditional CDF of an EDG out-of-service due to maintenance was assessed for full power operation and during various stages of plant shutdown. The low power and shutdown PSA model for the Grand Gulf plant, a BWR, is more detailed, and therefore, the conditional CDF of EDG maintenance during power operation versus plant shutdown was compared numerically to obtain insights into risk (Staple et al., NUREG/CR-6166, 1994).

Both the CDF level and the increase in CDF for EDG maintenance were calculated for full-power operation and for each of the seven plant operating states (POSs) defined in the low-power and shutdown (LP&SD) PSA (Figure 4.4), with EDG in maintenance. Here, the time in the x-axis is proportionally divided between power operation and shutdown operation, considering the amount of time spent in each of those two types of operation. Then, the shutdown period is, similarly, proportionally divided among different shutdown POSs. The CDF level for EDG maintenance is the smallest during refueling (POSs 6 and 7), but is significantly higher when the plant is in cold shutdown, when the reactor-core isolation cooling (RCIC) system, i.e., the steam-driven source of water, is assumed to be unavailable.

POS DEFINITIONS

POS 1 - Low Power Operation and Reactor Shutdown
POS 2 - Cooldown with SGs to 345°F
POS 3 - Cooldown with RHR to 200°F
POS 4 - Cooldown with RHR to 140°F
POS 5 - Draining the RCS to Midloop
POS 6 - Midloop Operation
POS 7 - Fill for Refueling
POS 8 - Refueling
POS 9 - Draining RCS to Midloop after Refueling
POS 10 - Midloop Operation after Refueling
POS 11 - Refill RCS Completely
POS 12 - RCS Heatup Solid and Draw Bubble

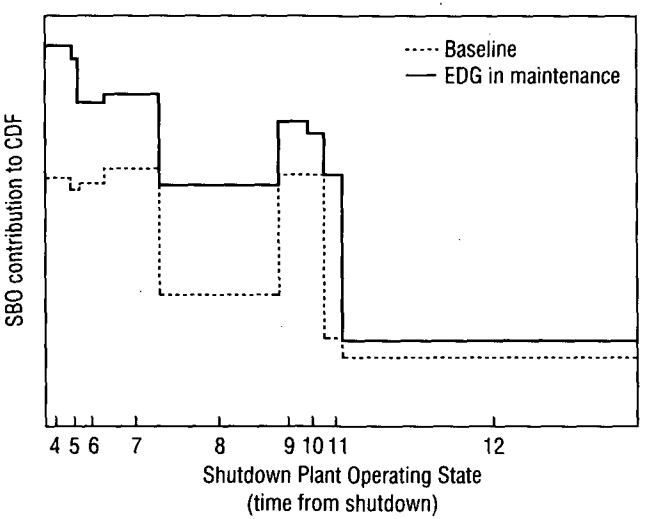

Figure 4.3 Change in CDF (due to SBO sequences) for taking an EDG out-of-service during different shutdown plant operational states (Surry 1 nuclear plant, PWR)

Table 4.3 Relative CDF Impact of EDG Out-of-Service for Maintenance (Surry 1 Nuclear Plant, PWR)

Plant Operational State	Average Duration (hrs.)[1]	ΔCDF [1,2] (EDG in Maintenance)
POS O (Full Power)	-	M
POS 4 (Cooldown with RHR to 140°F)	154	H
POS 5 (Draining the RCS to Midloop)	46	H
POS 6 (Midloop Operation)	183	H
POS 7 (Fill for Refueling)	374	H
POS 8 (Refueling)	810	M to L
POS 9 (Draining RCS to Midloop after Refueling)	206	M
POS 10 (Midloop Operation after Refueling	107	M
POS 11 (Refill RCS Completely)	118	M
POS 12 (RCS Heatup Solid and Draw Bubble)	1840	L

1: H: High, M: Medium, L: Low
2: ΔCDF is the increase in CDF due to EDG being out of service for maintenance from the baseline CDF in the POS

The CDF level during low power and hot shutdown modes (POSs 2, 3, and 4) is comparable to that during full-power operation. Similar to the PWR, the CDF level for EDG maintenance is substantially reduced during refueling, and is considerably higher during certain periods of shutdown.

4.5 Insights for Scheduling Maintenances

The benefit of scheduling PM during power operation primarily is, to assure the reliable operation of the equipment, and, at the same time, reduce the burden of maintenance during shutdown. Such scheduling is partly necessitated by the longer fuel cycles, and also due to the desire to reduce the outage duration of a shutdown.

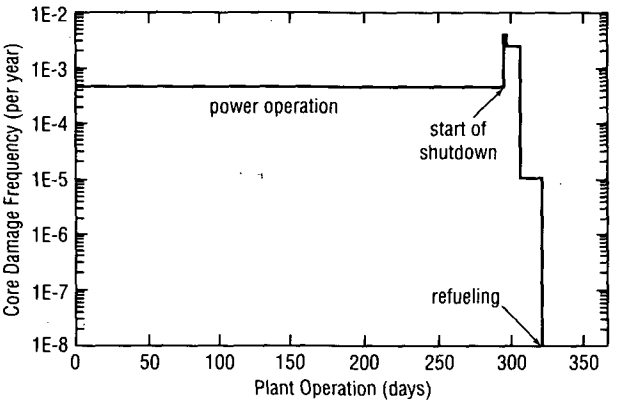

Figure 4.4 Change in CDF for taking an EDG out-of-service during different modes of plant operation (Grand Gulf nuclear station, BWR).

Scheduling a short PM during power operation may involve a small risk, but repeated use of LCOs for PM can significantly increase the risk due to increased component unavailability. Also, it can mask component failures being recorded. By scheduling PMs just before Technical Specification Surveillance testing, failures may be corrected; the test may not detect all failures in the standby period, thus yielding optimistic reliability data. Performing PM usually requires disassembling the equipment. Therefore, the equipment cannot be returned to service at short notice if a need arises.

The primary motivation for scheduling all PM during shutdown is to reduce the risk impact from the associated downtimes. When the risk impact of maintenance downtime during the early stages of reactor shutdown is comparable with the risk impact during power operation, a low impact can be achieved by scheduling short-duration maintenance during power operation. Similarly, a long-duration maintenance may be scheduled during extended periods of reactor shutdown (e.g., refueling) when the decay heat is low and the water level is high. Also, we expect that carrying out certain maintenances at short intervals can improve the reliability of some equipment; this leads to a consideration of a maintenance program distributed between power operation and shutdown periods.

Table 4.4 presents general insights on scheduling PMs. PMs are divided into three categories depending on the frequency at which the PM is needed since it has bearing on scheduling the activity:

1. Scheduled PMs that need to be performed at intervals of less than 18 months,

2. Scheduled PMs that need to be performed at intervals of 18 months or more,

3. Condition-directed PMs, based on test results, needed to correct degradations of equipment which may lead to failures.

Table 4.4 Scheduling Maintenances

Type of Maintenance and Frequency	Maintenance Duration	Problems to be Considered if Maintenance is Scheduled		Insights
		During Power Operation	During Shutdown	
1. Scheduled PMs Fixed frequency PMs that need to be performed between a refueling outage (less than 18 months)	a) $\leq$AOT	• repeated use may impose unacceptable risk • repeated use before testing masks failure, unreliable data on components' failure	• unreliable component during power operation • plant outage duration can be lengthened	• may schedule during power operation • optimize PM during power operation and shutdown • monitor unavailability due to PM (if PM duration or frequency during power operation is excessive, find and correct causes); or set limit for PM duration and frequency during power operation
	b) Longer than AOT	• risk impact may be unacceptable	• unreliable component during power operation	• may be performed during power operation with extended AOT to assure reliability • could involve exemption to AOT • avoid "running start" on maintenance

Table 4.4. Scheduling Maintenances (Cont'd.)

Type of Maintenance and Frequency	Maintenance Duration	Problems to be Considered if Maintenance is Scheduled		Insights
		During Power Operation	During Shutdown	
2. Scheduled PMs Fixed frequency PMs that need to be performed every 1½ to 2 yrs (or longer)	a) < AOT†	• none	• plant outage duration can be lengthened	• schedule during power operation or shutdown • optimize PM program between power operation and shutdown
	b) ~ AOT*	• uncertainty that PM can be completed and the component can be returned to service within an AOT. • repeated use of LCOs for such maintenance imposes unacceptable risk	• risk impact during certain shutdown periods may be significant	• schedule during shutdown • define allowable states during plant shutdown, e.g., avoid early stages of shutdown.
	c) Longer than AOT	• risk impact may be unacceptable • uncertainty that PM can be completed and the component can be returned to service	• risk impact during certain shutdown periods significant	• schedule during shutdown • define allowable plant configuration and state for such maintenance • allow sufficient time to complete maintenance uninterrupted

†< AOT means approximately one half of AOT or less, *~ AOT means durations from one half AOT to one AOT.

Table 4.4. Scheduling Maintenances (Cont'd.)

Type of Maintenance and Frequency	Maintenance Duration	Problems to be Considered if Maintenance is Scheduled		Insights
		During Power Operation	During Shutdown	
3. Condition - Directed PMs As needed to correct degradation of equipment (choices include scheduling maintenance during power operations, waiting until the next shutdown, or immediately proceeding to shutdown)	a) < AOT	• repeated use increases risk from downtimes	• unnecessary risk from shutting down • increased risk during power operation	• schedule during power operation • control or monitor frequency to avoid misuse
	b) ~ AOT	• uncertainty that PM can be completed and the component may be returned to service within an AOT	• larger relative risk to perform maintenance during critical phases of shutdown	• schedule during power operation • for scheduling during power operation, test of redundant component to assure availability, before start of PM, may be desirable
	c) Longer than AOT	• uncertainty that PM can be completed and the component can be returned to service	• increased risk of shutting down with unreliable equipment • long wait to perform maintenance if a preferable state in shutdown mode is to be chosen	• depends on a number of factors, e.g., severity of degradation, time from next scheduled outage, potential for common-cause failure • may involve changes to TS if scheduled during power operation, e.g., increased AOT, additional test requirements

5. SURVEILLANCE TEST INTERVAL (STI)

Basic Concepts

Surveillance Test Interval (STI): The surveillance requirements of Technical Specifications have a specified frequency in which the surveillance test must be performed. The STI is the associated interval at which the surveillance test is performed.

STI Risk Contribution: This is the risk contribution associated with the surveillance test, or the STI. The STI risk contribution mainly arises from the possibility that a component may fail between tests. By performing tests, we can limit the risk associated with the otherwise undetected failures, called test-limited risk. Other STI risk contributions are those caused by the test, e.g., test-caused transients.

Test-Limited Risk: The test-limited risk is the STI risk contribution that can be limited by the test, namely by detecting failures that may have occurred since the last test or the time when the equipment was last known to be operational.

Test-Caused Risk: Some tests may cause adverse effects, for example, due to errors in testing causing plant transients, or to wearout of the equipment. By extending the STI or reducing the number of tests, we generally can reduce their adverse effects. The STI risk contribution from these adverse effects is called test-caused risk.

Standby Time-Related Failures: The failures related to deterioration and events that occur over time are called standby time-related failure examples of which include corrosion, erosion, and wear.

Cyclic Demand-Related Failures: The failures related to the stresses which occur only at the instant of a demand are called cyclic demand-related failures. Examples of such failures include electrical and mechanical stresses occurring when the component is demanded (i.e., when the component is started).

Chapter Outline

List of Symbols

λ the time-related component failure rate per unit time

q the average component unavailability

Q_i, $i = 2,3,4$ the average unavailability of multiple components, i.e., two, three, or four components; the formulas are given as a function of test strategy

R_D the STI risk contribution which is limited by the test

ΔR the increase in risk level associated with the component being down

R_1 the core-damage frequency evaluated with the component assumed to be down

R_0 the core-damage frequency evaluated with the component assumed to be up

T the surveillance test interval

5.1 Current Practices and Issues

Surveillance tests are required to be periodically (e.g., monthly or quarterly) performed by Technical Specifications. The periodic test interval defined in the Technical Specifications is called the Surveillance Test Interval (STI).

The primary purpose of surveillance testing is to assure that the components of standby safety systems will be operable when they are needed in an accident. By testing these components, failures can be detected that may have occurred since the last test or the time when the equipment was last known to be operational.

However, the number of surveillance tests required by Technical Specifications is enormous, requiring the nuclear industry and the regulatory agency to spend substantial resources on planning, conducting, and verifying them. Some tests may even have an adverse impact on safety because of their undesirable effects (e.g., test errors causing plant transients, or wearout of the equipment due to testing).

In general, these undesirable effects will be reduced if the STI is increased, because then fewer tests will be conducted. By extending the STI, we also can obtain the additional benefit of reducing resources on testing. However, an important disadvantage here is that the fault-exposure time, i.e., the time during which the component will be subject to failures during standby (strictly speaking, standby time-related failures), will correspondingly increase as the STI increases.

This chapter addresses evaluation of STIs considering the STI risk contribution that arises from the failures that may occur between tests and are detected by the test; or in other words, the risk contribution that may be limited by defining an STI. The undesirable or adverse effects of testing and their risk contributions are discussed in the next chapter. For many risk-significant components, the adverse effects of testing has important implications in extending the STI and the methods presented in Chapter 6 should be considered. The method presented here is applicable to a large portion of surveillance testing whose adverse effects are negligible. We discuss how the STI for these tests can be systematically evaluated based on the STI risk contribution that arises from the failures occurring between tests and neglecting the adverse effects of testing.

5.2 Overview of the Risk Contributions Associated with an STI

The risk contribution associated with an STI, i.e., the STI risk contribution, arises mainly from the possibility that the component will fail between consecutive tests. The value of this STI risk contribution depends on the probability of the component failing within the STI. As the time increases from the last test, the

probability that the component is failed increases, and hence, this risk contribution increases with time from the last test. The probability of the component being failed drops essentially to zero after the test if it effectively detects and corrects failures. The figure below illustrates the sawtooth pattern reflecting the failed probability behavior. So, by performing the test, we can limit the risk associated with the otherwise undetected failures. For this reason, we call this STI risk contribution test-limited risk. (It is sometimes called test-detected risk since it measures the risk from the detection of failures between tests.)

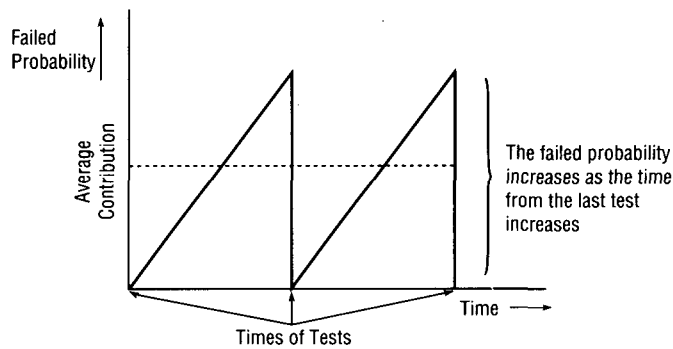

Figure 5.1 The STI risk contribution associated with the probability of the component failing between tests

Other STI risk contributions besides the failed probability contribution can be associated with the test if it is inefficient; these other contributions include one arising from a test-caused failure in which the test itself is instrumental in causing the component to fail. Other adverse effects include those associated with wearout of the component, trips, and failures of other components caused by the tests.

Since we focus on surveillance tests with negligible adverse effects, the STI risk contribution of interest here is that associated with the component failing between tests; in other words, we will focus on the risk contribution that can be limited by the test by detecting potential failures between consecutive tests, i.e., the test-limited risk.

The surveillance tests usually are assumed to be periodic, carried out at equal intervals. The average of the time-dependent risk contribution between tests usually is taken to be the STI risk contribution which is evaluated.

The specific risk measure in calculating the STI risk contribution needs to be defined. For components in safety systems whose function is to prevent core damage, the most applicable measure is the core-damage frequency. Surrogate risk measures also can be used, such as a safety-function unavailability. For components in safety systems whose function is to mitigate the consequence of an accident, the applicable risk measure is the frequency of severe consequence accidents, or the associated consequence-related risk. Surrogate measures also can be used, in which case all the component's relevant contributions should be included in the surrogate measures.

5.2.1 Overview of the Risk Contributions Associated with Several STIs

When several components, whose STIs are being evaluated, do not interact, i.e. are in different minimal cutsets, then the overall STI risk contribution is the sum of their individual contributions. For example, when several components in a system train are tested by a given test, then the overall STI risk contribution associated with the test is the sum of the individual contributions. When two or more components do interact, i.e. are in the same minimal cutset, then the overall STI risk contribution involves an appropriate multiplication of the individual contributions. The actual calculation of the STI risk contribution is covered subsequently.

5.2.2 Risk Importances of STIs and Risk Contributions of STIs

The risk importance of an STI is defined to be the associated STI risk contribution. The risk importance of a surveillance test is defined to be the sum of associated risk contributions if several components are tested by a given test. The risk importances of a set of STIs can be used to prioritize the STIs for various applications.

5.2.3 Basic Formula for the Component Unavailability

Assuming a constant, standby time-related failure rate, the average component unavailability, q, is determined from the formula

$$q = \frac{\int_0^T (T-t)e^{-\lambda t}\lambda\, dt}{T} \qquad (5.1)$$

$$= 1 - \frac{1}{\lambda T}(1 - e^{-\lambda T})$$

where

$T =$ the surveillance test interval for the component

and

$\lambda =$ the time-related component failure rate per unit time.

If $\lambda T << 1$, then the above formula for q can be approximated by the formula,

$$q \cong \frac{1}{2}\lambda T, \tag{5.2}$$

which is the one most often used in PSAs. We note that λ is the time-related component failure rate associated with failures occurring between the tests. However, the failures detected for a component (by a surveillance test or an actual demand during plant operation) may not all be time-related. Some of the failures may be related to the stresses imposed on the component by demanding or starting the component (called cyclic demand-related failures). The appropriate failure rate to use will be addressed further in a subsequent section.

5.2.4 Basic Formula for the Test-Limited Risk for a Tested Component

As discussed earlier, we will focus on the test-limited risk here.

Let

R_D = the STI risk contribution which is detected by the test

= the test-limited risk contribution

ΔR = the increase in risk level associated with the component being down

= $R_1 - R_0$

where

R_1 = the core-damage frequency evaluated with the component assumed to be down (i.e., with the component unavailability set to "True")

R_0 = the core-damage frequency evaluated with the component assumed to be up (i.e., with the component unavailability set to "False")

Then, the test-limited risk can be determined by the following formula (Samanta et al., NUREG/CR-5200, 1988; Vesely, NUREG/CR-3541, 1983):

$$R_D = q\Delta R$$

$$= \frac{1}{2}\lambda T \cdot (R_1 - R_0) \tag{5.3}$$

where q represents the average probability of component failure associated with the component failing between tests, discussed earlier. The expression (R_1-R_0), or ΔR, is known in reliability literature as the risk importance or Birnbaum importance, which indicates the sensitivity of the core-damage frequency to the basic event associated with the tested component.

Surveillance tests may have additional benefits which are not explicitly quantified:

- They may detect potential failure mechanisms at an early stage, requiring repair, and thus removing, or significantly decreasing, the possibility of failure. Potential common-cause failures also may be detected.

- In much standby mechanical equipment, testing may help to prevent corrosion or the accumulation of impurities, and lubricate various piece-parts, so contributing to their reliability.

However, these aspects are indirectly included through component failure rate, λ, which reflects these beneficial influences of surveillance tests.

Thus, the test-limited risk associated with the probability of finding the component failed is the average probability of component failure q times the increase in risk level due to the failure ΔR. The increase in risk level ΔR is similar to that evaluated for an AOT risk contribution where the component going down is due to

its failing between tests (see, Section 3.2.6 and Appendix B). The test-limited risk as given above is the standard test contribution used in a PSA; however, specific details of applying the formula become important when test-limited risks are the focus. The above formulas also give the test-limited risk for a given component when multiple components are included in the test; however, if some components interact (are in the same minimal cutset), then the risk importance obtained from the PSA will reflect the unavailabilities of the other components.

5.2.5 Basic Formula for the Test-Limited Risk When Several Noninteracting Components Are Tested by a Given Test

When several noninteracting components (i.e., in different minimal cut sets) are tested by a test then let,

ΔR_i = the increase in risk level associated with the ith component going down

q_i = the average unavailability for the ith component associated with a failure occurring between tests

and

R_D = the test-limited risk which is detected by the test.

Then, the formula for R_D is given by

$$R_D = \sum_{i=1}^{n} q_i \Delta R_i$$

$$= \sum_{i=1}^{n} \frac{1}{2} \lambda_i T \Delta R_i \qquad (5.4)$$

where n represents the number of components tested.

We note that, for components in the same train, the increase in risk ΔR_i will be the same. When several interacting components are tested by a given test (which is unusual), then using the minimal cutset contributions to determine the test-limited risk is the most direct approach. This is discussed below.

5.2.6 Using the PSA to Determine the Test-Limited Risk Contribution

The PSA can be used to calculate the increase in the risk level ΔR and to obtain the component unavailability, q, the contributing factors in calculating the test-limited risk contribution. The considerations involved in calculating R_1 and R_0 to obtain ΔR are discussed in Section 3.2.6 and in Appendix B.

When the effect of change in STI for one or more components are being evaluated, then the PSA can be directly used to calculate the change in the risk measure, e.g., in the CDF. The calculation of PSA results where changed STIs are included incorporates interactions among the STIs. The differences between the results (i.e., CDF when the STIs are changed from the baseline CDF) provides the test-limited risk contribution for changing the STIs.

In such a calculation, the contributions of common-cause failures need to be appropriately modified. The common failure terms modeled as a function of the test interval should be modified to reflect the new STI. Typically, common-cause failures are modeled using a β-factor or Multiple Greek Letter model (Mosleh eta al., NUREG/CR-4780, 1988) where the common-cause failure of multiple component is a function of the STI. When changing STIs, care should be taken to change this term within the common-cause contribution. The common cause of failing multiple components resulting from human error following a test is not a function of the STI, but may be affected by the test strategy used.

When different test strategies are being evaluated, this human error term needs to be evaluated. Specific assumptions that were used in quantifying the human error common-cause term should be identified and checked if they apply for the test strategy being analyzed. For example, if the term was developed assuming a sequential test strategy, but a staggered test strategy is being analyzed, then the term needs to be modified to reflect this change. The failure probability from human error common-cause for a staggered test strategy is expected to be significantly lower than that for the sequential test strategy.

5.2.7 Uncertainty Considerations in Evaluating Test-Limited Risks

The uncertainties associated with evaluating test-limited risks involve the uncertainties associated with evaluating the component's unavailability, q, and the risk increase ΔR. The PSA uncertainties associated with the minimal cutsets containing the unavailability, q, can be used to extract the uncertainties associated with STI risk evaluations.

5.2.8 Using Minimal Cutsets to Calculate Test-Limited Risks

The test-limited risk for a component or set of components also can be determined by identifying those minimal cutsets which contain one or more of the STI contributions. The sum of the relevant minimal cutset contributions then is equal to the test-limited risk. To evaluate changes in the test-limited risks for changes in the STIs, the difference between the minimal cutset contributions with, and without, the STI changes will be the difference between the test-limited risks. In using the minimal cutsets, one should assure that the STI contributions are all included in the set of minimal cutsets used. Even though use of the minimal cutsets gives the same results, the above basic formulas for the test-limited risks are useful, since they show the basic contributing factors to the STI risk.

5.2.9 Specific Considerations for the Evaluation of Multiple Test-Limited Risks

When multiple STIs are modified or are defined, then the total test-limited risk from the multiple STI changes or definitions needs to be properly evaluated. Instead of using the PSA to evaluate all the modifications at a given run, the individual test-limited risks can be evaluated one at a time, provided that the updated STIs are used for the other relevant components. An iterative procedure then can be employed in which individual STIs are successively updated, using the above formulas for the individual component STI risk contributors. These one-at-a-time evaluations or iterative evaluations are useful if acceptable criteria on test-limited risks are defined, and the STIs are to be selected to satisfy the risk criteria.

5.2.10 Considerations in Separating the Component Failure Rate into Time-Related and Demand-Related Contributions

Since the test-limited risk is associated with a failure occurring between tests, the failure rate which should be used in calculating the test-limited risk should be the standby time-related failure rate, which is associated with causes that can occur while the component is in standby between tests. The time-related failure rate is expressed in units of per time, such as per hour. The total failure probability of a component sometimes is broken down into a time-related contribution plus a cyclic demand-related contribution. The latter is the probability contribution associated with failures which are caused by demanding, starting, or cycling the component. Decomposing the failure probability into a time-related and cyclic demand-related contribution results in a lower test-limited risk because only part of the component's failure rate is treated as time-related. However, treating only part of the failure rate as being time-related when this is not the case underestimates the test-limited risk, and this breakdown of the failure rate needs to be justified through data analysis or engineering analyses, if it is used.

Also, sometimes only the failure probability, i.e., the component unavailability, q, may be provided without a failure rate provided. In such a case, the effect of change in test interval cannot be evaluated unless the component test interval, T, is used to convert the unavailability, q, in terms of λ and T. When the breakdown between time-related and cyclic demand-related contribution is unknown, all failures can be assumed to be time-related to obtain the maximum test-limited risk contribution.

5.2.11 Considerations in Accounting for Test Scheduling in Computing the Test-Limited Risk

If two or more tested components are in different trains in the same system, or more generally, if the tested components are in the same minimal cutset, then the total test-limited risk is affected by the relative scheduling of the tests. The standard PSA quantification of the test-limited risk assumes that the relative test times of components follow no specific schedule and are randomly placed with regard to one another. By staggering the test times of components in different trains or in the same minimal cutset, then the test-limited risk will be reduced for the same STIs as compared to the independent PSA assumption. Conversely, if the tests are carried out sequentially, then the test-limited risk will be increased compared to the independent PSA assumption. Also, the human error common cause terms following a test may be affected by other relative scheduling of the tests (or the test strategy used). Those terms may need to be modified to reflect a change in scheduling (see Section 5.2.6).

When test-limited risks are calculated for two or more components which appear in the same minimal cutset, if the PSA is used to determine the test-limited risk, then one needs to check that the tests are not actually carried out sequentially. The test-limited risk can be adjusted to account for scheduling if specific scheduling is incorporated into the procedures. Formulas for the adjustment factors can be determined from standard reliability formulas for sequential, staggered, and independent testing. These formulas, for component unavailabilities for combinations of up to four components, are given in the next section.

5.2.12 Formulas for the Product of Component Unavailabilities Accounting for Test Scheduling

Let

λ = the component time-related failure rate

and

T = the test interval,

then formulas are given below (Nuclear Power Reactor Safety, E. Lewis, 1977) for the unavailability contribution for a combination of similar components in the same minimal cutset, with the first-order exponential approximation usually used in a PSA. The test scheduling factor can be taken as the ratio of the applicable unavailability divided by the unavailability using the PSA independence assumption.

Two-Component Unavailability Contribution Q_2

$$Q_2 = \frac{1}{4}\lambda^2 T^2 \qquad \text{Independent Tests} \qquad (5.5)$$

$$Q_2 = \frac{1}{3}\lambda^2 T^2 \qquad \text{Sequential Testing} \qquad (5.6)$$

$$Q_2 = \frac{5}{24}\lambda^2 T^2 \qquad \text{Staggered Testing} \qquad (5.7)$$

Three-Component Unavailability Contribution Q_3

$$Q_3 = \frac{1}{8}\lambda^3 T^3 \qquad \text{Independent Tests} \qquad (5.8)$$

$$Q_3 = \frac{1}{4}\lambda^3 T^3 \qquad \text{Sequential Testing} \qquad (5.9)$$

$$Q_3 = \frac{1}{12}\lambda^3 T^3 \qquad \text{Staggered Testing} \qquad (5.10)$$

Four-Component Unavailability Contribution Q_4

$$Q_4 = \frac{1}{16}\lambda^4 T^4 \qquad \text{Independent Tests} \qquad (5.11)$$

$$Q_4 = \frac{1}{5}\lambda^4 T^4 \qquad \text{Sequential Testing} \qquad (5.12)$$

$$Q_4 = \frac{251}{7680}\lambda^4 T^4 \qquad \text{Staggered Testing} \qquad (5.13)$$

5.3 Evaluating STI Risks

5.3.1 The Steps Involved in a Systematic STI Evaluation

A systematic process should be carried out when evaluating the risks associated with either existing or proposed STIs; the steps below represent such a systematic process. To carry out each step, the appropriate analysis described in the earlier methodology sections needs to be conducted. Each step involved is described briefly in the following pages.

Steps Involved in Systematic STI Risk Evaluations

1. Identify the STIs to be evaluated.

2. Determine the risk contribution associated with the STIs.

3. Determine the risk-based STIs which satisfy given criteria.

4. Check the STI evaluations by substituting the risk-based STIs and calculating the associated risk.

5. Perform sensitivity and uncertainty evaluations to address issues and uncertainties associated with the STI evaluations.

6. Document the evaluations and prepare a summary table of the results.

Step 1. Identify the STIs to be Evaluated

The STIs which are candidates for risk-based evaluations should be identified. All the STIs in a given system or in a given set can be candidates for possible modification. Alternatively, specific STIs can be selected, based on certain deterministic criteria; for instance, those tests that are considered as deserving detailed quantitative risk analyses.

Step 2. Determine the Risk Contribution Associated with the STIs

If minimal cutset contributions are used directly to determine the test-limited risk, then the minimal cutsets should be identified which contain one or more of the tested component unavailabilities, q. The sum of the minimal cutset contributions then is the STI risk contribution or the test-limited risk R_D.

It also is useful to determine the contributing factors to the STI risk. The test-limited risk, R_D, associated with failures occurring between successive tests is given by

$$R_D = q\Delta R$$

where

q = the component unavailability

and

ΔR = the risk increase associated with the component going down.

The component unavailability, q, is given by the formula

$$q = 1 - \frac{1}{\lambda T}\left(1 - e^{-\lambda T}\right)$$

$$\cong \frac{1}{2}\lambda T \text{ for } \lambda T << 1$$

where

λ = the time-related component failure rate (per unit time)

and

T = the test interval.

If minimal cutset contributions have been summed to obtain R_D for a given component, then ΔR is simply R_D divided by the tested unavailability q. Since the failure of the component generally is latent, reconfigurations and modified testing when the component is down should not be incorporated when evaluating ΔR. Common-cause failure contributions associated with the component failure should be incorporated.

If only a specific fraction of failures is assumed to be time-related in estimating λ, then the basis for this assumption should be given, and sensitivity studies on the effects of varying the fraction also should be carried out.

Step 3. Determine the Risk-Based STIs which Satisfy Given Criteria

Risk-based STIs can be determined by controlling the individual STI contributions to risk to be within given values. The sum of the test-limited risks also can be controlled to be within acceptable values, although this control can be carried out in Step 4 when the risk contributions from all the risk-based STIs are checked. For risk-based test intervals selected to control individual test-limited risks, the intervals T can be selected to be less than a certain value; e.g., $R_D \leq S$, where S is a relative or absolute criterion. The formula for R_D can be substituted to determine the allowed risk-based STI. Sensitivity studies can be made to assess the effects on the risk-based STI by using different alternatives to calculate R_D.

Step 4. Check the STI Evaluations by Substituting the Risk-Based STIs and Calculating the Associated Risk

The cumulative risk contribution from the risk-based STIs and the interactions among the test-limited risks can be checked by recalculating the PSA results with the risk-based STIs incorporated. The interactions among the STIs occur when two or more risk-based STI contributions occur in the same minimal cutset. In this case, the risk contributions are multiplied instead of being added. If the re-evaluated PSA results are too high because of these effects, then the causes can be identified and modified risk-based STIs defined.

Step 5. Perform Sensitivity and Uncertainty Evaluations to Address Issues and Uncertainties Associated With the STI Evaluations

Because of the PSA uncertainties, there will be uncertainties in the test-limited risks R_D which are calculated. These, in turn, are due to the uncertainties in

the component unavailabilities, q, and the risk increases, ΔR, which are multiplied to give R_D. The uncertainties in q and ΔR can be determined from the PSA, or sensitivity studies can be undertaken. The uncertainty or sensitivity evaluation results need to be reported.

Step 6. Document the Evaluations and Prepare a Summary Table of the Results

The STI risk evaluations carried out in the previous steps should be fully documented with the specific data used and calculations carried out. The results obtained in each step should be clearly identified, and the results should be summarized as a table.

5.3.2 Data Needs for STI Evaluations

The data needs for STI evaluations are summarized below. These data are in addition to the information available as part of the PSA study. It must be emphasized that, if planned early, many of the data discussed below can be collected when collecting data for the PSA without many additional resources.

- A list of the components being tested; any component realigned from the safety position during a test; duration of the test; and the test frequency recommended by the manufacturer.

- The efficiency of the test, i.e. the failure modes detected by the test (in regard to components, support system interfaces, and so forth). Bounding assumptions can be made if obtaining detailed information is costly.

- Surveillances that have potential for negative effects, e.g., that may cause disturbances including the potential for introducing plant transients, or may cause unnecessary wear of the equipment. Preliminary evaluations can be used to identify if a detailed analysis should be performed (as presented in Chapter 6).

- The failures observed for a component at a surveillance test or otherwise, may need to be evaluated to determine whether the failure mechanism is cyclic demand-related or standby time-related. Separating failure data in to these categories may require detailed information or engineering judgment.

5.4 Examples of Evaluations of Test-Limited Risks

5.4.1 Introduction

Example evaluations of test-limited risks are given here. The risk contributions which are calculated are STI core-damage frequency (CDF) contributions; the examples are taken from NUREG/CR-5200 (P.K. Samanta et al., 1988). They are described here in terms of the methodology and calculations which were presented in the previous chapters. The methodology is similar to that in NUREG/CR-5200, with additional considerations and clarifications on their applications.

The next section presents an example of an evaluation of an test-limited risk for a case where several components are tested by the same test. Then, tables are shown of test-limited risks for given components and test intervals that were similarly calculated. This type of evaluation can be used to prioritize STI risks. Similar tables also can be constructed for proposed STIs. Sensitivity studies or uncertainty studies also would be given for any assumptions or contributions which could affect the conclusions. The last section considers risk strategies involving STIs.

5.4.2 Calculation of the Test-Limited Risks

As an example of an test-limited risk evaluation, consider a surveillance test carried out on the High Pressure Injection (HPI) System which tests the HPI pump 36C. When this pump is tested, the operation of the valve SW CV 3810 also is tested. These are the principal components tested, as defined by the test. Because of the actuation of the signal to the pump and the flow through the test lines, the operation of other components tested are the valves BW1X and BW2X, SW CV 3810 and SW CV 18C, valve CV 1408B, and the valve MU18C.

To determine the test-limited risk, the minimal cutsets containing the unavailabilities of one or more of these components are identified, and all the minimal cutset contributions summed; this sum is the STI contribution for the test. For the PSA used, the sum of the associated minimal cutset contribution is 6.8×10^{-5} per year, which is the STI contribution. We note that all the minimal cutsets are summed which contain at least one of the components tested. If only the minimal cutset contributions with the principal components tested are summed, then the test-limited risk for the test will be underestimated. This will result in a small error if the additional components tested have small minimal cutset contributions; however, in certain cases, they can be non-negligible. Thus, a check must be made that all the dominant minimal cutset contributions are represented for all components included in a test.

To obtain the risk increase, ΔR, associated with the test, all the failures of components which are tested can be set to a True State and the increase in CDF determined. Alternatively, the test-limited risk can be divided by the component unavailability q.

5.4.3 Tables of Test-Limited Risks

Tables 5.1 and 5.2 display the calculated test-limited risks for surveillance tests of components in the Emergency Feedwater (EFW) system and in the HPI system. Such displays can be used to present results for prioritizing the test-limited risks at a plant, and for presenting the test-limited risks for proposed new STIs. Again, such presentations should be accompanied by sensitivity studies or uncertainty studies when sensitivities in given assumptions or data can affect the conclusions.

5.4.4 Risk Strategies Involving STIs

Ideally, the proposed STI modifications would result in a decrease or no net increase in risk. A risk increase arising from proposed STI relaxations can be compensated for by risk reductions in other STI contributions, or more generally, by risk reductions in other activities. If the risk increases are small, then risk reduction does not need to involve large amounts of resources. For instance, configuration control (discussed in Chapter 8), or an extra inspection or a quality assurance check may suffice. In general, these strategies should be acceptable from engineering considerations and not be based on numerical manipulations.

To reduce the risk contribution R_D associated with an STI, the basic formula for R_D can be used as a guide (which is one of the values of calculating the basic contributing factors to R_D):

$$R_D = q\Delta R$$

where

q = the component unavailability

$$\simeq \frac{1}{2}\lambda T$$

and

ΔR = the increase in risk level with the component down.

Thus, to reduce the risk contribution R_D, either the component unavailability q or the risk importance ΔR can be reduced. To reduce q, either the component's failure rate or its surveillance test interval can be reduced.

The risk importance ΔR associated with the test-limited risk involves the unavailabilities of the other contributors in the same minimal cutset as the STI contribution. By examining these other contributors, strategies can be devised for reducing ΔR; these can involve testing other components more frequently (especially if these other tests are relatively inexpensive), checking for misconfigurations before the test is conducted, improving the reliabilities of one or more components in the minimal cutset, or reducing the AOTs of one or more components.

Table 5.1 STI CDF Contributions for the Emergency Feedwater (EFW) System

Principal Components Tested	Type of Test	Additional Components Tested	Test Frequency	STI CDF Contribution
Pump 7A	Flow	CS19 CS98 CS99 CV2802 CVY-3 CVY-4 CVY-1 CVY-2	Monthly	2.9E-5
CV2626	Stroke	None	Quarterly	1.6E-5
CV2620	Stroke	None	Quarterly	1.2E-5
CVY-1	Stroke	None	Quarterly	1.2E-5
Pump 7B	Flow	CS19 CS98 CS99 CV2800	Monthly	9.6E-6
CVX-2	Stroke	None	Quarterly	7.8E-6
CVX-1	Stroke	None	Quarterly	6.2E-6
CVY-2	Stroke	None	Quarterly	2.0E-6
CV2670	Stroke	None	Quarterly	1.7E-6

Table 5.2 STI CDF Contributions for the High Pressure Injection (HPI) System

Principal Components Tested	Type of Test	Additional Components Tested	Test Frequency	STI CDF Contribution
Pump 36C & SW CV 3810	Flow Stroke	BW1X CV1408B BW2X MU18C SW CV3810 SW CV18C	Annual	6.8E-5
Pump 36C	Flow	BW1X CV1408B BW2 MU18C	Monthly	4.4E-5
SW CV3810	Stroke	SW CV18C	Annual	2.4E-5
Pump 36A & SW CV3808	Flow Stroke	BW1X CV1407A BW3X MU18A SW CV3808 SW CV018A	Annual	1.4E-5
Pump 36A	Flow	BW1X CV1407A BW3X MU18A	Monthly	1.4E-5
Pump 36B & SW CV3809	Flow Stroke	BW1X CV1407A BW3X MU16 MU17 MU18B SW CV389 SW CV18B	Annual	1.4E-5
Pump 36B	Flow	BW1X CV1407A BW3X MU16 MU17 MU18B	Monthly	1.4E-5

6. ADVERSE EFFECTS OF SURVEILLANCE TESTING

Basic Concepts

Adverse Effects of Testing: The operating experience of nuclear power plants indicates that some surveillance tests may be associated with some of the following adverse effects: causing plant transients, equipment wear, misconfiguration, unavailability resulting from test downtime, radiation exposure, or unnecessary burden on plant personnel.

Criteria for Risk-Effectiveness of a Test: If the test-limited risk is greater than the test-caused risk for a given test interval, then the test is risk-effective, and vice versa.

Risk-Based Test Interval: The interval for which the total risk impact of the test is minimized. Usually, this calculated test interval is considered along with engineering and operational considerations to define an acceptable test interval.

Risk Contributions Constituting Test-Caused Risk: The risk contributions associated with the adverse effects of the test. If an adverse effect, e.g., test-caused transients, is predominant among the various adverse effects, then the test-caused risk can be approximated by the risk contribution from test-caused transients.

Test-Caused Risk: The STI risk contribution caused by testing, or associated with the adverse effects of testing. When the adverse effects are expected to be significant or evident from the operating experience, then this contribution should be taken into consideration in evaluating the surveillance requirements.

Total Risk Impact of a Test: The sum of the test-limited and test-caused risk contributions. To optimize the test interval from a risk standpoint, we need to minimize this total risk impact associated with the test.

Chapter Outline

List of Symbols

ϕ the proportion by which the initiating event group is caused by the test-caused transients, namely, the extent to which the frequency of the initiating event group is attributable to the test-caused transients; $0 \leq \phi \leq 1$

I_j the frequency of the initiating event group associated with the test-caused transient

$N_{IE\text{-}j}$ the number of transient events belonging to the relevant initiating event group

N_{test} the number of transient events due to the test

p_{trip} the probability that a transient will occur during, or as a result of, the given test

$q(n,t)$ component unavailability as a function of the number of tests, n, performed and the elapsed time since the last test, t

$\bar{\Delta q}_n$ the average increase in component unavailability that results from n tests

R_C the risk contribution which is caused by the test; $R_C = R_{trip} + R_{wear} + R_{config} + R_{down}$

R_{config} the risk contribution from potential misconfiguration following test

R_{down} the risk contribution associated with test downtime

R_T the total risk impact of the test; $R_T = R_D + R_C$

R_{trip} the risk contribution from test-caused plant transients

R_{wear} the risk contribution from test-caused equipment wear

$R_{IE\text{-}j}$ the risk contribution of the j-th initiating event group to the total plant risk

$\bar{R}_{C,n}$ the average increase in the test-caused risk due to equipment wear resulting from test-caused degradations of n tests on the equipment

$\bar{R}_D$ the average risk impact limited by the test; this impact does not depend on the number of tests

$\bar{R}_{T,n}$ the total risk impact of the test comprising the test-limited risk and the test-caused risk due to equipment wear; $\bar{R}_{T,n} = \bar{R}_D + \bar{R}_{C,n}$

6.1 Current Practices and Issues

As briefly discussed in the previous chapter, some tests may cause adverse effects. When such adverse effects are expected to be significant or evident from operating experience, then the tests should be evaluated considering both the beneficial and adverse effects. The explicit consideration of the adverse effects along with the beneficial effects will help to establish risk-effective surveillance requirements that will minimize the total risk implication associated with such tests.

In general, we can reduce the adverse effects of testing by extending the surveillance test intervals (STIs) because, then, fewer tests will be conducted. Extending the STI may be associated with some or all of the following benefits:

1) Plant transients are less likely to be caused by testing.

2) The tested equipment is less likely to wear out.

3) The components involved in the test (e.g., isolation valves) are less likely to be misconfigured after the test.

4) The equipment's unavailability due to downtime for the test will be decreased because tests are less frequent.

5) Exposure of plant personnel to unnecessary radiation will be reduced.

6) Unnecessary burden on plant personnel also will be reduced.

However, as we extend the STI, the equipment will, correspondingly, be more exposed to failures. As a result, the risk impact associated with potential failures, or the test-limited risk, will be larger because there is a higher chance that the equipment may fail between the periodic tests. Therefore, we need to strike a balance between the opposing effects; i.e., the more we extend the STI, the smaller the adverse effects, but the greater the risk impact from the increasing fault-exposure time.

6.2 Test-Caused Risk and Total Risk Impact

Let

R_D = the STI risk contribution which is detected by the test

= the test-limited risk contribution

and

R_C = the STI risk contribution which is caused by the test.

= the test-caused risk contribution.

We then can define the total risk impact:

R_T = the total risk contribution which is associated with the test

$$= R_D + R_C \tag{6.1}$$

R_T is the contribution computed in PSAs. Often, R_C is assumed to be zero. However, for some tests, R_C may be significant, as evident from operating experience. We note that the total risk impact is defined as $R_D + R_C$, as opposed to $R_D - R_C$. The reason for this definition is that, although R_D is beneficial risk impact, it accounts for the risk from failures occurring between tests; the greater R_D as a result of increasing test interval, the higher will be the risk because of the increasing chance of failure between tests.

The risk-based method to quantify R_D was discussed in Chapter 5. In this chapter, we focus on R_C and discuss how R_T can be taken into consideration in determining risk-based optimal test interval.

6.2.1 Adverse Effects of Testing

R_C is the risk contribution which is caused by the test itself. Table 6.1 lists such risk contributions associated with a test, along with their causes.

The test-caused risk contributions listed in Table 6.1 are all subject to a risk analysis based on the risk measure, core-damage frequency, or other risk measures of higher levels, such as releases of radioactive material, offsite consequences of the radioactive material, or public health risk. Although other risk measures at a lower level, such as safety-system unavailability, can be used to evaluate R_{wear}, R_{config}, and R_{down}, the test-caused risk contribution due to transients, i.e., R_{trip}, cannot be

Table 6.1 Test-Caused Risk Contributions and Their Causes

Identifier	Risk Contribution	Causes of the Risk
R_{trip}	Risk from test-caused trips	Human error, equipment failure, procedural inadequacy.
R_{wear}	Risk from test-caused equipment wear	Inherent characteristics of the test, procedural inadequacy, human error.
R_{config}	Risk from test misconfigurations or errors in component restoration	Human error, procedural inadequacy.
R_{down}	Risk associated with test down-time in carrying out the test	Unavailability of the component during the test. Affected by the test override capability.

evaluated using the safety-system unavailability as the risk measure because the unavailability will not be affected, in general, by the variation in the likelihood of a trip occurring during a test.

The use of a same risk measure in analyzing all the different kinds of risk contributions associated with a test will facilitate the evaluation of its risk-effectiveness. Core-damage frequency is the lowest-level risk measure that can be used to evaluate all the test-caused risk contributions listed in Table 6.1, and therefore, is used here as the primary risk measure to quantify these various risk contributions.

From Table 6.1, the risk contribution caused by a test, R_C, can be expressed in a general form as:

$$R_C = R_{trip} + R_{wear} + R_{config} + R_{down} \quad (6.2)$$

where,

R_{trip} = risk from test-caused plant transients
R_{wear} = risk from test-caused equipment wear
R_{config} = risk from potential misconfiguration following test
R_{down} = risk associated with test downtime

For any specific test, a number of the contributions on the right-hand side will not be relevant, or will not be significant. When the risk-effectiveness of a test program or procedure for several individual components is evaluated, then the contributions for each test plus the contributions from any interactions will need to be considered.

Besides those defined in Table 6.1, sometimes two other adverse effects of a test may be encountered: radiation exposure to plant personnel, and unnecessary burden on plant personnel. These two adverse effects differ from those in Table 6.1 in that: 1) the radiation exposure to plant personnel is not amenable to a risk analysis based on the core-damage frequency as a risk measure because the core-damage frequency, or some other lower-level risk measures, are not affected by the amount of the radiation exposure to plant personnel; and 2) the unnecessary burden on plant personnel, in general, also is not suitable for a risk analysis. However, although excluded from the quantitative risk analysis, these adverse effects can be considered qualitatively along with the results of quantitative risk analysis for evaluating surveillance requirements.

All these adverse effects may not be associated with a given test, or some effects may be more significant then others. If so, we can focus on the dominant contributions of the test, which can be identified using the insights gained from the comprehensive examination of all Technical Specification surveillance requirements (NUREG-1366, Lobel et al., 1990). The plant-specific data on the test also may be reviewed, if deemed necessary. The comprehensive examination used the following, important adverse effects, as the criteria to screen surveillance requirements that need to be improved:

a) Plant transients
b) Unnecessary wear
c) Burden on licensee's time
d) Exposure of personnel to radiation

Table 6.2 shows, for several example tests, the dominant adverse effects that were identified. For example, the NUREG-1366 study identified unnecessary wear and licensee burden as dominant adverse affects of the auxiliary feedwater (AFW) testing. A significant cause of the unnecessary wear of the AFW pumps is testing the pumps by recirculating flow through a minimum recirculation line which is not adequately sized. Even if these recirculation lines are increased, frequent testing (monthly in some plants) will contribute to the wear. The licensee burden was determined in terms of time required that cannot be justified by the safety significance of the surveillance.

Table 6.2 Adverse Effects of Several Example Tests Identified as Dominant in the NUREG-1366 Study

Surveillance Requirement	Plant Transient	Unnecessary Wear	Licensee Burden	Radiation Exposure
Partial stroke testing of main steam-isolation valve (MSIV)	√			
Turbine overspeed protection	√		√	
Verify that diesel generator starts and reaches rated speed		√		
Fast start and loading of diesel generator		√		
Auxiliary Feedwater (AFW) Pump Testing		√	√	
Verify proper valve lineup every 31 days for emergency core cooling systems and containment isolation valves			√	√

Among the various risk contributions of Table 6.1 that are subject to risk analyses, the risk from potential misconfiguration following test, R_{config}, is evaluated as part of human reliability analysis in a PSA (NUREG/CR-4772, Swain, 1987). The risk associated with test downtime, R_{down}, can be assessed similarly as maintenance downtime contribution, namely, by considering the fraction of time during which the component is unavailable.

In this chapter, we show how the risk from test-caused plant transients, R_{trip}, and the risk from test-caused equipment wear, R_{wear} can be evaluated using a PSA. These adverse effects generate significant safety concerns because of: 1) potential plant transients which challenge safety systems; and 2) significant wear-out of equipment which increases the unavailability of safety systems or functions, and thereby, reduces the plant's capability for mitigating accidents.

6.2.2 Risk-Effectiveness of Testing

Once risk contributions associated with a test (or a group of tests) are quantified, then the test can be evaluated from a risk perspective. One way is to compare the test-limited risk contribution, R_D, with the test-caused contribution, R_C. The test is risk-effective if the risk limited by the test is greater than the risk caused by the test:

$R_D > R_C$: risk-effective test

Conversely, the test is risk-ineffective if the test-caused risk contribution is greater than the test-limited risk contribution:

$R_C > R_D$: risk-ineffective test

Figure 6.1 shows a conceptual plot of the test-limited risk, the test-caused risk, and their corresponding total risk, versus a test parameter of interest. The figure shows only one possible pattern of behaviors in R_D and R_C; other patterns can easily be envisioned. The test parameter can be the test interval, the probability of a trip occurring during the test, the aging caused by the test, or any other relevant parameter. With studies such as that conceptualized in the figure, regimes and conditions for risk- effective tests can be identified. Present tests can be evaluated and criteria which ensure that the test is risk-effective can be determined. These evaluations also can provide a basis for prioritizing the tests for their test-caused contributions and sensitivities.

The risk-effectiveness may be evaluated by considering only some specific contributions constituting R_C. Suppose that only the contribution due to test-caused transients, R_{trip}, is predominant among the specific contributions of R_C. The criteria for risk effectiveness then can be represented as:

$R_{trip} < R_D$:test risk-effective with regard to test-caused transients

The risk-effectiveness of the test can be evaluated with regard to test-caused transients, even if some of the other risk contributions are not insignificant compared to R_{trip}. When more test-caused contributions are considered, then broader conclusions can be reached.

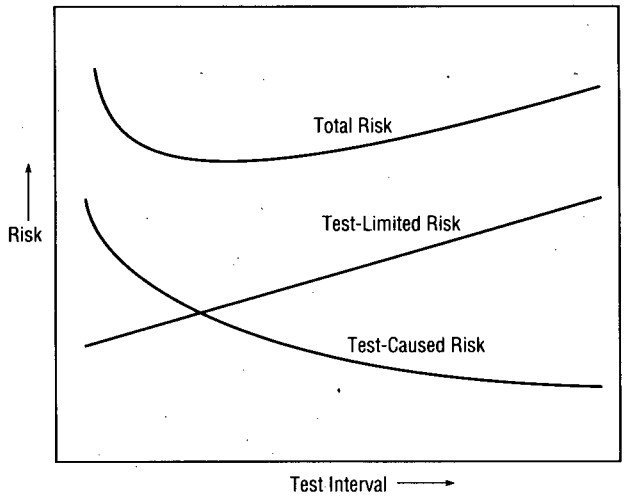

Figure 6.1 Risk contribution of surveillance testing versus test interval

Another way of evaluating the test from a risk perspective is in terms of its total risk impact defined as: $R_T = R_D + R_C$. An advantage of using total risk as a measure to evaluate testing is that it helps to define an optimal test interval. The risk-based, optimal test interval, T_{opt}, can be taken from the value where R_T reaches its minimum because we should minimize the total risk impact of the test. However, this calculated minimum should not be taken too strictly in view of uncertainties in risk quantification, and also other operational or practical factors.

6.3 Risk Impact of Transients Caused by Testing

6.3.1 Impact of Test-Caused Transients on the Plant

Once a transient occurs during testing with the plant at power, it generally causes the process condition of the plant to deteriorate, and consequently, causes a reactor trip. Hence, the risk impact of the test-caused transient or the resultant trip depends on the performance of the plant's safety systems, and sometimes, on the operator's actions following the transient.

As an example, the main steam isolation valves (MSIVs) of some pressurized water reactors (PWRs) are periodically partial-stroke tested (typically 10% closed) during power operation. However, such a test may result in a full closure of the valve due to an operator's error in performing the test, or to a failure of the test equipment.

The inadvertent full closure of the MSIV reduces the heat-removal capability of the power conversion system, and thus, may require intervention of the neutron chain reaction through the reactor protection system (RPS), or the operators, if the RPS fails to properly respond. Even after the successful intervention of the heat production in the reactor, some safety systems other than the RPS also will be required to perform successfully to prevent potential core damage.

Therefore, to evaluate the risk impact of the transient that may occur during MSIV testing, we need to consider the response of the plant safety systems and the operators to the transient. These considerations are typically done in PSAs. The following section introduces a PSA-based formula, and then describes the procedure for evaluating the risk impact. An example application is given in Section 6.3.3.

6.3.2 Basic Procedure for Evaluating the Risk Impact of Test-Caused Transients

The plant transients induced by testing are a kind of initiating event from a viewpoint of PSA because they will cause or require a reactor trip. Hence, we can evaluate the risk impact of test-caused transients from the risk contribution associated with the relevant initiating event group:

$$R_{trip} = \frac{N_{test}}{N_{IE-j}} R_{IE-j} \qquad (6.3)$$

$$= \phi R_{IE-j}$$

where,

R_{trip} = the risk contribution from test-caused plant transients

R_{IE-j} = the risk contribution of the j-th initiating event group to the total plant risk

N_{test} = the number of transient events due to the test

N_{IE-j} = the number of transient events belonging to the relevant initiating event group

ϕ = the proportion by which the initiating event group is caused by the test-caused transients, namely, the extent to which the frequency of

the initiating event group is attributable to the test-caused transients ($0 \leq \phi \leq 1$)

The following procedure shows how we can evaluate the risk impact of test-caused transients using the basic formula for R_{trip} above, within a PSA model.

Step 1: Identify the transient categories associated with the transient that may be caused during, or as a result of, the test

To evaluate the risk contribution due to test-caused transients using the formulas discussed in the previous section, it first is necessary to identify the associated transient categories that may be caused during, or as a result of, the test. The categories associated with the test-caused transient can be identified from the EPRI transient categories (EPRI NP-2230, McClymont et al., 1982), by considering how the test is conducted and what kinds of transients the test can cause, or has caused in the operating history of the plant. Although a PSA, such as done in the individual plant evaluation (IPE) studies, may not model these transients directly, we can find initiating event groups that are associated with the transients. Also, we can identify from licensee event reports (LERs) those transient events caused by the testing under consideration.

Step 2: Associate transient categories with the plant-specific initiating event groups

To use transient categories, the categories should be associated with the initiating event groups modeled in the plant-specific PSA, considering the characteristics of the transients included in the transient categories and the initiating event groups. For this association, we can classify each of the transient categories into the relevant initiating event group.

Step 3: Evaluate the risk contributions of the initiating event groups

The risk contribution of the specific initiating event group, say the j-th initiating event group ($R_{IE\text{-}j}$), can be easily obtained from the plant-specific PSA by summing up the frequencies of all the accident sequences beginning from the initiating event group.

Step 4: Estimate ϕ

We can now estimate from plant operating data the proportion ϕ by which the frequency of the initiating event group is attributable to test-caused transients:

i) Classify the transient events in the data base into the relevant categories, identifying the transients due to the tests whose risk impacts are being evaluated.

ii) Obtain the number of transient events associated with each of the initiating event groups, i.e., $N_{IE\text{-}j}$, by adding the numbers of transients in the categories which are associated with the initiating event group.

iii) Obtain the number of transient events attributable to each of the given tests, i.e., N_{test}, by adding the numbers of transients in the categories which are associated with the test.

iv) Calculate ϕ from N_{test} and $N_{IE\text{-}j}$; $\phi = N_{test} / N_{IE\text{-}j}$.

Step 5: Evaluate the test-caused risk contribution due to transients

The test-caused risk contribution from test-caused transients now can be evaluated by multiplying the risk contribution of the relevant initiating event group to the total plant risk, $R_{IE\text{-}j}$, by the proportion ϕ; namely, $R_{trip} = \phi R_{IE\text{-}j}$.

6.3.3 Example Evaluation of the Risk Impact of Test-Caused Transients

As a practical example, we apply the procedure to the MSIV operability testing of a BWR. The operating experience of BWR plants suggests that the test caused a significant number of plant transients. The PSA for a BWR conducted as part of the NUREG-1150 study is used for evaluating the risk impact. The LERs for 30 BWRs for 1985 were used to analyze transients, assuming that all the plants conducted MSIV testing quarterly.

Step 1: The EPRI transient categories for BWRs will be used here because we are evaluating the risk contribution of testing at a BWR. Table 6.3 lists the BWR categories associated with the transients that may be caused during, or result from, the MSIV test. Only two categories are associated with the test-caused transients, i.e., categories 6 and 7, which represent inadvertent full closure of one MSIV, and partial MSIV closure, respectively.

Although there is another category that is connected to the MSIV, i.e., category 5 for main steam-isolation valve closure, the transients belonging to this category are not caused by the MSIV testing. This particular transient occurs when any one of various steam lines and nuclear system malfunctions require termination of steam flow from the vessel automatically or by the operator's action.

Step 2: Each of the 37 BWR transient categories should now be associated with the initiating event groups defined in the PSA; Table 6.4 shows a part of such an association (NUREG/CR-5775, Kim et al., 1992). For instance, the transient category 5 is classified into the initiating event group T2, which incorporates all the transients that occur with the power conversion system initially unavailable.

Table 6.3 Association of Test-Caused Transients with EPRI BWR Categories

Test	BWR Transient Category
MSIV Operability Test	6. Inadvertent closure of one MSIV 7. Partial MSIV closure

Table 6.4 Association of Transient Categories with Initiators

Transient Category	Definition	Initiator
1	Electric load rejection	T3A
2	Electric load rejection with turbine bypass valve failures	T3A
3	Turbine trip	T3A
4	Turbine trip with turbine bypass valve failure	T3A
5	Main steam isolation valve closure	T2
6	Inadvertent closure of one MSIV	T2
7	Partial MSIV closure	T2
8	Loss of normal condenser vacuum	T2
9	Pressure regulator fails open	T3A

Step 3: Table 6.5 shows the risk contributions of each initiating event group, $R_{IE\text{-}j}$, to the total core-damage frequency. This information is readily available from the PSA document or the computerized PSA model; otherwise, $R_{IE\text{-}j}$ can be derived by summing the frequencies of those accident sequences that are induced by initiator j. The sum of the risk contributions for each of the initiating event groups represents the average, total core-damage frequency from the level-1 PSA. Table 6.5 shows the risk contribution of initiator T2 relevant to the MSIV testing as: $R_{T2} = 5.4 \times 10^{-7}$ per year.

Step 4: The proportion ϕ can be estimated as follows:

i) The transient events of the plant's operating data base can be classified into relevant transient categories of the 37 BWR categories. For instance, Table 6.6 shows the data base includes 10 transient events that can be classified into transient category 1.

ii) The transient that may be caused by MSIV testing is associated with initiating event group T2 because the power conversion system (PCS) will become unavailable if the transient occurs (refer to Table 6.5). According to Table 6.6, the data analysis identified 18 transient events belonging to T2 initiator; there are only four transient categories belonging to T2, i.e., categories 5, 6, 7, and 8. The number 18 is obtained by summing the numbers of transients for the four categories; namely, $N_{T2} = 18$.

iii) The number of transients caused by MSIV testing, N_{test}, can be obtained by summing the numbers of test-caused transients for categories 6 and 7 which are shown in the last column of Table 6.6: $N_{test} = 3$. Of the six transients in categories 6 and 7, three of them, namely a half, were caused by MSIV testing. (Some transients belonging to other categories also may have been caused by certain types of testing. However, these are not identified in the column of "Number of Test-Caused Transients" for other categories because the data analysis evaluated only the MSIV test.)

iv) Now, we can calculate the proportion: $\phi = N_{test} / N_{T2} = 3/18 = 0.17$; namely, 17 % of the frequency of the initiating event group T2 is attributable to the MSIV testing.

Step 5: We can now calculate the risk contribution of transients that may be caused by quarterly MSIV testing:

$$R_{trip} = \phi R_{T2} = 0.17 \times (5.4 \times 10^{-7}/\text{yr}) = 9.0 \times 10^{-8}/\text{yr}.$$

Table 6.5 Risk Contributions of the Initiators

Initiator	Description	Risk Contribution (per year)
T1	Loss of offsite power (LOSP) transient	6.2E-6
T2	Transient with the power conversion system (PCS) unavailable	5.4E-7
T3	Transient with the PCS initially available made up of T3A, T3B, and T3C	Sum of risk contributions of T3A, T3B, and T3C
T3A	Transients of the T3 group other than those below	1.0E-6
T3B	Transients due to an inadvertent open relief valve in the primary system	4.5E-8
T3C	Transients involving loss of feedwater (LOFW), but with the steam side of the PCS initially available	4.7E-7
A	Large loss of coolant accident (LOCA)	8.4E-6
S1	Intermediate LOCA	8.6E-8

6.3.4 Basic Formulas for Sensitivity Analysis and Criteria for Risk-Effectiveness

For sensitivity analyses of the test-caused risk due to transients, R_{trip}, to the variation in test interval, T, we can transform the expression for R_{trip}, discussed in Section 6.3.2, to the following formula in terms of T:

$$R_{trip} = \frac{p_{trip}}{I_j T} R_{IE-j} \qquad (6.4)$$

where,

I_j = the frequency of the initiating event group associated with the test-caused transient

Table 6.6 Plant Operating Experience to Estimate ϕ

Transient Category[a]	Initiator[b]	Number of Transients	Number of Test-Caused Transients
1	T3A	10	
2	T3A	2	
3	T3A	11	
4	T3A	0	
5	T2	3	
6	T2	4	2
7	T2	2	1
8	T2	9	
9	T3A	1	

[a]For definition of these categories, see Table 6.4.
[b]For definition of these initiators, see Table 6.5.

$R_{IE\text{-}j}$ = the risk contribution of the j-th initiating event group to the plant's total risk

p_{trip} = the probability that a transient will occur during, or as a result of, the given test

From this formula for R_{trip} and that for R_D discussed earlier, we can establish a criterion for risk-effectiveness of surveillance testing. The test is risk-effective with regard to test-caused transients if:

$$T > \sqrt{\frac{2\,p_{trip}}{\lambda I_j}\,\frac{R_{IE\text{-}j}}{R_1 - R_0}} \qquad (6.5)$$

The test is risk-ineffective if T is smaller than the value of the right-hand side.

The risk-effectiveness criterion on the test interval should be used only when the probability, p_{trip}, that a transient will occur during, or as a result of, the test can be reasonably estimated. In general, the less likely a test-caused transient will occur, the more operating data are necessary to obtain a reasonable estimate of its probability.

Let

T_{min} = the minimum test interval, such that the test is risk-effective with regard to test-caused transients, as long as the test interval is greater than the minimum.

We then can derive the following expression by setting R_D equal to R_{trip}:

$$T_{min} = \sqrt{\frac{2\ p_{trip}}{\lambda I_j} \frac{R_{IE-j}}{R_1 - R_0}} \tag{6.6}$$

The risk-effectiveness criterion can be stated in terms of T_{min} as follows: if $T > T_{min}$, the test is risk-effective; otherwise, it is risk-ineffective.

The optimal test interval, at which the total risk impact is minimized, can be obtained from the following formula:

$$T_{opt} = \sqrt{\frac{2\ p_{trip}}{\lambda I_j} \frac{R_{IE-j}}{R_1 - R_0}} \tag{6.7}$$

which is identical to T_{min}. However, in general, T_{min} may differ from T_{opt}; e.g., when a nonlinear unavailability model is used for R_D.

6.3.5 Example Sensitivity Analysis and Interpretation of Results

To evaluate the effects of various test intervals on the plant from a risk perspective, we can analyze the sensitivity of the risk impact of test-caused transients to test interval. The risk impacts that need to be considered are: 1) the test-caused contribution from transients, R_{trip}, 2) the test-limited contribution, R_D, and 3) the total risk impact of the test, R_T.

Figure 6.2 shows a sensitivity analysis for MSIV operability testing which was conducted using the following formulas discussed earlier:

$$R_T = R_D + R_C$$

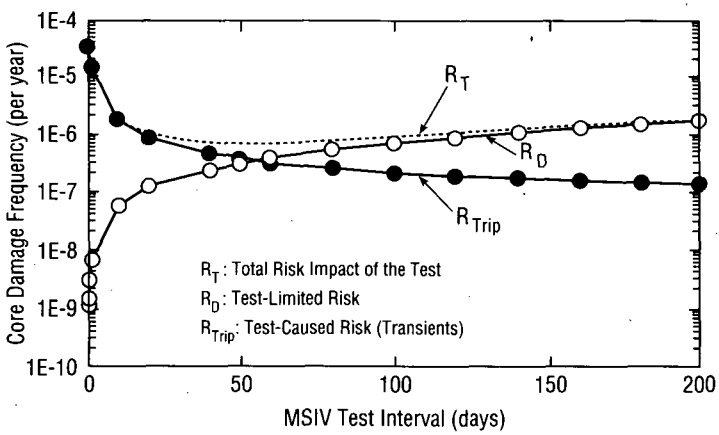

Figure 6.2 Risk-sensitivity of MSIV testing

$$R_{trip} = \frac{p_{trip}}{I_j T} R_{IE-j}$$

$$R_D = \frac{1}{2}\lambda T \cdot (R_1 - R_0)$$

Here, it was assumed that test-caused transients are the most dominant adverse effect of the MSIV testing, as the NUREG-1366 study (Lobel et al., 1990) indicates (see Table 6.2), and also that others are negligible compared to this dominant effect. Hence, only the test-caused risk contribution from test-caused transients is compared to the test-limited risk contribution in evaluating the risk-effectiveness of the test.

From the sensitivity analysis, we obtain the following insights:

1. R_{trip} decreases as T is increased because fewer transients are expected as the test is conducted less frequently. However, then R_D increases because, the test is more likely to detect a failure.

2. The curves for R_D and R_{trip} intersect when the test interval is approximately 54 days. This value is the minimum test interval, T_{min}. The test interval must be longer than 54 days for the MSIV test to become risk-effective; otherwise, it is risk-ineffective.

3. The risk-effectiveness of the test with regard to test-caused transients also can be seen by comparing the test-limited risk contribution to the test-caused risk contribution due to transients. In the region where $T > 54$ days, R_D is larger than R_{trip}, and thus, the test is risk-effective. Where $T < 54$ days, the test is risk-ineffective.

4. This example used the LER data base for 30 BWRs for 1985, assuming that the operability of MSIVs is tested quarterly at all the plants. However, at some plants the MSIVs were being tested more frequently; e.g., a biweekly surveillance when the test failure occurred. If the minimum test interval of 54 days is assumed to be applicable to this plant, the biweekly test is risk-ineffective with regard to test-caused transients, because the interval is shorter. Even if other types of adverse risk impacts, nonnegligible compared to R_{trip}, are considered, this biweekly test at the plant will be risk-ineffective.

5. The analysis was based on a PSA and also on the analysis of plant operating data, i.e., LERs. As a result, the quantitative results are associated with their corresponding uncertainties. Therefore, the numerical results from this analysis should not be taken too strictly, unless an uncertainty analysis is performed and taken into account in the decision-making process for evaluating the STI.

6. Sensitivity analyses, as shown in Figure 6.2, can be very useful in defining a test interval or evaluating a potential modification to it. The calculated, optimal test interval, T_{opt}, is 54 days, the same as T_{min}; however, the curve of R_T indicates that the total risk impact only marginally increases when T is changed; for example, from 54 or 91 days (i.e., the current quarterly test interval) to 150 days. We note that the more the interval is extended beyond T_{opt}, the more the test will become risk-effective because the difference between the test-limited risk and the test-caused risk accordingly increases. In addition, we also should take into consideration that the sensitivity curves of R_{trip} and R_T to the variation of T depend on the parameters λ, the equipment failure rate, and p_{trip}, the probability of a transient occurring during testing, which are assumed constant with respect to the test interval. The values of λ and p_{trip} may change, especially when the test is conducted less frequently than formerly. In such a case, the failure rate, λ, may decrease if the test had an adverse effect on the equipment, or it may increase if the test had a positive effect in terms of lubrication, cleanup, required movement of pieceparts, and so on. The value of p_{trip} may increase because the operators are more likely to make errors when testing less frequently. When these aspects are included in the decision process, a reasonable extension of the test interval based on the sensitivity analyses may

be limited to a factor of two or so. When experience is gained with this extension, further modifications may be justified.[1]

6.3.6 Data Needs for Evaluating Test-Caused Transients

The method presented here is based on analyzing transient events, including those caused by tests, using the PSA-based formulas discussed in Sections 6.3.2 and 6.3.4. Hence, we need a PSA for the plant for which the adverse risk impact of testing can be evaluated. The risk contribution of initiating event groups to the total plant risk, may be obtained from the PSA document; otherwise, a computerized model of the PSA can be used. The PSA computer model also can be used to evaluate the conditional core-damage frequency with the component assumed up or down, which is necessary to assess the beneficial risk impact of the test.

We can obtain the transient events from the following plant operating data:

1) Performance Indicator Reports: These reports list the number of reactor trips and safety system actuations at each plant, the date of the events, and the numbers of the relevant licensee event reports (LERs).

2) LER System: Reactor trips are described in LERs.

When test-caused transients for a single plant are evaluated, the plant-specific data may be sparse unless the plant's operating experience covers a substantial period. When this is the case, more data may be used from the operating experience of other plants of similar vintage, such as BWR/4, assuming that the likelihood of occurrence of test-caused transients are similar for all the plants in the data base. (The performance indicator reports classify plants according to design classes.)

6.4 Risk Impact of Equipment Wear Caused by Testing

In this section, we consider the risk contribution associated with test-caused wear of equipment, as another specific, test-caused risk contribution.

---

[1]The Standard Technical Specifications, recently developed (September 1992), recommend that the frequency of MSIV testing will be in accordance with the Inservice Testing (IST) Program, or 18 months. The IST program typically requires quarterly testing for pumps and valves, with possible relief of the test requirement (i.e., extension of the test interval) given a reasonable justification.

6.4.1 Concept of Stress on the Equipment

Some safety-significant components of nuclear power plants, such as an emergency diesel generator or an auxiliary feedwater pump, are tested often enough to raise concern about the progressive wear-out of the equipment due to the accumulation of degradation caused by the test. This degradation may be caused by inherent characteristics of the test, procedural inadequacy, or human error, as discussed earlier.

Furthermore, as time passes, the component also may show aging effects, such as corrosion or erosion. Together, these can increase the unavailability of the component, and thereby, the unavailability of the associated safety system and function; in turn, this can reduce the plant's capability of mitigating an accident.

The degradation from testing and aging effects are induced by two kinds of stresses, i.e., demand, and standby stresses. Demand stress acts only when the equipment is asked to function or is operating; standby stress acts while the equipment is in the standby state. For standby components which are periodically tested, generally, the combination of both stresses causes the equipment to degrade, and ultimately, to fail.

To illustrate how both stresses act together to cause an equipment to fail, let us take an example from a study of the reliability of diesel generators. Consider the case that a connecting rod, weakened by corrosion, fails catastrophically when a diesel is started for operation. This failure was caused by standby stress, which induced the corrosion of the rod. However, it also was caused by demand stress, because although the rod was in a weakened state, it would not have failed if there had been no demand for operation.

6.4.2 Test-Caused Degradation Model to Evaluate Component Unavailability

Based on the concept of stress on equipment and the characteristics of the degradation mechanisms caused by testing and aging, we can formulate the following test-caused component degradation model for component unavailability:

$$q(n,t) = \rho(n) + \int_{nT}^{nT+t} \lambda(n,t')dt' \qquad (6.8)$$

$$\rho(n) = \rho_0 \cdot (1 + p_1 n) \tag{6.9}$$

$$\lambda(n,t) = \lambda_0 \cdot (1 + p_2 n) + \alpha \cdot (nT + t) \tag{6.10}$$

where,

n	=	the number of tests performed on the equipment
t	=	the time elapsed since the last test
$q(n,t)$	=	the component unavailability as a function of the number of tests performed and the elapsed time
$\rho(n)$	=	the failure probability for cyclic demand-caused failures
T	=	the test interval
$nT + t$	=	the time since the last renewal point
$\lambda(n,t)$	=	the standby failure rate (per unit time) for failures occurring between tests
ρ_0	=	the residual cyclic demand-failure probability
p_1	=	the test degradation factor associated with demand failures
λ_o	=	the residual standby time-related failure rate
p_2	=	the test degradation factor for standby time-related failures
α	=	the aging factor associated with aging alone

These expressions represent a model which was linearized from the original, non-linear test-caused degradation model (NUREG/CR-5775, Kim et al., 1992). This linear model can be used for most purposes and is used here.

Some of the parameters, such as the residual demand-failure probability, ρ_0, and the residual standby time-related failure rate, λ_o, can be obtained from the studies on diesel generator reliability (e.g., NUREG/CR-4810, Vesely et al., 1987; NUREG/CR-5510, Vesely et al., 1990; or EPRI-4264, Mollerus et al., 1985). Other parameters can be derived from those that are obtainable from some reports; for example, we can derive the aging factor associated with aging alone, α, from the linear aging rate of the aging model (NUREG/CR-4769, Vesely, 1987) under certain assumptions.

In the expressions above, the unavailability, q(n,t), and the standby failure rate, $\lambda(n,t)$, are represented as a function of n and t. The reason for this functional notation is that the standby failure rate is assumed to be affected not only by the standby time, but also by test-caused degradation. Therefore, component unavailability becomes a function of the number of tests performed on the component

and the time elapsed since the last renewal. However, the cyclic demand failure probability, $\rho(n)$, is represented as a function of only the number of tests, n, i.e., it is assumed that the cyclic demand-failure probability depends only on how many tests were conducted on the component.

6.4.3 Basic Formulas for Risk-Impact Analysis and Criteria for Risk-Effectiveness

The test-caused component degradation model provides a means to estimate the time-dependent component unavailability and its resultant risk impact as a function of the number of tests on the component and the time elapsed since the last overhaul.

Let $\bar{R}_{C,n}$ be the average increase in the contribution to core-damage frequency or test-caused risk resulting from test-caused degradations of n tests on the equipment. We can evaluate $\bar{R}_{C,n}$ using the following formula:

$$\bar{R}_{C,n} = \{\text{the average risk level between } [nT, nT + T]\} - \{\text{the average risk level between } [0,T]\}$$

$$= \Delta\bar{q}_n \cdot (R_1 - R_0)$$

$$= \left(p_1\rho_0 n + \frac{1}{2}p_2\lambda_0 Tn\right) \cdot (R_1 - R_0) \qquad (6.11)$$

where $\Delta\bar{q}_n$ denotes the average increase in component unavailability that results from n tests, and only the test-caused degradation effect is taken into account without considering the aging effect, i.e., $\alpha = 0$. This formula also can be used to analyze the sensitivity of the risk contribution due to test-caused component degradations to variations in the number of tests or the test interval.

Based on this formula, we can establish a criterion on the number of tests for risk-effectiveness. The n-th test is risk-effective with regard to test-caused degradation if:

$$n < \frac{\frac{1}{2}\lambda_0 T}{\rho_0 p_1 + \frac{1}{2}\lambda_0 p_2 T} \qquad (6.12)$$

For the n-th test to be risk-effective, the number of tests performed on the component since the last overhaul should satisfy the above criterion. When the

number of tests on the component is less than the value of the right-hand side in the criterion, then the contribution to core-damage frequency caused by the test will be less than the contribution to core-damage frequency detected by the test. Hence, the test is risk-effective until n tests are conducted.

6.4.4 Assumptions and Limitations in Evaluating the Test-Caused Degradations

The test-caused component degradation model not only incorporates aging effects, but separately takes into account test-caused degradation. However, the degradation model and the formulas for evaluating the risk impact associated with such degradations are based on the following assumptions that should be considered in using the approaches:

(1) Test-caused component degradations affect cyclic demand failure probability, and also standby failure rate; i.e., the component will be more vulnerable to both cyclic demand-related and standby time-related failures as more tests are performed on it.

(2) The standby time-related failure rate increases because of test-caused degradation effects, as well as aging effects.

(3) The time-dependent aging mechanism on the standby failure rate can be represented by a Weibull distribution (NUREG-0492, Vesely et al., 1981).

(4) The demand degradation or failure mechanism is not affected by time. In other words, the cyclic demand failure probability depends only on the number of tests performed on the equipment, not on the idle or dormant time.

6.4.5 Example Application to Diesel-Generator Test

Using the test-caused degradation model, we can perform a sensitivity analysis on the risk impact of test-caused equipment degradations versus test interval. The emergency diesel generator (EDG) was chosen here because of the concern about such degradations on this component, and because reliability data are available to estimate the degradation parameters of the model. The method described can be applied to other components.

The values of the degradation parameters, such as p_1 and p_2, can be estimated from the ratio for cyclic demand-related to standby time-related failures, assuming:

When the number of tests is large, the average increase in component unavailability, which is evaluated by the test-caused component degradation model, is the same as that estimated by the aging model (NUREG/CR-4769, Vesely, 1987).

Figures 6.3 and 6.4 show the sensitivity to monthly and quarterly testing of the diesel generators, respectively, of three different kinds of core-damage frequency impacts: 1) the test-limited core-damage frequency contribution, R_D, (2) the test-caused core-damage frequency contribution due to equipment wear, $R_{C,n}$, and 3) the total core-damage frequency impact of the test, $R_{T,n}$.

The results show that the test is risk-effective for monthly testing up to 61 tests, i.e., approximately 5 years after the last overhaul, and for quarterly testing up to 111 tests, i.e., about 28 years after the last renewal time. However, when the test is no longer risk-effective, the total impact for quarterly testing is greater than that for monthly testing by about a factor of 3.

Figure 6.5 shows the risk-effective lifetime for diesel generator testing as a function of test interval. The lifetime increases with increasing test interval because the degradation effects of the tests accumulate more slowly. However, the total risk at the end of the lifetime also increases when the test interval is increased. For example, if an interval of 1 month is extended to 3 months, then the risk-effective lifetime will increase from 5 years to 28 years, i.e., by a factor of 5.6. However, as indicated above, the total risk at the end of the lifetime for quarterly testing will be about three times higher than that for monthly testing. (The total risk at the end of the lifetime is 3.5E-5 per reactor-year for monthly testing, and 1.1E-4 per reactor-year for quarterly testing.)

The numerical results from this example should be interpreted cautiously. The data available to estimate the degradation parameters are sparse, which significantly influences the results; in this study, these parameters were estimated from reliability studies of several diesel generators. For specific applications, we recommend combining data from diesels with similar design, test, maintenance, and overhaul characteristics, and consequently, to determine the effective requirements for tests and overhauls.

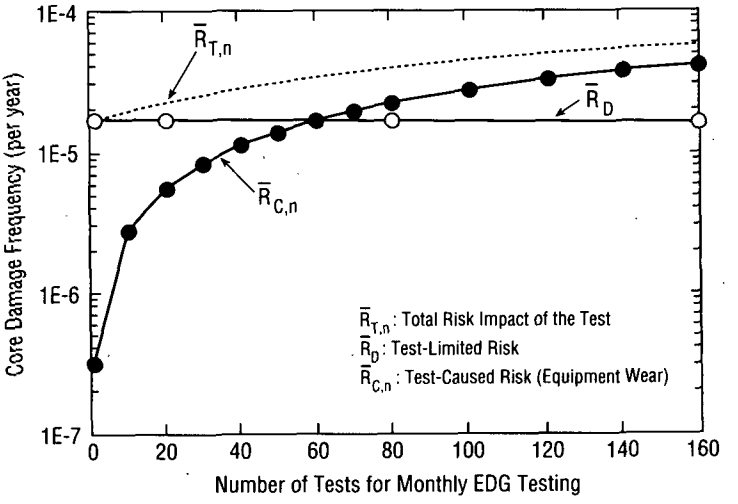

Figure 6.3 Risk-effectiveness of monthly EDG testing

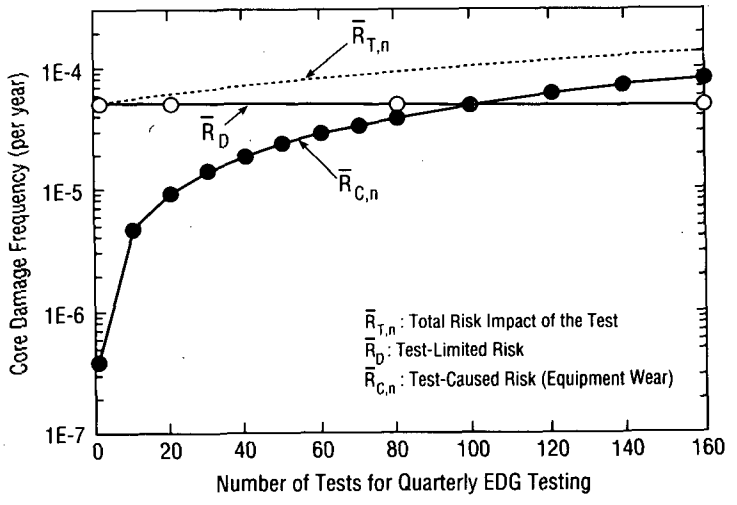

Figure 6.4 Risk-effectiveness of quarterly EDG testing

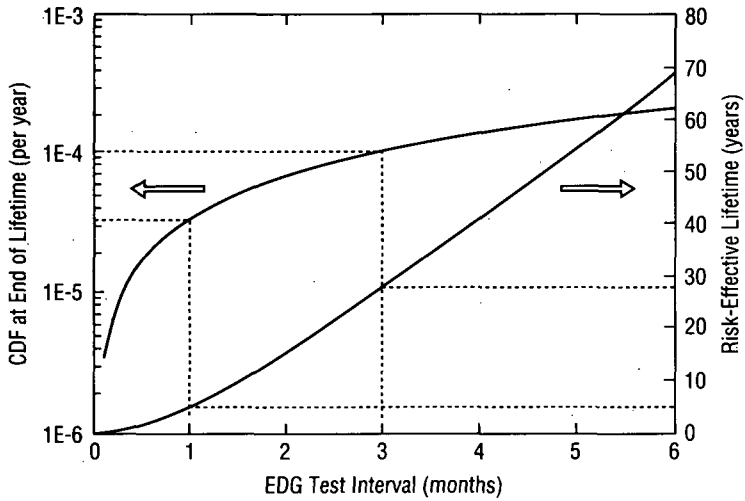

Figure 6.5 Risk-effective lifetime and the total test risk at the end of lifetime for EDG testing

6.4.6 Data Needs for Evaluating Test-Caused Equipment Degradation

The method here is based on the test-caused component degradation model and a PSA. We can use a computerized model of the PSA to assess the conditional core-damage frequency with the component assumed up or down, i.e., R_1 or R_0, which is necessary to evaluate the average contribution of test-caused risk due to equipment degradations, i.e., $R_{C,n}$.

To use the test-caused degradation model, we need to estimate the various parameters for the component, such as the residual cyclic demand failure probability, ρ_0, the residual standby time-related failure rate, λ_o, and the aging rate, α. Several reliability studies have been made on EDGs because of the great importance of their reliability in nuclear plant safety, and the adverse risk implications due to frequent testing with the ensuing degradations of equipment. Some values for the parameters may be taken from the results of these previous studies. For instance, the aging rates for EDGs can be obtained from NUREG/CR-4769 (Vesely, 1987), as we indicated earlier.

However, whenever possible, the values should be obtained for the specific component being evaluated. Particularly, one should try to estimate the test-degradation factors associated with cyclic demand or standby time-related failures, i.e., p_1 or p_2, for the specific component because they may be strongly component-specific.

7. ACTION STATEMENTS REQUIRING PLANT SHUTDOWN

Basic Concepts

LCO Operating Risk: The risk associated with continuing power operation while of the failed equipment is repaired. Similar to the single-event AOT risk.

LCO Shutdown Risk: The risk associated with shutting down the plant with the failed equipment.

Risk-Comparison Approach: The approach to comparing the risk of continuing power operation with the risk of shutting down the plant during a failure to decide on the LCO requirement.

Operational Policy Alternatives: The available alternatives during plant operation given one or more failures in systems needed to remove decay heat. Examples of alternatives include whether or not to test a redundant train, and whether to go to hot shutdown or cold shutdown to complete the repair.

Risk-Based Action Statements: The actions (e.g., AOT for repairs, plant shutdown, testing redundant train) for a failure situation based on risk analyses of the available alternatives.

Chapter Outline

Example Applications to Evaluate LCO Risks	7.4.2
Formulas for Calculating the LCO Risks	7.3.3, 7.3.4
Data Needs for Using the Risk-Comparison Approach	7.3.7
Recommendations for Risk-Based Action Requirements	7.4.3, 7.5

List of Symbols

$\bar{d}$	the mean downtime
$P_d(t)$	the probability of not completing the repair until time t
$P_{IE\text{-}i,SD}$	the probability that the initiating event i will occur during transition to shutdown
r_{CO}	the core-damage probability associated with continuing power operation with the failed equipment
r_{SD}	the core-damage probability associated with shutting down the plant with the failed equipment
$r_{SD/IE\text{-}i}$	the conditional probability of core damage for the initiating event, i, requiring shutdown cooling
$r_{SD\text{-}0/IE\text{-}i}$	the conditional probability of core damage at the start of shutdown cooling for the initiating event i
$r_{SD\text{-}0}(k \rightarrow k+1)$	the conditional probability of core damage associated with the change in plant's state from phase k to phase k+1
R_{CO}	the core-damage frequency associated with continued power operation with the failed equipment
$R_{SD}(k)$	the core-damage frequency for phase k
$R_{SD/IE\text{-}i}(t)$	the conditional frequency of core damage during shutdown cooling at time t for the initiating event i
$\bar{t}_k$	the mean duration of phase k

7.1 Introduction

7.1.1 Current Requirements and Definition of the Problem

Limiting conditions for operation (LCOs) define the allowed outage times (AOTs) and the actions to be taken if the repair cannot be completed within the AOT. Typically, the action required is plant shutdown. In Chapter 3, we discussed methods for analyzing AOTs focussing on controlling the risk during power operation. This partly addresses action requirements because the actions are applicable at the end of the AOT. However, in situations where the risk associated with the action, i.e., the risk of plant shutdown given a failure in the safety system, may be substantial, a strategy is needed to control the risk implications. When a system needed to remove decay heat is inoperable or degraded at power, shutting down the plant may not necessarily reduce risk, compared to continuing power operation and giving priority to completing the repairs. Analyzing these TS requirements and exploring various available alternatives is the focus of this chapter.

For example, for a residual heat removal (RHR) system of a BWR plant in the United States consisting of three trains, a 3-day AOT is defined for single-train failures. However, the action statement requires that the plant is shut down when failures are detected in multiple (i.e., two or three) trains.

These action requirements primarily are directed towards minimizing the risk during power operation, assuming that shutting down the plant is relatively safe; namely, the risk of shutdown is assumed to be negligible. This is not necessarily a reasonable assumption for such a system that removes decay heat. A comparative analysis of risk impacts of action alternatives can address these failure situations.

7.1.2 Failures in Systems for Removing Decay Heat

When failures occur in the following systems, the ability of the plant to remove decay heat may be impaired:

1. RHR system of a BWR or PWR that provides long-term removal of decay heat

2. Auxiliary Feedwater (AFW) system of a PWR which provides feedwater to steam generators to remove decay heat from the primary system

3. Component cooling water (CCW) system of a PWR that provides cooling water to the RHR system

4. Standby service water (SSW) system of a BWR or PWR that subsequently removes heat from the RHR or CCW system for the BWR or PWR, respectively

5. Emergency power system of a BWR or PWR that provides electric power to the systems used to remove decay heat following a reactor scram

Shutting down the plant in such failures may impose substantial risk, which may be comparable or exceed the risk associated with continuing power operation and giving priority to the repairs. Hence, in evaluating the AOTs or action statements for these systems, the shutdown risk can be taken into account explicitly and compared with the risk of continued power operation.

7.2 Basic Concepts of the Comparative Analysis of LCO Risks

7.2.1 Comparison of Conditional LCO Operating and Shutdown Risks

When a safety system enters an LCO because of failure of one or more components in the system, TS allow for one of the two alternatives: a) continue power operation and repair the failed equipment within the defined AOT, or b) shut down the plant to complete the repairs in a shutdown state. We call these alternatives the basic operational alternatives, and the risks associated with these alternatives the LCO risks. The risk associated with repairing the equipment while continuing power operation is called LCO operating risk; the risk associated with shutting the plant down is called LCO shutdown risk.

Figure 7.1 shows a conceptual plot of LCO operating and shutdown risks in terms of core-damage frequency for failure of a system which is needed to remove decay heat. At time A when the failure is detected, the two basic operational alternatives are applicable, i.e., continued power operation, and plant shutdown. The solid line represents the risk profile for continued operation, while the dotted line is the profile for the shutdown.

Upon detecting the failure at time A, the LCO operating risk increases above the baseline due to the increased unavailability of the initially affected (i.e., failed or degraded) system during potential occurrences of accident scenarios requiring it to be operational to prevent core damage. The baseline represents the level of risk associated with power operation when no known failures exist.

The initial increase in the LCO shutdown risk, (Figure 7.1), results from the system's unavailability during the potential occurrences of accident scenarios initiated by events occurring while the plant is being brought to shutdown. Specifically, the increase in risk in the initial stage of shutdown arises from: 1) the unreliability of the

systems which are needed during the change in plant's state, or which must be started up, and 2) the vulnerability of the plant to transients caused by the changes in the plant's state. After entering a stable shutdown state, the risk level usually decreases with time because of the diminishing decay heat, meaning lower capacity requirements on safety systems, and longer time available for recovery if a critical safety function is lost during a shutdown-cooling mission. Obtaining a lower risk level in a stable shutdown mode, compared to the continued-operation alternative, is the principal motivation of going to shutdown.

At time B, when the component is repaired and returned to service, both operating and shutdown risks decrease. The operating risk decreases to the baseline risk level, i.e., the level before the failure was detected, whereas the shutdown risk decreases below the baseline risk level for the power operational mode, because of the much lower rate of heat production in the reactor during shutdown compared to power operation. Another small peak in the shutdown risk at time C arises from the unavailabilities of systems that are needed when the plant is restarted up, and the plant's vulnerability to transients that may be caused by the changes in the operational mode. In this period, the risk is also a function of the rate of heat production, as represented by a small dip which then slowly increases to the baseline risk level as the plant reaches full power operation.

The period that is directly relevant to evaluating action requirements or AOTs for failures in the safety systems is from time A to time B, i.e., the predicted or actual repair time for the component. The risk over this period, i.e., core-damage probability, can be obtained by integrating the conditional CDF to compare the LCO operating and shutdown risks. If the operating risk is smaller than the shutdown risk, then, from a risk point of view, the alternative of continued operation is preferable to the shutdown alternative, and vice versa.

7.2.2 Comparison of LCO Operating and Shutdown Risks

Figure 7.2 compares the core-damage probability (CDP) contributions over the repair time, beginning from time A when the failure is detected. The CDP for operating risk is smaller than that for shutdown risk until time X, when the two curves intersect. Therefore, from a risk perspective, it is more beneficial to continue power operation than to shut down the plant if the operability of the initially affected system can be restored before time X. Where the repair takes longer than the period A to X, it is advisable to shut down the plant.

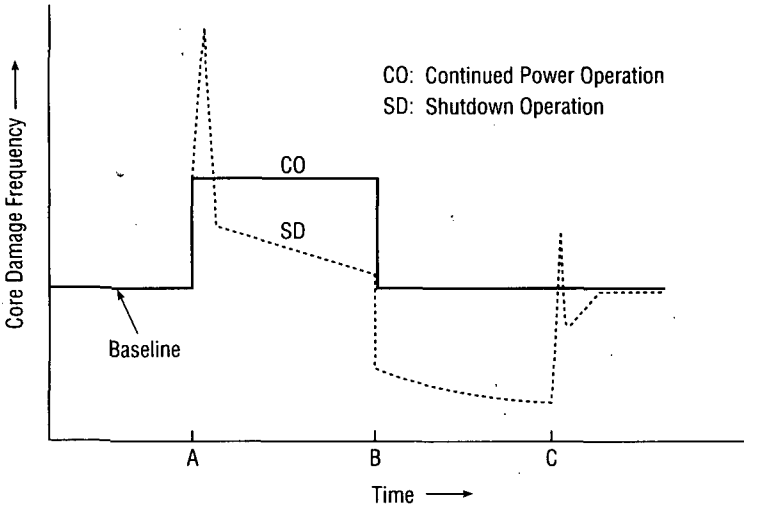

Figure 7.1 Comparison of LCO risks (core-damage frequency) for the basic operational alternatives of continued power operation and shutdown

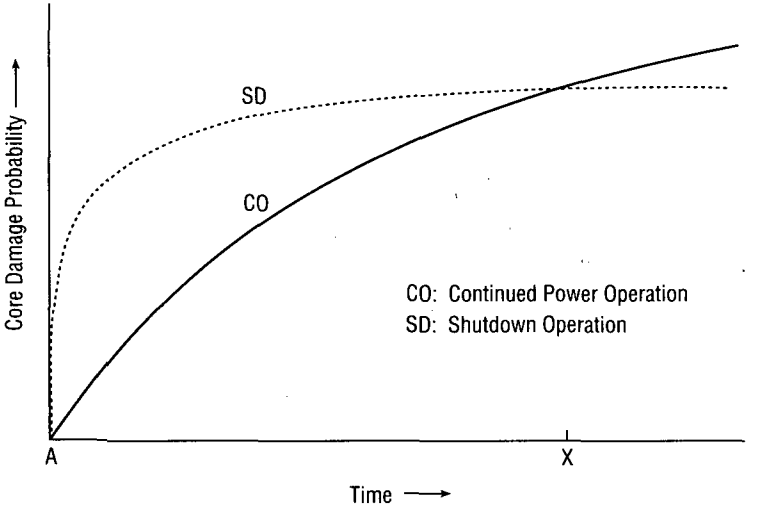

Figure 7.2 Comparison of LCO risks (core-damage probability) for the basic operational alternatives of continued power operation and shutdown

7.2.3 Other Considerations in Defining Action Requirements

The risk profiles discussed above are based on several assumptions. An important assumption was that, in the case of the shutdown alternative, the plant is shut down directly after the failure is detected. However, in general, some AOT may be useful so that plant personnel can evaluate the repairs needed and restore the operability of the failed equipment without shutting down the plant, at least for short repairs.

Suppose that 3 days of AOT is given for a failure situation in the technical specifications and that the plant personnel cannot repair the component within the AOT. They may shut down the plant three days after finding the failure. In this case, the failure will incur LCO operating risk from the time the failure was detected until the shutdown is initiated, and also LCO shutdown risk. Compared to a plant shutdown right after the failure detection, this case will incur a larger risk by the risk accumulated before the plant is actually shut down. Hence, the timing of shutdown should be considered in determining risk-effective action requirements that will minimize the total risk impact associated with a given failure.

Furthermore, oftentimes we do not know exactly how long the repair of certain failures will take. The distribution of repair time should be considered in assessing the risk associated with the failures. In addition to the timing of shutdown and the repair time, other issues should be taken into account in determining risk-effective action requirements, e.g., whether the status of redundant train(s) should be checked, and whether the plant should go to hot shutdown or cold shutdown as the optimum target state. These issues can be addressed by sensitivity analyses, which we will discuss later.

7.3 Method for Evaluating LCO Operating and Shutdown Risks

We can evaluate the LCO operating and shutdown risks using typical PSA models, e.g., based on fault trees and event trees. Specifically, the LCO operating risk can be easily assessed by running a computerized PSA model for full-power operation, after appropriately modifying the unavailability of the failed equipment and adjusting the parameter for common-cause failure. This process of quantifying the LCO operating risk is the same as that of quantifying the risk for a downed component, discussed in Chapter 3 and Appendix B.

Quantifying the LCO shutdown risk will be greatly facilitated if a PSA for low-power and shutdown operations is available, such as for Surry (NUREG/CR-6144, 1994) or Grand Gulf (NUREG/CR-6143, 1994). However, these PSAs are available only for a few plants and, even then, the models are not computerized in a form that can be readily usable for TS applications.

A method, called risk-comparison approach, was developed in a study to analyze the action requirements for the residual heat removal and standby service water systems of a BWR (T. Mankamo et al., NUREG/CR-5995, 1993). This method can be used to evaluate and compare the LCO operating and shutdown risks; also, it can address the specific features useful in modeling and quantifying shutdown risk.

Here, we describe the risk-comparison approach to illustrate how the LCO operating and shutdown risks can be assessed. Figure 7.3 shows the main steps of the approach. The following are its salient features:

1. The risk-comparison approach uses shutdown transient diagrams (STDs) and extended event sequence diagrams (EESDs) to model accident sequences, as opposed to the event trees and fault trees typically used in PSAs. These tools for sequence-modeling evolved from the need to obtain time-dependent risk quantification in modeling shutdown-related transients, and in considering operational alternatives in failure situations of standby safety systems. The models incorporate initiators for various plant states, including shutdown phases, plant responses of safety systems, and risk-significant operator actions.

2. Using EESDs to model sequences involves explicit representation of success/failure paths, and recovery paths to each sequence of events. Modeling up to a system or subsystem level is adequate and also limits unnecessary complexity.

3. Systems are modularized by grouping components into functional blocks. An example of a typical module is an RHR pump train, including the pump, associated isolation valves, and the minimum-flow recirculation line.

4. Heatup and recovery scenarios are analyzed using a simplified heat transfer model to give credit to the diminishing level of decay heat when the plant is shut down.

5. The minimal cut sets from the STD and EESD models are reduced by retaining only the dominant contributors, supplemented by additional minimal cut sets such that all initiating events modeled are represented.

6. The quantification of sequences is based on transition rates from one plant/system state to another (expressed as probabilities per unit of time). This feature is connected to the use of EESDs for event sequence modeling, which incorporates plant states. This approach incorporates various time-

dependent aspects, such as functional or operational dependencies on the actual state of the plant, and on previous scenarios of events.

7. The risk measures, such as conditional core-damage frequency or core-damage probability, can be evaluated for alternatives of continued power operation and plant shutdown. Sensitivity analyses can address issues like the timing of shutdown or the additional test requirements.

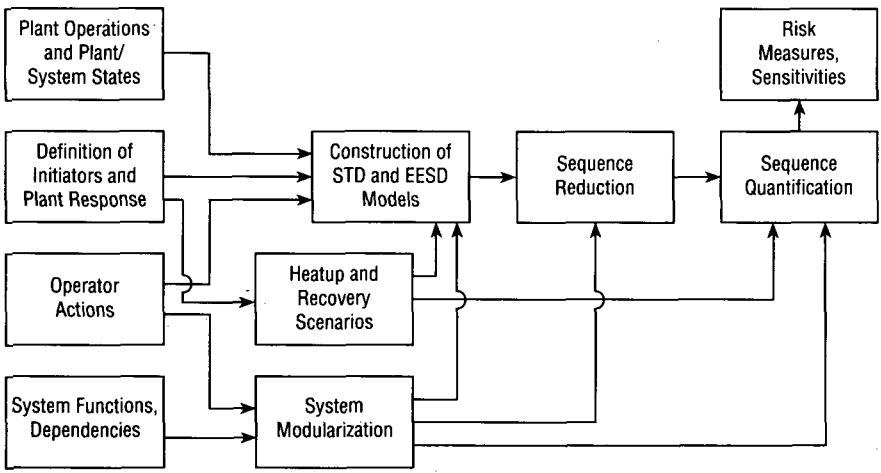

Figure 7.3 Main steps of the risk-comparison approach

In the remainder of this section, we discuss this approach in more detail, especially compared to the typical event tree-fault tree approach of PSAs. Section 7.4 give an example of its application focussing on deriving the risk-based insights to improve action requirements.

7.3.1 Shutdown Transient Diagrams and Extended Event Sequence Diagrams

Shutdown transient diagrams (STDs) are used at the highest level of the modeling hierarchy to describe:

- Initiating events for power operation state
- Disturbance transients during a controlled shutdown

The subsequent events or plant states are represented in the STDs until the initiating events of shutdown cooling are reached, which require the removal of decay heat from the reactor.

The extended event-sequence diagrams (EESDs) are used to model the phased missions and event sequences of plant response to those initiating events of shutdown cooling. The event sequences in the EESDs end with undesirable states of the plant, called near-mission failure states. Such states are those where critical safety functions are lost and an undesired core damage will occur if the recovery measures fail.

The EESDs primarily describe operational states, dependencies, and preferences of equipment operation. The connection with plant hardware is made through Boolean expressions, which describe how the functional entities are realized by system modules. Components are grouped into functional blocks called modules that are basic entities in the reduced block diagrams used for system modeling.

The core-damage frequency is estimated from the event sequences, derived from the STDs and EESDs, using the initiator and transient frequencies and unavailability estimates from the system modules. This quantification is made by considering those relevant factors, such as the diminishing level of decay heat, the resulting time-margin available for recovery, or the possibility of repairing the failures which caused the LCO shutdown.

7.3.2 Heatup and Recovery Scenarios

The risk of shutting down is evaluated accounting for the diminishing level of decay heat following a reactor shutdown. As the decay heat decreases, the time margin to recover from near-mission failure states increases.

This time margin available for recovery is called heatup time, which depends on the delaying buffers, such as the remaining water in the reactor or the subcooling margin of the suppression pool in a BWR, or the dry-out time of steam generators in a PWR. The relative importance of these delaying buffers depends on the specific event sequence.

7.3.3 Basic Formulas for the Risk-Comparison Measures

Let

r_{CO} = the core-damage probability associated with continued power operation over the downtime of the failed equipment

R_{CO} = the increased core-damage frequency associated with continued power operation with the failed equipment

$\bar{d}$ = the mean downtime

Then, the risk of continued power operation can be assessed similarly to the single-event AOT risk defined in Chapter 3:

$$r_{CO} = R_{CO} \cdot \bar{d} \tag{7.1}$$

Here, we measure R_{CO} in terms of the increased CDF, and not the increase in CDF, as used in Chapter 3. Both the shutdown risk and the continued power-operation risk are measured in terms of the increased CDF to provide a basis for comparison.

The expected probability of core damage for the shutdown alternative, r_{SD}, can be obtained as

$$r_{SD} = \sum_i P_{IE\text{-}i/SD} \cdot r_{SD/IE\text{-}i} \tag{7.2}$$

where the summation is over all initiating events, and

$P_{IE\text{-}i/SD}$ = the probability that the initiating event i will occur during the transition to shutdown,

$r_{SD/IE\text{-}i}$ = the conditional probability of core damage for the initiating event i requiring shutdown cooling.

We can evaluate the conditional probability of core damage for the initiator IE-i as follows:

$$r_{SD/IE\text{-}i} = r_{SD\text{-}0/IE\text{-}i} + \int_{t=o}^{\infty} dt \cdot R_{SD/IE\text{-}i}(t) \cdot P_d(t) \tag{7.3}$$

where

$r_{SD\text{-}0/IE\text{-}i}$ = the conditional probability of core damage at the start of shutdown cooling for the initiator i,

$R_{SD/IE\text{-}i}(t)$ = the conditional core-damage frequency during shutdown cooling at time t for the initiator i, and

$P_d(t)$ = the probability that the component is down at time t (i.e., probability that repair is not completed by time t).

In these expressions, the CDF for a given initiating event of shutdown cooling, $R_{SD/IE\text{-}i}(t)$, as well as the risk variables, r_{CO}, r_{SD}, R_{CO} are all conditional on a given failure. However, for simplicity, the failure condition is not explicitly indicated in the expressions.

7.3.4 Alternative Formula for the Risk of Shutdown

We can approximate the probability of core damage for the shutdown alternative, r_{SD}, by first dividing the shutdown into several phases. For instance, the plant shutdown state may be separated into three phases: 1) power reduction (phase 1) from full power until the reactor becomes subcritical, 2) reactor cooldown (phase 2) subsequently from 0% power until the shutdown cooling system, such as the residual heat removal system, can be used, and 3) shutdown cooling (phase 3) where the shutdown cooling system is used to remove decay heat.

Let

$r_{SD\text{-}0}(1\rightarrow2)$ = the conditional probability of core damage associated with the change in plant's state from phase 1 to phase 2

$r_{SD\text{-}0}(2\rightarrow3)$ = the conditional probability of core damage associated with the change in plant's state from phase 2 to phase 3

As an example, $r_{SD\text{-}0}(1\rightarrow2)$ includes the contribution to CDP from potential disconnection of external grid triggered by a turbine trip. $r_{SD\text{-}0}(2\rightarrow3)$ encompasses the risk associated with the failure to start the shutdown cooling systems, or errors in the system's alignment, if relevant.

Then, the probability of core damage for the shutdown alternative, r_{SD}, can be assessed by

$$r_{SD} = R_{SD}(1) \cdot \bar{t}_1 + r_{SD\text{-}0}(1\rightarrow2) + R_{SD}(2) \cdot \bar{t}_2 + r_{SD\text{-}0}(2\rightarrow3) + R_{SD}(3) \cdot \bar{t}_3 \quad (7.4)$$

where,

$R_{SD}(k)$ = the core-damage frequency during phase k (k = 1, 2, or 3)

$\bar{t}_k$ = the mean duration of phase k (k = 1, 2, or 3)

$R_{SD}(1)$, $R_{SD}(2)$, and $R_{SD}(3)$ represent the average CDF over each phase, conditional upon the given failure situation. If a computerized PSA model for low-power and shutdown is available, then these CDFs can be easily assessed after adequately changing the unavailability of the inoperable equipment.

7.3.5 Risk Quantification for the Basic Operational Alternatives

The quantification can be performed first for the basic operational alternatives of continued power operation (CO) and shutdown (SD), under the following nominal assumptions:

1. In the SD alternative, the controlled shutdown is undertaken directly after the fault is detected.

2. The repairs of the detected fault or multiple faults independently progress during shutdown operations.

3. The target state of the LCO shutdown is the cold shutdown state.

4. Other redundant trains are tested operable and returned into standby.

The influences of the variation in these various aspects can be analyzed as a sensitivity analysis.

7.3.6 Sensitivity Analysis to Identify Operational Policy Alternatives

For LCOs on systems that are required for shutting down the plant, the major decision is the choice between continued power operation and transition to shutdown. Instead of simply requiring shutdown when an AOT is exceeded, the action statements for such a condition may provide more detailed operational guidelines to assure better control of the risk.

The following questions suggest those operational policy alternatives that we may need to consider:

a) Should redundant trains undergo additional testing or inspection to identify multiple failures immediately, or to identify an available success path so that a sufficient AOT can be provided to complete repairs without incurring undue risk due to continued operation?

b) Is it important for risk to assure the availability of other systems and components through testing or inspection to minimize the risk of the continued power operation?

c) Should an early portion of the AOT be used to decide between shutdown and continued operation to control the total risk?

d) When a decision to transfer to the shutdown mode has been made, should operations proceed quickly to an operational state where alternate systems for decay-heat removal can be used, or should the plant stay in hot shutdown to complete the repair?

e) When a decision to transfer to shutdown mode has been made, should plant personnel postpone any repairs until a stable shutdown state is achieved?

Answering these questions helps to define action statements that will improve the safety significance of the Technical Specification. The risk-comparison approach we discussed here can be used to evaluate these policy alternatives.

7.3.7 Data Needs for Evaluating Action Statements Requiring Shutdown

Data available in a PSA for full-power operation provide the basic data for evaluating the risks of continued power operation and plant shutdown. In addition, the PSA for low-power and shutdown operations, if available, will significantly ease the acquisition of the data necessary to implement the risk-comparison approach, especially the evaluation of the risk of shutdown. The low-power and shutdown PSA typically include data, such as the durations of shutdown phases, and the frequencies of initiators that may occur during shutdown operation, e.g., loss of residual heat-removal.

The full-power PSA may be available for most operating plants, but the low-power and shutdown PSA may be available only for some plants, such as Grand Gulf and Surry. Hence, the data needed to evaluate action statements are discussed here, assuming that data from a full-power PSA only are available:

1. Plant-specific data on shutdown operations: To analyze shutdown phases in detail, plant-specific information may be needed, such as operating and abnormal procedures, shift supervisor's log books, or monthly operating reports. From this information, we can extract data useful for the analysis, such as timing of the plant shutdown, operational preferences of equipment during plant shutdown, or distribution of repair-time for the system analyzed. For a crude analysis, the data from a low-power and shutdown PSA for a similar type of plant could be used.

2. Plant-specific physical data: The evaluation of heatup and recovery scenarios, including estimates of heatup time, requires some physical data on the plant, such as the temperature of the ultimate heat sink, or the cooling capacity of the RHR system. These data typically are available from the plant's final safety analysis report (FSAR).

3. Frequency of disturbance transients during controlled shutdown: A review of the licensee event reports (LERs) for the plant may be needed to evaluate some items, such as the likelihood of disturbance transients during controlled shutdown. This likelihood plays an important role in evaluating the risk for a controlled shutdown, thereby affecting its comparison with the risk for continued operation.

7.4 Example Application to Standby Service Water System

The method for evaluating LCO operating and shutdown risks, called risk-comparison approach, was applied to the standby service water (SSW) system of a BWR. The event sequences were modeled using STDs and EESDs, particularly focussing on the transients that may occur during the transition to shutdown.

In this section, we present the results of quantifying the LCO operating and shutdown risks for failures in the SSW system, after briefly introducing the system and the present action requirements. We then summarize the practical insights from these analyses to control the risk implications of such failures. There is a detailed description of the sequence modeling and sensitivity analyses in NUREG/CR-5995 (T. Mankamo et al., 1993).

7.4.1 Standby Service Water System and Present Action Requirements

The SSW system, consisting of three subsystems, A, B, and C, removes heat from plant equipment that require cooling water for a safe reactor shutdown. SSW pumps A and B each has a 12,000 gpm capacity, while SSW pump C, dedicated to the high pressure core spray (HPCS) system, has a much smaller (1,300 gpm) capacity.

The SSW subsystems, especially A and B, provide cooling water to many safety-significant components, such as the heat exchangers of the RHR system, room/pump coolers for the low-pressure core-spray (LPCS) and reactor-core-isolation cooling (RCIC) systems, and jacket coolers of diesel generators. Hence, a failure or degradation in the SSW system will affect the operability of other systems which are supported by the SSW system. For example, the failure of SSW subsystem A also will cause RHR subsystem A and DG subsystem A to be inoperable along with front-line systems, LPCS and RCIC.

Table 7.1 summarizes the action requirements for the SSW system which are applicable to the power operation mode. For a single failure, i.e., when SSW subsystem A, B, or C is inoperable, the TS allows 3 days; if the operability of the failed subsystem cannot be restored within 3 days, then the plant must be shut down.

Table 7.1 Action Requirements for the SSW System

Inoperable SSW Subsystems	AOT
A or B or C	3 days
"A and C" or "B and C"	3 days
A and B[a]	0 hours
A, B, and C[a]	0 hours

[a]Whenever both SSW subsystems (A and B) are inoperable, if cold shutdown cannot be attained as required by this action, the reactor's coolant temperature should be kept as low as practical by using alternate methods of heat removal.

For double failures of the SSW system, the TS gives different AOTs, depending on which subsystems are inoperable. When SSW trains A and C, or B and C are down, the plant may continue power operation with the equipment inoperable up to 3 days; namely, these double failures have the same AOT as the single failures.

When SSW subsystems A and B, or all SSW subsystems (triple failures) are inoperable, the TS requires "immediate" plant shutdown (0 hours of AOT). Then, the TS also limits the timing of shutdown so that the plant at least should be in hot shutdown within the next 12 hours, and in cold shutdown within the following 24 hours.

7.4.2 Risk Comparison of the Basic Operational Alternatives

Table 7.2 gives the LCO operating and shutdown risks for failures in the SSW system. Figures 7.4 and 7.5 show how the conditional core-damage frequency and core-damage probability change for the continued power operation (CO) and shutdown (SD) alternatives in single, double, and triple failures of the SSW system.

Table 7.2 Risk Quantification for Failures in the SSW System

LCO State (Failures of SSW Trains)	Core-Damage Frequency in Power Operation State (per year)	CDF Increase Factor	Crossing Point of the SD/CO Alternatives (days)
Baseline	2.1E-6	1.0	N/A
Single (A)	1.5E-5	7.4	~3
Double (AB)	3.3E-4	160	~3
Triple (ABC)	7.4E-3	3600	~14

Core-Damage Probability per Failure Situation		
Continued Operation (CO)	Controlled Shutdown (SD)	CDP Ratio (SD/CO)
N/A	N/A	N/A
2.3E-8	5.7E-8	2.5
4.5E-7	9.6E-7	2.1
1.1E-5	3.3E-5	3.0

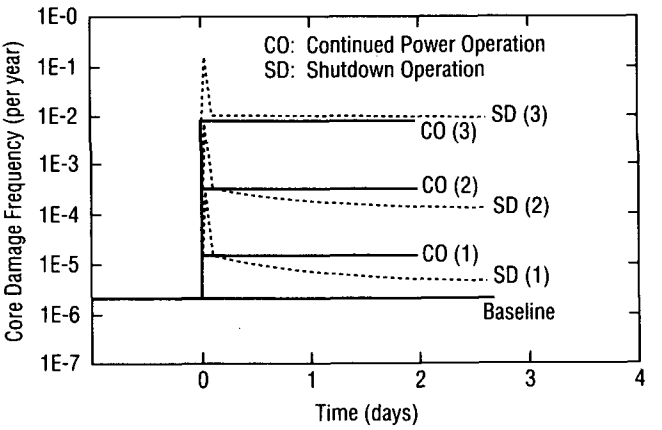

Figure 7.4 Conditional core-damage frequency for the continued operation and shutdown alternatives in failures of the SSW system (For example, CO(2) denotes the CO alternative for double-train failures)

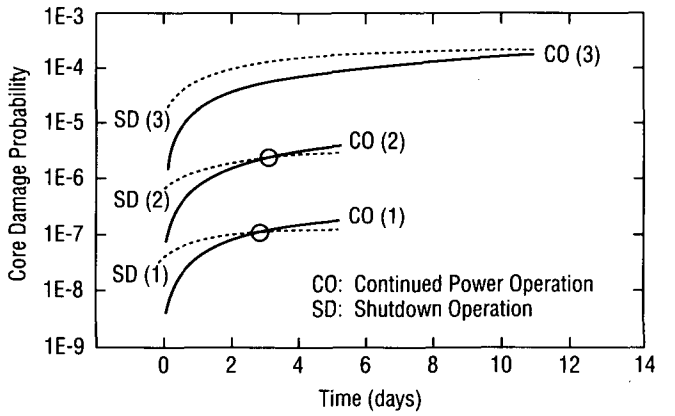

Figure 7.5 Cumulative core-damage probability over predicted repair time in failures of the SSW system (For example, SD(2) denotes the SD alternative for double-train failures)

1. Single-Failure Situation: Where one SSW train (e.g., train A) is detected failed during power operation, the core-damage frequency increases by a factor of about 7 over the baseline (see, Table 7.2). If the CO alternative is taken, the core-damage frequency will remain at this level until the operability of the failed train is restored. If the SD alternative is taken (directly after detecting the failure), then the plant temporarily will have higher CDF than the operating CDF during the initial transition period of power reduction and state changes. However, after this initial increase, the CDF slowly declines, resulting in a smaller and smaller CDF compared to the operating CDF. The estimate of CDP over time indicates that the risk of continued operation is smaller than that for shutdown until about 3 days (see, Figure 7.5).

2. Double-Failure Situation: When two SSW trains (e.g., trains A and B) are detected failed, the CDF profiles for both CO and SD alternatives are similar to those in a single failure, except that the CDF is increased by a factor of 160 over the baseline. Figure 7.5 shows that the CDPs for CO and SD alternatives again intersect at about 3 days.

3. Triple-Failure Situation: Where all the three SSW trains are detected failed, the conditional CDF dramatically increases by a factor of about 3600 over the baseline. However, in contrast to single-and double-failures, for several days CDF remains higher than for the CO alternative. The intersection of the CDPs occurs about 14 days after shutdown.

Figure 7.4 compares the SD risk profile for triple failures, with those for single and double failures. When all SSW trains are inoperable, the plant becomes vulnerable to loss of offsite power and loss of instrument air system initiating events, during shutdown as well as during power operation because of the resulting loss of the power conversion system and lack of major means to remove decay heat. In addition, these initiators have a higher frequency in shutdown states than in power operation state. As a consequence, the CDF remains high in the cold shutdown state, and the CDPs for the two alternatives cross at a long predicted repair time, i.e., 14 days (Figure 7.5).

Table 7.2 summarizes the results of this case study for failures in the SSW system of the BWR. These results include: 1) the CDF in the power operation state, 2) the increase in CDF for the continued-operation alternative, 3) the crossing point of the core-damage probabilities for the shutdown and continued power operation (SD/CO) alternatives, and 4) the expected core-damage probability for different failure situation in SD/CO alternatives along with the ratio between these probabilities. In particular, the ratio of the CDPs for SD/CO alternatives indicates that the SD alternative is unfavorable in all three failures of the SSW system.

7.4.3 LCO Recommendations for the Specific Example Analyzed

The risk-comparison analysis of failures in the SSW system of the particular plant resulted in the following recommendations:

1. The present AOT requirement for a single SSW-train failure is 3 days. This AOT may remain the same with the additional condition that, by the end of the first day, redundant trains are tested to assure that there are no additional failures. If the repair of the initial failure is completed within the first day, then no additional tests are required. If feasible, any diagnostic measure that can determine the condition of the redundant train(s), should precede, or replace the need for, an actual demand test, particularly when the test may have adverse effects.

2. The SSW trains are tested relatively frequently during power operations because they are run for mixing chemical additives and to test other safety-system components. The recommendation to test redundant SSW train(s) should not result in unnecessary additional testing. This recommended test can be omitted if a successful test was performed recently, e.g., in the previous 72 hours, and if there is no clear indication of a common-cause failure.

3. The current LCOs distinguish among different double failures; for example, a 3-day AOT is given for failure of SSW trains A and C, and B and C, but shutdown is required for failure of SSW trains A and B. Similarly, shutdown is required for failure of all three SSW trains. This study recommends 2 days of AOT for double- and triple-failures in the SSW system. With this change, the AOT for all double failures in the SSW system will be the same. This recommendation is justified because the impacts on core-damage frequency of different double-failure combinations are similar.

   In using this 2 days of AOT for double- and triple-failures in the SSW system, a decision needs to be made at the end of the first day whether one of the trains can be completely repaired by the end of the second day. If, by then, it is judged that this cannot be accomplished, then shutdown should be initiated immediately to avoid accumulating risk during power operation.

4. For multiple failures, if the repair time is expected to exceed 2 days, then shutdown should be initiated at the end of the first day, and cold shutdown should be reached within the next 12 hours. The time to reach cold shutdown differs from that currently allowed (12 hours to reach hot

shutdown, and 24 hours to reach cold shutdown), because here, to minimize the risk impact, an orderly cold shutdown should be achieved without delay.

7.5 General Recommendations for Risk-Based Action Statements

The risk-comparison approach discussed thus far also was applied to the auxiliary feedwater system of a PWR. Figure 7.6 graphically represents the general recommendations drawn from these studies to improve the action statements from a risk perspective:

1. The use of an AOT may be defined in the following manner. The initial portion of the AOT can be used to complete short repairs. For longer repairs, the needed repair time is assessed within the first phase of the AOT. If it is considered longer than the AOT, then shutdown can be initiated to minimize the accumulation of risk during power operation with such a failure. To identify the situation more clearly, especially where common-cause failures are suspected, additional tests of redundant train(s) may be conducted. Then, the applicable AOT should be followed, depending on the outcome of the test.

2. In the case of multiple failures, an AOT should be provided to allow at least one of the failed trains to be restored to operable status. As for a single failure, multiple failures also should have an AOT. This differs from some current TS requirements of immediate shutdown when multiple failures are detected. However, the AOT for multiple failures should be shorter than that for single failures.

3. Assessment of risk impact of staying in a particular mode (e.g., hot shutdown versus cold shutdown) can be used to decide on the applicable mode to be reached when a decision is made to shut down the plant. For example, in a BWR, the conditional CDF of staying in hot shutdown may be high compared to cold shutdown; if so, cold shutdown should be reached without delay.

4. If small risk is incurred, especially for continuing power operation, then the TS requirements can be relatively simple and flexible.

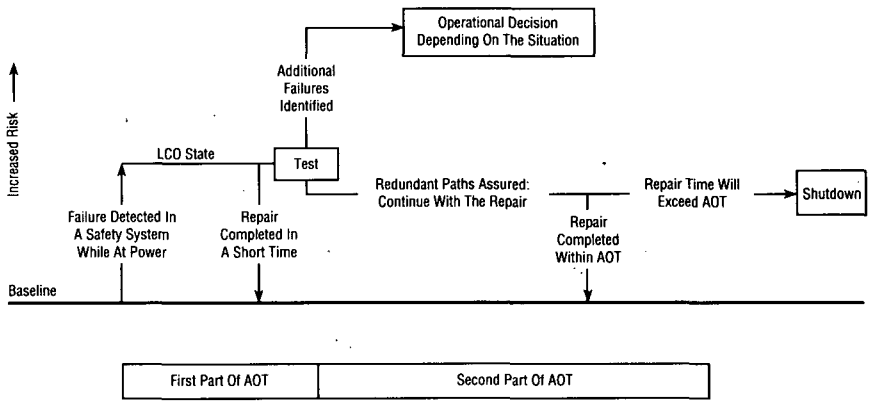

Figure 7.6 Recommendations for risk-based action requirements

There are several practical points that also should be taken into account in considering possible changes in the action requirements:

1. If an AOT is defined, it must be sufficiently long to complete a large percentage (e.g., ~90%) of repair needs; this will avoid any adverse effects of incomplete or hurried repairs.

2. The AOTs chosen should follow discrete values normally used in Technical Specifications such as 1 day, 2 days, 3 days, or 7 days, for ease of implementation.

3. Care should be taken that the relative risk-comparison of the operation alternatives is not the only factor in defining the action requirements. If mechanically followed, this approach could result in longer AOTs for multiple failures, thus possibly providing incentives to declare multiple failures when repairs for single failures cannot be completed within the prescribed AOT.

4. When AOTs for multiple failures are defined in TS, it implies that, when one failure is repaired, the action for the remaining fewer failures needs to be followed. There is a significant risk advantage to promptly repairing one of the failures in the case of multiple failures. In principle, AOTs should reflect this risk perspective, where possible, by consistently defining longer AOTs for fewer failures.

5. The requirement for additional testing of a redundant train should consider its adverse effects. If feasible, any diagnostic measure that can determine the condition of the redundant train should precede or replace the need for an actual demand test. In the special case where testing the redundant trains involves substantial adverse effects, then it may be more beneficial not to do so.

8. MANAGING PLANT CONFIGURATION

Basic Concepts

Configuration or Downed-Configuration: Configuration is a state of the plant and is defined by the status of components. Multiple components which are simultaneously down is called a downed-configuration or simply, a configuration.

Configuration Risk: Configuration is the risk associated with a specific configuration or from occurrences of configuration during plant operation. The configuration risk, measured in terms of core-damage frequency, include the increase in CDF caused by a configuration, the increase in CDP for a given occurrence of a configuration, and the increase in CDP from occurrences of configuration in a given time period.

Managing Back-Up Components: This involves knowing the components which can carry out the functions as those which are down.

Managing Configuration Frequency: This involves tracking frequency at which configuration occurs and modifying procedures and testing to control the occurrences, as necessary and feasible.

Managing Downed Components: This involves scheduling maintenances and tests so that critical combinations of components are not down at the same time.

Managing Outage Time: This involves knowing how long a configuration exists before the risk incurred becomes significant. It also involves knowledge of the alternatives that can extend the time without increasing the risk.

Managing Plant Configurations: The management of plant configuration involves specific measures to avoid occurrences of risk-significant or critical configuration. When PSAs are directly used, it is sometimes called risk-based management of plant configuration or risk-based configuration control.

Risk-Significant or Critical Configuration: The risk-significant or critical configurations are those combinations of components which when down cause large increase in the risk measure, e.g., CDF.

Outline of the Chapter

List of Symbols

d downtime during which the configuration exists.

f_c frequency of occurrence of the configuration.

r the risk impact from the occurrence of a given configuration, measured in terms of the core-damage probability increase. Similar to single-event AOT risk, but addressing statuses of multiple components.

ΔR increase in core-damage frequency, caused by a configuration.

R_t expected increase in core-damage probability, due to occurrences of configurations over t.

In previous chapters, we discussed the risk-based analyses of AOTs and SRs and approaches to define/modify these requirements using such analyses. In these approaches, we primarily focussed on analyzing a single component, or a single train of components within a safety system, at a time. However, during the operation of a nuclear power plant, multiple components across systems may simultaneously be unavailable, disabling multiple trains of different safety systems. A safety system train or component may be unavailable because of failure, maintenance, or testing. An assembly of multiple components downed at the same time is called downed-configuration, or simply, the configuration. In this chapter, we discuss risk-based analyses of plant configurations in defining TS requirements, and also, management of these configurations to assure safety during operation.

This concept of managing or controlling plant configuration using risk-based methods encompasses many aspects of the TS and integrates many different requirements in a cohesive manner. With the advances in the computational tools and PSA methods, this approach is increasingly attractive and many think that similar approaches will be used in operating nuclear power plants in the future. As discussed here, these approaches have strong interfaces with TS and have the potential to streamline both the requirements and their implementation during plant operation.†

8.1 Definitions and Issues in Managing Plant Configurations

As defined here, a configuration is a state of the plant and is defined by the status of the components. The configuration of a plant also is defined by what the status of the systems and safety function are, which, in turn, depend upon the components' status. The components' statuses are defined in terms of the functional statuses, i.e., the component is operational (up-state), or not (down-state). Since we are primarily dealing with standby safety system components, a component is in down-state when it is detected to be failed in a surveillance test or is taken down for maintenance or testing. It is in up-state, when it has just been successfully tested or is operating following a demand. In most cases, the component is in standby where its condition can be detected by a test or a demand.

During power operation and plant shutdown, the statuses of the components change, and hence, the system statuses and plant configuration change. The plant configuration impacts the plant's risk because the protection provided by a component is lost when it is down. If design or procedural changes are instituted in the plant, then these will cause the components' statuses to have different effect on the system statuses and on plant risk. The management of plant configuration becomes difficult because the status of a standby component often is not apparent unless it is tested.

A plant configuration involving simultaneous outages of multiple components can imply significant risk. In the language of PSA, the core-damage frequency can be significantly higher when multiple components are unavailable, i.e., when their functions are lost. Control of plant configuration resulting from component unavailability is important because all plant risks, all accidents and incidents, and all accident precursors arise because specific configurations have occurred. If configurations are managed so that critical, high-risk ones do not occur, then risk from plant operation would be small, and no accident or incident would occur.

---

†The term configuration control or configuration management here relates to the control of component/system availability and unavailability and is not concerned with configuration control or configuration management interpreted as accurate/up-to-date recording of system drawing and the control of system modifications.

The LCOs in TS contribute to the management of plant configurations in the following ways:

a) assuring that repair of individual component failure is performed in the allotted period, i.e., within the defined AOT for individual failures,

b) requiring that the plant be shutdown for failure of redundant trains within a safety system.

Many other combinations of component outages are not explicitly addressed in the TS which imply that simultaneous outages of these combinations are not forbidden. Typically, these combinations can result from outages of components in different safety systems. For example, simultaneous outage of an auxiliary feedwater (AFW) pump and a valve in the low pressure injection system (LPIS) is not forbidden by the TS. Simultaneous outages can occur due to various reasons:

- failures of multiple components requiring repair,
- scheduled preventive maintenance of multiple components,
- component outage due to a required surveillance test, and scheduled maintenance or failure of other components,
- combinations resulting from testing, maintenance, and failure of components.

Unless specific measures are taken, because of the many test and maintenance activities carried out at a plant, simultaneous outages of multiple components are likely. Realizing that simultaneous outages cannot be completely avoided, the management of plant configuration can help to avoid the occurrence of risk-significant configurations. Specifically, by identifying risk-significant configurations, precautions can be taken such that deliberate actions, e.g., test and maintenance, do not contribute to their occurrence. At the same time, configurations with minimal risk implications can be allowed when it is advantageous for carrying out test and maintenance.

8.2 Areas of Application

Probabilistic safety assessments (PSAs) provide an effective tool to identify the risk implications of plant configurations, i.e., the CDF of a plant due to outages of safety-system components. This tool also can identify the risk-significant configurations so that measures are taken to avoid or reduce the likelihood of their occurrence.

The evaluation of risks associated with plant configuration and their management are considered in the following areas:

- Scheduling of Preventive Maintenance: In many cases, preventive maintenance (PM) are routinely performed during power operation of a nuclear power plant where multiple components are simultaneously taken out-of-service. PSAs can be used to assess the risk implication of the PM schedules and decide on an acceptable schedule where large peaks in risk are avoided. Scheduling of PM was discussed in detail in Chapter 4.

- Extensions of AOTs: When extensions to AOTs are considered, there is an increased likelihood that because of them, multiple components may be simultaneously unavailable. The risk implications of likely combinations of components for which AOTs may be extended can be assessed to assure that the probability remains low of having large CDF peaks from plant configurations as a result of these extensions.

- Control of Risk-Significant Plant Configurations: In general, PSAs can be used to identify specific risk-significant configurations so that plant activities, e.g., tests and maintenance, are designed or organized such that these configurations are avoided. This type of evaluation can have three uses. First, specific plant configurations with risk implications, not forbidden in the TS, can be identified, and LCO action requirements, e.g., plant shutdown, can be defined. Second, a hierarchy of important plant configurations can be defined for personnel involved in carrying out test and maintenance activities, and third, relaxed requirements can apply for those configurations forbidden in TS but which have low risk impact.

8.3 Method for Analyzing Risk Due to Plant Configurations

The risk associated with a plant configuration resulting from simultaneous outages of multiple components is similar to that associated with the outage of a single component, i.e., the AOT risk measures discussed in Chapter 3.

In analyzing risk from plant configurations, the statuses of the components are of interest. Component states consist of the downed state in which the component is unavailable (has an unavailability equal to 1), the up-state in which the component is available (has an unavailability equal to 0), and intermediate states, in which the component has an intermediate unavailability value between 0 and 1. Here, the principal interest is in measuring the risk associated with downed configuration, because they imply large increases from baseline risk. However, when a redundant component is tested to be available, then the risk impact maybe lower, and the calculation of risk should account for this effect.

An example of a downed configuration is: pump A down because of repair, diesel B down because it is undergoing corrective maintenance, and valve A down because it is in a closed position and the operating position is the open one. In this sense, the interest is not on accurately assessing all configurations resulting from the up and down states of components, but rather those with large risk implications.

Risk Measures of Plant Configuration

Similar to AOT risk analyses, three risk measures are associated with a plant configuration. Measured in terms of core-damage frequency of a nuclear power plant, they are:

ΔR = the increase in core-damage frequency (CDF) caused by the configuration, given that the configuration exists, which includes components that are tested to be available,

r = the core-damage probability increase from the occurrence of a given configuration (single CDP contribution), and

R_t = the accumulated core-damage probability increase over some period t (time-period CDP contribution).

These measures are expressed in terms of two additional factors:

f_c = the frequency of occurrence of the configuration

d = the downtime during which the configuration exists

The single core-damage probability (CDP) contribution, r, is simply the product of the CDF increase, ΔR, and the downtime d.

$$r = \Delta R \cdot d \tag{8.1}$$

The increase in time-period core-damage probability R_t from a configuration also is simply expressed as a product:

$$R_t = f_c \cdot t \cdot \Delta R \cdot d \tag{8.2}$$

= expected increase in core-damage probability over time, t, due to occurrences of frequency, f_c, and duration, d.

Compared to r, R_t contains the extra factors $f_c t$, which gives the number of times the configuration is expected to occur in a period t. Thus, R_t is the increase

in core-damage probability from all occurrences of the configuration in period t. Since $f_c t$ can be smaller or larger than one, R_t can be smaller or larger than r.

The differences among the three risk perspectives associated with configurations are illustrated in the figures below. Figure 8.1 is a differential representation of the increase in the core-damage frequency, ΔR, over the baseline core-damage frequency level for the duration, d, that the configuration exists. The single-event contribution to core-damage probability, r, also is represented by the rectangular area (the product of core-damage frequency increase ΔR and the downtime d). To include the frequency of occurrence of a configuration, Figure 8.2 shows repeat occurrences of a particular configuration in an observation period. The pointwise increase in the core-damage frequency is the same in all cases, and the downtime in all cases was assumed to be the same.

While a nuclear power plant is operating, the same or different configuration will occur over time. Figure 8.3 depicts the pointwise core-damage frequency level due to occurrences of various configurations. The single core-damage probability contribution is represented by the shaded area in the figure. Figure 8.4 shows the time period core-damage probability contribution, R_t, obtained by combining the contributions of all occurrences of configurations. Different conditional CDF level signifies that different combination of components was down during the period.

Use of Different Configuration Risk Measures

To prioritize plant configurations in terms of their risk implication, the important measure is the conditional CDF increase ΔR, given that the configuration has occurred. The risk-significant configuration to be avoided during test and maintenance can be identified in terms of this measure; the other two measures, r and R_t, are not necessary for this application.

To identify an allowed period, similar to the AOT for single component downtime, the risk measure, r, is relevant, i.e., the single-event CDP contribution for the configuration. This measure can be used to define the period for which the configuration can be allowed to exist, i.e., within which period one of the component should be returned to service. This analysis is applicable for configurations where the conditional CDF increase ΔR is not large, but the integral impact can be significant if the configuration exists for long. The time-period CDF contribution, R_t, is expected to be very small since the frequency of occurrence of these configuration typically is small.

When measuring the overall trend of configuration risk in a plant, the measure R_t is applicable. If scheduled plant activity, e.g., routine preventive

maintenance, results in occurrences of different plant configurations through a year, then, along with the conditional CDF increase (ΔR), R_t should be calculated.

Calculation of Risk from Plant Configurations

To assess the configuration risks, the important calculation is the quantification of conditional CDF for which Standard PSA computer codes can be used.

The precautions necessary to calculate ΔR are similar to those discussed in the AOT risk analyses (Chapter 3 and Appendix B) to estimate the conditional CDF, given a component is down. For emphasis, we briefly discuss those points particularly relevant for calculating configuration risks.

To quantify the CDF for a given configuration, multiple component unavailabilities that give the plant configuration in question are set to the "True" state. These components may appear in the same minimal cut, causing a significant jump in the cutset frequency, i.e., a cutset with relatively small frequency can become a significant contributor to the CDF. Care should be taken to assure that cutset truncation does not eliminate cutsets that can be a significant contributor for a given configuration.

In this quantification, the boolean reduction process also can be very important. Otherwise, there may be significant overestimation. Also, the basic PSA first may need to be modified. PSAs contain the average contribution of maintenance downtime (based on the mean down time in a year), and correspondingly, the test downtimes based on the average time for a test. The contribution of maintenance and test downtime in the model should be reduced to zero because no additional components, other than those defining the configuration, are expected to be down. Care must be taken to exclude only the downtime contributions of the components in the model and not all others.

To evaluate the risk impact of configurations currently disallowed by the TS, the PSA model may need to be modified to include these combinations. PSAs take into account the TS requirements and deliberately remove these configurations from the model before accident sequences are quantified if they are disallowed by the TS.

Dependent or common-cause failure terms may require separate treatment. In many cases, this term is calculated separately and does not retain specific component designator. This term should be modified when one or more of the components included in this term is down. A separate calculation may be needed to revise the estimate of this term, corresponding to the configuration being quantified.

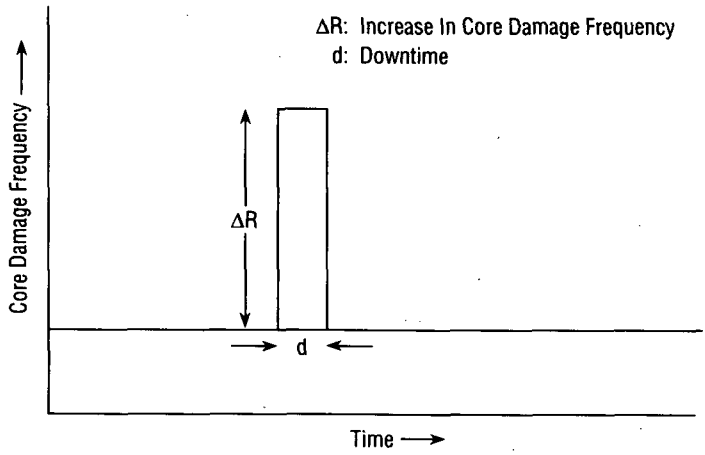

Figure 8.1 Illustration of the increase in core damage frequency due to downed-configuration

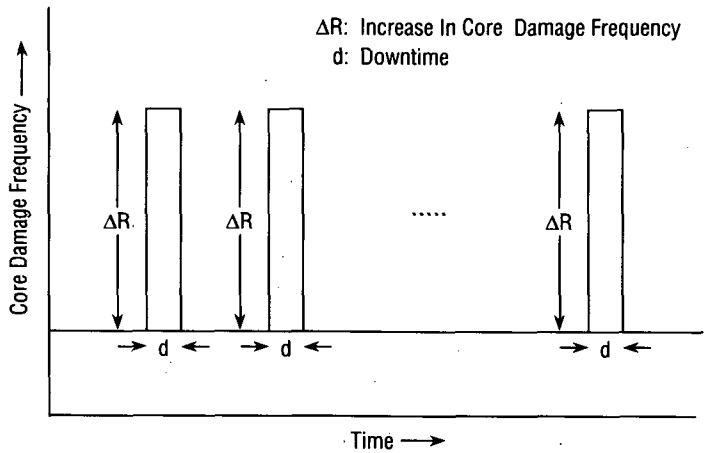

Figure 8.2 Illustration of increases in core damage frequency due to repeat occurrences of downed-configuration

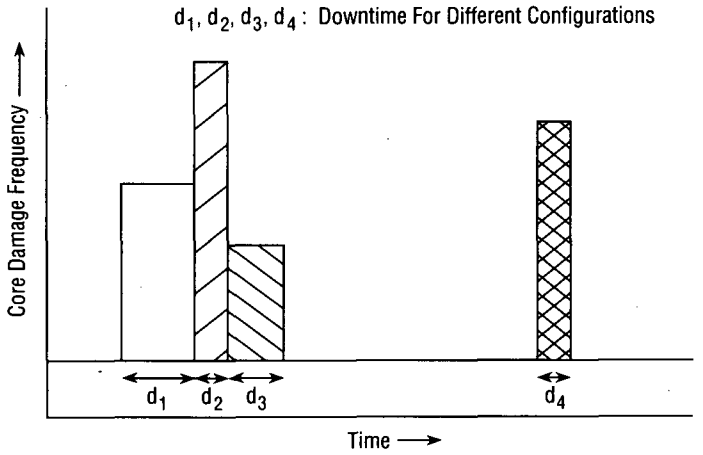

Figure 8.3 Illustration of configuration risk during operation of a nuclear power plant

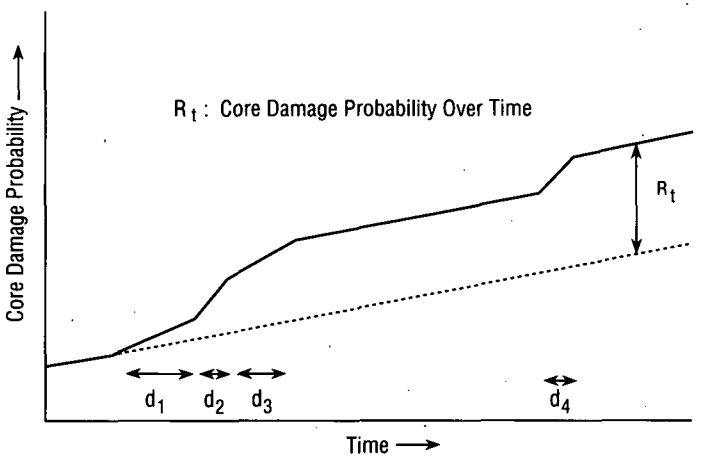

Figure 8.4 Representation of time period configuration risk during operation of a nuclear plant

8.4 Example Analysis of Configuration Risk at a Plant

Table 8.1 gives an example analysis of configuration risk. Here, we show selected outage configurations, CDF when these configurations occur, factor increase from the baseline CDF, and the single CDF contribution, r, for an AOT of 7 days. This sample was selected from a detailed analyses of various outage configurations at a plant (Samanta et al., NUREG/CR-5641). We use it to explain the management of plant configurations discussed earlier.

Some configurations can cause significant increases in the plant CDF. In this example, these configurations cause a CDF level greater than 1 x 10^{-3}/yr when they occur. During test and maintenance, it can be assured that these components are not deliberately taken out-of-service simultaneously. If feasible, specific plant actions can be defined for such configurations. Configurations in the next category do not necessarily have larger risk impact than some of the risk-significant components. It may be prudent to control the duration for which these configurations exist. For example, if these configurations occur emergency repairs may be required to be completed within one day. Other configurations with low risk impact can be controlled by the AOT of the individual component, and if necessary, may be candidates to be considered for allowing longer AOT providing operational flexibility during plant operation.

8.5 Strategy and Framework for a Risk-Based Configuration Control

PSAs provide the essential basis to achieve a risk-based configuration control at a nuclear power plant; so far, a full-scale risk-based configuration control has not yet been implemented. Here, we present a general framework which defines different aspects of such an approach.

We focus on the four factors which determine the risk impact or safety impact of a configuration:

1. the components which are simultaneously down,
2. the back-up components which are known to be up,
3. the duration of time the configuration exists (the outage time), and
4. the frequency at which the configuration occurs.

The first factor determines the loss of capability. The second factor determines the alternative components which are available to make up the lost capability. The third factor determines the integrated risk impact, and the last factor determines the accumulated risk impact which occurs from the configuration over time.

Table 8.1 Examples of High, Medium, and Low CDF-Impacting Configurations at a Plant

Outage Configuration	CDF ΔR(/yr.)	Factor Increase in CDF	CDP Contribution r (AOT = 7 days)
High CDF Impact			
Battery-B ESW-AV22 EHV-FAN-CV64	7.2E-3	851	1.4E-4
EHV-FAN-BV64 ESW-AV23	3.7E-3	443	7.1E-5
Battery-B DG-B	3.6E-3	428	7.0E-5
Medium CDF Impact			
HCI-TDP EHV-AV273-1	2.1E-4	25	4.0E-6
DG-C ESW-MV0841	1.2E-4	14.3	2.4E-6
CRD-MDP-B ESW-AV23	8.7E-5	10.4	1.7E-6
Low CDF Impact			
HCI-MV14 ESF-PISL-52A	1.1E-5	1.3	2.1E-7
RCI-MV132 ESW-MV0841 RCI-MV21	9.4E-6	1.1	1.8E-7
CRD-MDP-B	9.3E-6	1.1	1.8E-7

The four factors which determine the risk impact of a configuration may be simply summarized:

1. downed components,
2. back-up components,
3. outage time, and
4. frequency.

Configuration management involves managing these factors (Figure 8.5), called the focal points of configuration management. Figure 8.6 expands on each of the focal points which are discussed below, and Figure 8.7 gives various techniques to achieve these objectives.

Managing Downed Components

Managing downed components involves considering importance, scheduling, and testing. For importance considerations, management of the downed components involves knowing which combinations cause large risk impacts if they are down simultaneously. The critical combinations of components can be determined from the plant PSA or from plant logic schematics using risk considerations. The critical combinations basically are a function of the plant design.

Managing downed components also involves scheduling maintenances and tests so that critical combinations of components are not down at the same time. In preparing the surveillance schedules, or the master surveillance schedule, operational considerations and resource constraints are important; however, avoiding critical combinations also is an important objective.

When components are in standby, it is not always apparent which are down. When failures of components are discovered, then additional ones may need to be tested to assure that they are also not down, so forming a critical combination of downed components. Thus, management also may involve testing after failure to assure that there are no such critical configurations.

These test-after-failure considerations involve knowing which additional components, if also down, constitute a critical configuration. These additional components can be called critical complements, since they complement the already downed components to form critical configurations. Furthermore, test-after-failure considerations involve knowing whether tests of these complementing components are feasible and effective in determining their status.

In summary, management of downed components involves:

1. Knowledge of critical component combinations,

2. scheduling of maintenances and tests to avoid the critical combinations, and

3. knowledge of critical complementing components and effective tests which can be performed on them.

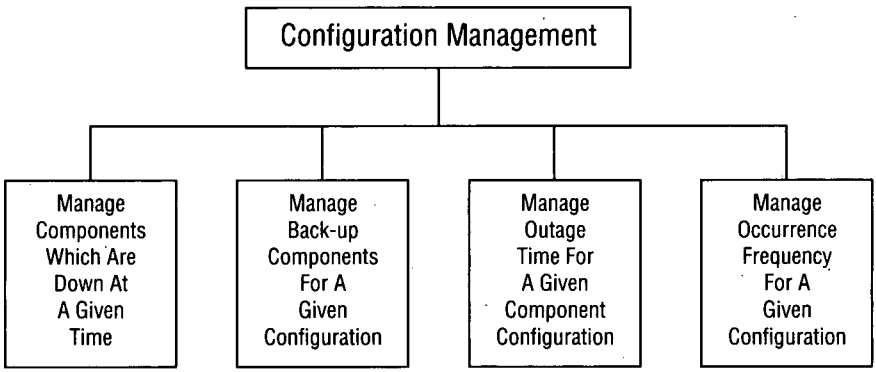

Figure 8.5 Basic focal points of configuration management

Managing Back-Up Components

Managing back-up components involves knowledge and testing considerations. To counter the loss of capability from components being down, other components can be checked to assure they are up. Management of back-up components involves knowing which components can carry out the same functions as those which are down. For a given configuration of downed components, the back-up components are determined from a PSA model or from a plant schematic, using risk considerations.

Management also involves knowing whether tests or inspections can be effectively performed on the back-up components to assure they are operational. This knowledge is obtained from plant operational and test considerations, as well as from considering reliability and risk.

Thus, management of back-up components involves:

1. Knowledge of the back-up components for given configurations of downed components, and

2. knowledge of effective tests which can assure the operation of the back-up components.

Managing Outage Time

Configuration management involves knowing how long a configuration can exist before the risk incurred becomes significant. Sometimes configurations cannot be avoided because of failures or of necessary corrective maintenances. Configuration management involves knowing how much time there is to complete the repairs or maintenances before the risk impact becomes significant.

The allowed outage time for a given configuration is an extension of the allowed outage times for individual components, as defined by TS. Configuration management involves determining allowed outage times for individual, and for configurations of downed components. Allowable outage times for multiple downed components can be quite different from those for single components because of their different impacts on risk. These allowable outage times should have a sound risk basis which not only controls risk but also reduces the burden by allowing larger outage times for unimportant configurations. All of these outage times can be determined from the plant PSA (or equivalent), taking into account the operational and resource considerations.

Management of outage times also involves knowing the alternatives that can extend the allowed outage time without increasing risk significantly. These alternatives can reduce burden when necessary and basically management involves effective testing of back-up components to assure they are up, where tests are effective.

Thus, the management of the duration of the configuration involves:

1. Knowledge of the allowed outage time for a configuration so that there is insignificant impact on risk, and

2. knowledge of the alternatives for extending the allowed outage time.

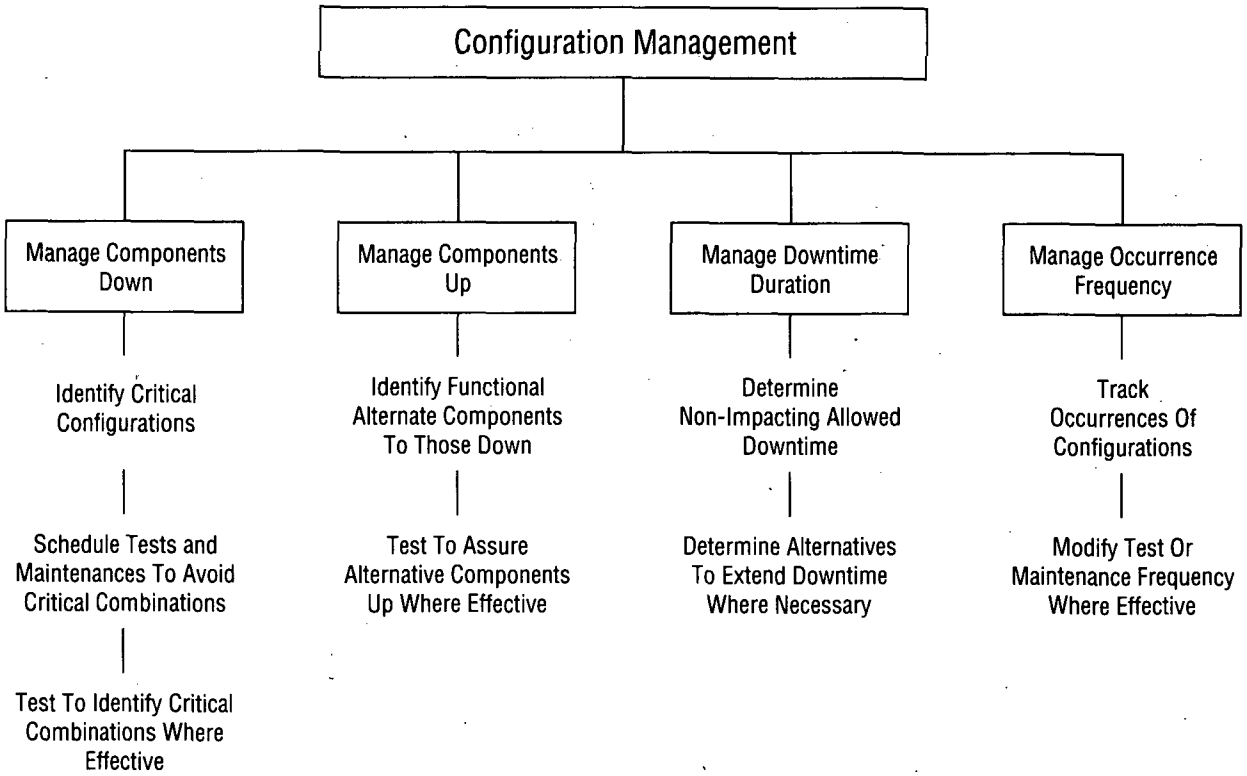

Figure 8.6 Focal points and subtopics of configuration management

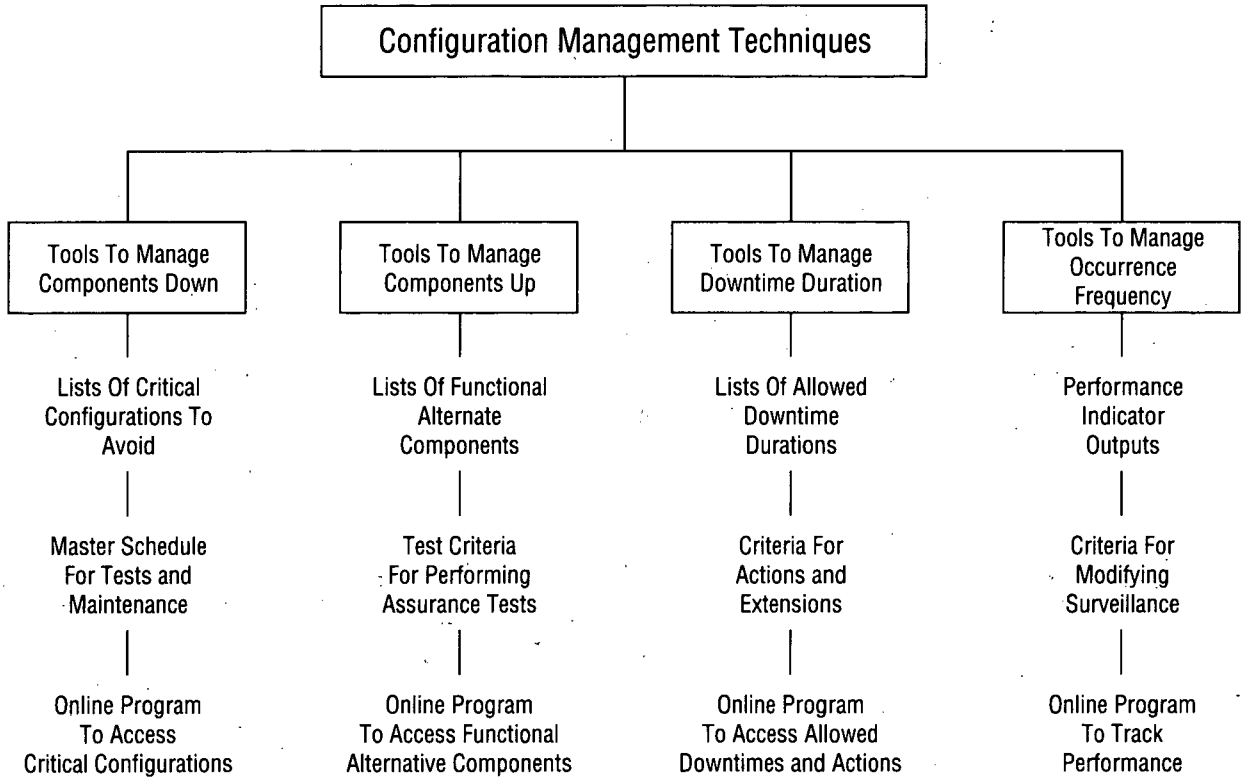

Figure 8.7 Techniques for configuration management

Managing Frequency

Finally, configuration management involves controlling the frequency at which configurations occur, especially risk significant ones. Controlling the frequency, in turn, involves tracking the occurrence of configurations, and modifying procedures and testing where necessary.

Tracking can be carried out through data collection and analyses, including the construction of appropriate indicators. Readjusting procedures and testing to modify the frequency involves having criteria, and identifying the relationships between the frequency and the testing and maintenance procedures. Modifying the procedures can involve either tightening or loosening the schedules. Operational considerations and the plant PSA can be used for these applications.

In summary, management of configuration frequencies involves:

1. Tracking the frequency, and
2. controlling it through appropriate procedural changes.

8.6 Insights on Managing Plant Configurations

The insights on risk-based analyses to manage plant configurations resulting from component outages are divided in these following categories:

- Risk from plant configurations,
- Calculation of configuration risk,
- TS control of configuration risks, and
- Use of PSAs to improve management of plant configurations.

Risk from Plant Configurations

Simultaneous outages of multiple components increase the risk level because the protection provided by the components is lost. The conditional increase in the risk level, e.g., conditional CDF can be significant for some configurations. At the same time, many configurations have minimum risk implications. The expected frequency of occurrences of the risk-significant configurations is small, and consequently, their impact on average CDF is expected to be small. However, the large peaks in risk that may result from plant configurations are the focus of these assessments.

TS Control of Configuration Risks

LCO in a TS define the duration, i.e., the AOT, for component downtimes and also define the action requirements, e.g., plant shutdown, when multiple components within a safety system are detected failed. These requirements control configuration risk by

a) forbidding simultaneous outages of many combinations that have high risk implications,

b) controlling the duration of a configuration to the minimum of the AOTs of the components involved.

Analyses of risk from downed components across system boundaries may reveal additional risk- significant configurations; TS can be modified to forbid or reduce their durations. As discussed previously, in cases where the risk of shutting down is large or considerable, an AOT to perform prompt repair can be defined. In several combinations, the risk implication is small and the TS control may not be necessary.

Calculation of Configuration Risks

The completed PSAs and the software available as part of the IPE program can be used to calculate the risks associated with different configurations. Calculation of plant CDF when multiple components are simultaneously unavailable involves preparing specific inputs. It also may involve regenerating cut sets to avoid truncation errors; then, the calculation time may be considerable. Efficient software to calculate conditional CDFs when multiple components are unavailable can be developed, using available PSA software.

Use of PSAs to Improve Management of Plant Configurations

The method discussed in this chapter and the framework presented can be the basis for managing plant configurations. The specific insights on using PSAs to improve management of plant configurations are summarized as follows:

- PSAs can be used to identify outage configurations with high CDF peaks. Such peaks can only be controlled by controlling these configurations. Limiting the allowed configuration downtime controls its impact, but not the CDF peak. These configurations can be avoided in scheduling test and maintenance.

- PSAs can be used to categorize the configurations in terms of their CDF levels, and strategies can be developed for their control during plant operation. This strategy may define where immediate shutdown is desirable, where a limited time is to be used to assure the availability of back-up components or promptly repair one of the components, and where no immediate action is necessary because of low risk implication.

- Planned maintenance schedules where multiple components are simultaneously taken out-of-service can be analyzed using PSAs, and if necessary, altered to assure that high peaks in risk are not incurred.

9. BIBLIOGRAPHY

Chapter 1

Bizzak, D.J., Stella, M.E., and Stukus, J.R., "Identification and Classification of Technical Specification Problems," EPRI NP-54-75, Electric Power Research Institute, December 1987.

Code of Federal Regulations, Title 10, "Energy," U.S. Government Printing Office, Washington, DC, Section 50.36, "Technical Specifications."

IAEA, Risk-Based Optimization of Technical Specifications for Operation of Nuclear Power Plants, IAEA-TECDOC-729, International Atomic Energy Agency, Vienna, Austria, December 1993.

IAEA, Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, International Atomic Energy Agency, Vienna, Austria, April 1991.

NRC, Final Policy Statement on Technical Specification Improvements for Nuclear Power Reactors, 10CFR Part 50, Federal Register Vol. 58, No. 139, July 22, 1993.

NRC, Standard Technical Specifications, General Electric Plants, BWR/6, NUREG-1434, September 1992.

NRC, Standard Technical Specifications, General Electric Plants, BWR/4, NUREG-1433, September 1992.

NRC, Standard Technical Specifications, Combustion Engineering Plants, NUREG-1432, September 1992.

NRC, Standard Technical Specifications, Westinghouse Plants, NUREG-1431, September 1992.

NRC, Standard Technical Specifications, Babcock-Wilcox Plants, NUREG-1430, September 1992.

NRC, "Severe Accident Risks: An Assessment of Five U.S. Nuclear Power Plants," NUREG-1150, Volumes 1 and 2, U.S. Nuclear Regulatory Commission, December 1990.

NRC, "Individual Plant Examination: Submittal Guidance," NUREG-1335, US Nuclear Regulatory Commission, August 1989.

NRC, Technical Specifications - Enhancing the Safety Impact, NUREG-1024, US Nuclear Regulatory Commission, November 1983.

NRC, "A Survey by Senior NRC Management to Obtain Viewpoints on the Safety Impact of Regulatory Activities from Representative Utilities Operating and Constructing Nuclear Power Plant," NUREG-0839, August 1981.

Samanta, P.K., Martinez-Guridi, G., and Vesely, W.E., "Reviewing a PSA-Based Analyses to Modify Technical Specifications at Nuclear Power Plants," NUREG/CR-6172, BNL-NUREG-52428, Brookhaven National Laboratory, to be published.

Chapter 2

Hickman, J., et al., "PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plant," NUREG/CR-2300, Volumes 1 and 2 (American Nuclear Society), January 1983.

NRC, "A Review of NRC Staff Uses of Probabilistic Risk Assessment," NUREG-1489, U.S. Nuclear Regulatory Commission, March 1994.

Vesely, W.E., and Goldberg, F.F., "FRANTIC - A Computer Code for Time Dependent Unavailability Analysis," NUREG-0193, U.S. Nuclear Regulatory Commission, October 1977.

Chapter 3

Bizzard, D.J., Trainer, J.E., McClymont, A.S., "Risk-Based Evaluation of Technical Specification Problems at the LaSalle County Nuclear Station, EPRI NP-5238, Electric Power Research Institute, June 1987.

Butter, J.C., et al., "Byron Generating Station Limiting Conditions for Operation Relaxation Program," WCAP-10526, Westinghouse Electric Corporation, Volumes 1 and 2, April 1984.

Houston Lighting and Power, "Proposed Amendment to the South Texas Project Nuclear Generating Station Unit 1 and Unit 2 Technical Specification Based on Probabilistic Analyses," Document ST-HL-AE-3283, February 1, 1990.

Jacobs, I.M., "Safety Test Intervals and Allowable Repair Time for Engineered Safeguards Systems," SRS Quarterly Digest, October 1979.

Mankamo, T., "A Risk-Based Approach to AOTs," NKS/SIK-1 (93)4, Avaplan Oy, Finland, February 1993.

Mankamo, T., "Standards for Allowable Repair Periods in Standby Safety System," SRS Quarterly Digest, October 1981.

Samanta, P.K., Martinez-Guridi, G., and Vesely, W., "Technical Evaluation of South Texas Project (STP) Analysis for Technical Specification Modifications," BNL Technical Report L-2591 1-11-94, Brookhaven National Laboratory, January 1994.

Samanta, P.K., Wong, S.M., and Carbonaro, J.C., "Evaluation of Risk Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, Brookhaven National Laboratory, August 1988.

Vesely, W.E., "Evaluation of Allowed Outage Times (AOTs) from a Risk and Reliability Standpoint," NUREG/CR-5425, BNL-NUREG-52213, Brookhaven National Laboratory, August 1989.

Wagner, D.P., Minton, L.A., and Gaertner, J.P., "Risk-Based Analysis Methods Applied to Nuclear Power Plant Technical Specifications," *Nuclear Technology*, Volume 84, March 1989.

Chapter 4

Chu, T.L., Musicki, Z., Kohut, P., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1," NUREG/CR-6144, BNL-NUREG-52399, Brookhaven National Laboratory, 1994.

Knochenhauer, M. and Engqvist, A., "Using PSA Models for Planning an Evaluation of Preventive Maintenance During Power Operation," CSNI/UNIPEDE Specialist Meeting on Improving Technical Specifications for Nuclear Power Plants, Madrid 1987.

Lakkso, K. (Ed.), "Optimization of Technical Specifications by Probabilistic Methods - A Nordic Perspective," Final Report of the NKA Project RAS-450, Technical Research Center of Finland, Espoo, Finland, May 1990.

Samanta, P.K., Kim, I.S., Uryasev, S., Penoyar, J., and Vesely, W.E., "Emergency Diesel Generator Unavailability and its Risk Impacts," NUREG/CR-5994, BNL-NUREG-52363, Brookhaven National Laboratory, to be published.

Smith, A.M., "Using Reliability-Centered Maintenance to Optimize PM Programs," *Nuclear Safety Journal*, September-October, 1987.

Staple, B.V., Kirk, H.K., and Yankle, J., "Risk Impact of BWR Technical Specification Requirements During Shutdown," NUREG/CR-6166, SAND93-3998, Sandia National Laboratories, October 1994.

Whitehead, D.W., Darby, J., Staple, B., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1," NUREG/CR-6143, Sandia National Laboratories, July 1994.

Chapter 5

Combustion Engineering Topical Report on RPS and ESFAS Surveillance Test Interval and Allowed Outage Time Extension, CEN-327, ABB-Combustion Engineering, Windsor, Connecticut, 1986.

Engqvist, A., Mankamo, T., "Test Scheme Rearrangement for Diesel Generators at Forsmark 1/2," PSA '89 International Topical Meeting on Probability, Reliability and Safety Assessment, Pittsburgh, PA, 1989.

General Electric, "BWR Owners' Group Technical Specification Improvement Analysis for BWR Reactor Protection System," NEDO-30851P, May 1985.

Lewis, E.E., Nuclear Power Reactor Safety, John Wiley & Sons, Inc., 1977.

Lofgren, E., Uryasev, S., and Samanta, P., "Technical Specification Defenses Against Common-Cause Failures," NUREG/CR-6140, BNL-NUREG-52397, Brookhaven National Laboratory, to be published.

Mankamo, T., "Test Strategies for Standby Diesel Generators," IAEA Technical Committee Meeting on Advances in Reliability Analysis and PSA, Budapest, 1992.

Mankamo, T. and Pulkkinen, U., "Test Interval Optimization of Standby Equipment," Technical Research Center of Finland, Research Note 892, VTT, Otakaari 7B, SF 02150, Espoo, Finland, 1988.

Mosleh, A. et al., "Procedures for Treating Common-Cause Failures in Safety and Reliability Studies," Vols. 1 and 2, NUREG/CR-4780, EPRI NP-5613, 1988.

Quinn, E.L., Dykes, A.A., and Bockhorst, R., "Risk-Based Evaluation of Surveillance Test Procedures at San Onofre Nuclear Generating Station," Transactions of American Nuclear Society, Vol. 56, pp. 343, 1988.

Samanta, P., Ginzburg, T., Vesely, W., "Consideration of Test Strategy in Defining Surveillance Test Intervals," BNL Technical Report A-3859, Brookhaven National Laboratory, 1988.

Samanta, P.K., Wong, S.M., Carbonaro, J., "Evaluation of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, Brookhaven National Laboratory, 1988.

Vaurio, J., "The Theory and Quantification of Common-Cause Shock Events for Redundant Safety Systems," *Reliability Engineering and System Safety*, Vol. 43, pp. 289-306, 1994.

Vaurio, J.K., "The Effects of Testing Arrangements on the Unavailability of Standby Systems," Proceedings of Probabilistic Safety Assessment International Topical Meeting, Clearwater Beach, Florida, Vol. 1, pp. 654-659, 1993.

Vesely, W.E., "Measures of the Risk Impacts of Testing and Maintenance Activities," NUREG/CR-3541, Battelle's Columbus Laboratories, November 1983.

Vesely, W.E. et al., Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, 1981.

Vesely, W.E., DeMoss, G.M., Lofgren, E.V., et al., "Evaluation of Diesel Unavailability and Risk Effective Surveillance Test Intervals," NUREG/CR-4810, BNL-NUREG-52022, Brookhaven National Laboratory, May 1987.

Westinghouse Electric, "Evaluation of Surveillance Frequencies and Out of Service Times for the Engineered Safety Features Actuation System," WCAP 10271, Revision 1, March 1987.

Chapter 6

Apostolakis, G.E. and Bansal, P.P., "Effect of Human Error on the Availability of Periodically Inspected Redundant Systems," IEEE Transactions on Reliability, Vol. R-26, No. 3, August 1977.

Kim, I.S., Martorell, S., Vesely, W.E., and Samanta, P.K., "Quantitative Evaluation of Surveillance Test Intervals Including Test-Caused Risks," NUREG/CR-5775, BNL-NUREG-52296, Brookhaven National Laboratory, February 1992.

Kim, I.S., Martorell, S.A., et al., "Risk Analysis of Surveillance Requirements Including Their Adverse Effects," *Reliability Engineering and System Safety,* 45(1994) 225-234.

Lobel, R. and Tjader, T.R., "Improvements to Technical Specifications Surveillance Requirements," NUREG-1366, U.S. Nuclear Regulatory Commission, August 1990.

McClymont, A.S. and Poehlman, B.W., "ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients," EPRI NP-2230, Electric Power Research Institute, January 1982.

McWilliams, T.P. and Martz, H.F., "Human Error Considerations in Determining the Optimum Test Interval for Periodically Inspected Standby Systems," IEEE Transactions on Reliability, Vol. R-29, No. 4, October 1980.

Swain, A.D., "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, February 1987.

Vesely, W.E., "Risk Evaluation of Aging Phenomena: The Linear Aging Reliability Model and Its Extensions," NUREG/CR-4769, April 1987.

Vesely, W.E., Kurth, R.E., and Scalzo, S.M., "Evaluation of Core Melt Frequency Effects due to Component Aging and Maintenance", NUREG/CR-5510, SAIC-89/1744, Science Applications International Corporation, June 1990.

Chapter 7

Chu, T.L., Musicki, Z., Kohut, P., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry, Unit 1," NUREG/CR-6144, BNL-NUREG-52399, Brookhaven National Laboratory, 1994.

Mankamo, T., Kim, I.S., and Samanta, P.K., "Technical Specification Action Statements Requiring Shutdown: A Risk Perspective with Application to the RHR/SSW Systems of a BWR," NUREG/CR-5995, BNL-NUREG-52364, Brookhaven National Laboratory, November 1993.

Mankamo, T. and Kosonen, M., "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/Tech Spec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

Whitehead, D.W., Darby, J., Staple, B., et al., "Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Grand Gulf, Unit 1," NUREG/CR-6143, Sandia National Laboratories, July 1994.

Chapter 8

Atefi, B. et al., "Feasibility Assessment of a Risk-Based Approach to Technical Specifications," NUREG/CR-5742, Vol. 1 and 2, Science Applications International Corporation, May 1991.

Horne, B.E., "The Use of PSA Methods for Planning the Maintenance and Testing Unavailability of Essential Plant at Heysham 2 AGR Power Station," Use of Probabilistic Safety Assessment to Evaluate Nuclear Power Plant Technical Specifications, IAEA-TECDOC-599, International Atomic Energy Agency, Vienna, Austria, 1991.

Puglia, B., Gallagher, D., Amico, P., and Atefi, B., "Risk-Based Technical Specifications: Development and Application of an Approach to the Generation of a Plant Specific Real-Time Risk Model," NUREG/CR-5925, SAIC 92/6668, Science Applications International Corporation, October 1992.

Samanta, P.K., Vesely, W.E., and Kim, I.S., "Study of Operational Risk-Based Configuration Control," NUREG/CR-5641, BNL-NUREG-52261, Brookhaven National Laboratory, August 1991.

Samanta, P.K., Vesely, W.E., and Kim, I.S., "Toward Risk-Based Control of Nuclear Power Plant Configurations," Nuclear Engineering and Design, 134(1992) 355-370.

Sursock, J.P. and True, D., "EPRI Perspectives on the Use of Risk-Based Technical Specifications in Controlling Plant Operations," Proceedings of PSA '91 Conference, International Atomic Energy Agency, Vienna, Austria, 1991.

Appendices

IAEA, "Modelling and Data Prerequisites for Specific Applications of PSA in the Management of Nuclear Plant Safety," IAEA-TECDOC-740, International Atomic Energy Agency, Vienna, Austria, April 1994

NRC, "A Review of NRC Staff Uses of Probabilistic Risk Assessment," NUREG-1489, U.S. Nuclear Regulatory Commission, March 1994.

NRC, "Individual Plant Examination: Submittal Guidance," NUREG-1335, U.S. Nuclear Regulatory Commission, August 1989.

General References

EPRI, "Common Aging Terminology, A Glossary Useful for Understanding and Managing the Aging of Nuclear Power Plant Systems, Structures, and Components," February 1993.

NRC, "A Review of NRC Staff Uses of Probabilistic Risk Assessment," NUREG-1489, U.S. Nuclear Regulatory Commission, March 1994.

Vesely, W. et al., Fault Tree Handbook, NUREG-0492, U.S. Nuclear Regulatory Commission, January 1981.

APPENDIX A ATTRIBUTES OF PSA FOR TS APPLICATIONS

NUREG-1489, "A Review of NRC Staff Uses of Probabilistic Risk Assessment" 1994, provides general guidance (Appendix B; Section B.4) for using PSAs in issues resolution analyses. This guidance is applicable for TS applications. Here, we briefly discuss the specific desirable attributes of a PSA for carrying out the risk-based or PSA-based analyses of TS discussed in this handbook. In defining the methods, we assumed certain attributes or features of the PSA, which are summarized here.

We first describe the PSA attributes on which the AOT and STI analyses (methods discussed in Chapters 3 and 5) are based, and then discuss additional attributes on which the applications presented in other chapters are based.

Summary of PSA Modeling Attributes for AOT and STI Applications

- A Level I PSA model in which the internal initiating events are analyzed is the primary basis for these analyses; to evaluate containment system AOTs and SRs, a Level 2 PSA is the basis. To evaluate requirements relating to external events, external event initiators should be included.

- System fault trees should be detailed enough to specifically include all the components for which surveillances and maintenances are performed and are to be evaluated.

    - For AOT evaluations, system train level models are adequate as long as all components belonging to the train are clearly identified (i.e., the failure of all those components that cause the train to fail). In using train-level models, common-cause contributions still must be adequately treated.

    - For evaluating STIs, individual component-level models are necessary.

- Component unavailability models should include significant contributions from random failure, common-cause failure, test downtime, and maintenance downtime.

  - Additional details in terms of separating the failure rate contributions into cyclic demand- and standby time-related contributions can be incorporated, if justifiable, for evaluating surveillance requirements.

  - The component unavailability model needs to have the flexibility to separate contributions from test and maintenance downtime. For evaluating an AOT, the contribution from maintenance downtime can be equated to zero to delete it. For an STI evaluation, the contribution from test-downtime determines a contribution to risk from carrying out the test.

- Treatment of common-cause failures and human errors should be realistic; overconservative estimates of these contributors may mask the effects of TS measures. For example, if the estimate of human error in restoring a component after a test is too large, then the effect of changing a test interval can be underestimated in terms of its contribution to the measure of total risk.

- The common-cause failure contributions preferably should be modeled such that they can be modified to reflect the condition that one or more of the components is unavailable.

- In addition to the dominant accident sequences identified in the basic PSA, additional accident sequences may need to be considered which could become non-negligible if AOTs or STIs are changed. This assures that quantifications of core-damage frequency for different test and maintenance activities are not underestimated, and also increases the number of surveillance and maintenance activities that can be analyzed for AOTs and SRs.

- A computer package should be used to generate accident-sequence minimal-cut sets when components are assumed to be unavailable (i.e. down) for surveillance or maintenance. The use of pre-processed, i.e., truncated minimal cut sets from the base case PSA may not suffice because the cut set important to the surveillance/maintenance condition already may have been truncated.

PSA Attributes for Evaluating Surveillance Test Strategy

- To account for the effects of test placements for redundant components in relation to each other (e.g., staggered or sequential test strategy), time-dependent models and additional evaluations may be needed, using specialized codes. Time-dependent evaluations can be made using system fault-tree models to decide on the test strategy for the redundant components in the system. The corresponding system unavailability can be used to determine the core-damage frequency.

PSA Attributes for Analyzing Action Statements Requiring Shutdown

These attributes are not considered part of PSAs that evaluate risk during power operation, e.g., IPEs being completed for NPPs. They are PSA supplements, developed as part of the analyses of Action Statements as discussed in NUREG/CR-5995 (Mankamo et al. 1993).

- Various stages of the shutdown cooling phases, and operator interactions should be modelled to assess the impact on core-damage frequency of shutting the plant in a LCO.

- Any initiating event not modelled in the basic PSA, but important during the shutdown phases, should be modelled. Specific examples are those events which challenge the RHR system and which can render part of it unavailable. Also, the initiating event frequency during the transition to shutdown may have to be reassessed since the frequency then may differ from that during power operation, e.g., increased loss-of-offsite power or loss of main feedwater frequency during transition to shutdown.

- Different recovery paths applicable at various stages of shutdown should be modelled to realistically quantify the risk of shutting down considering diminishing decay heat levels.

- Available time margins for reactor core uncovery and suppression pool heatup (in a BWR) or steam generator dry-out (in a PWR) need to be modelled to evaluate specific accident sequences.

PSA Attributes for Analyzing the Risk for Equipment Outage Configurations for Managing Plant Configurations

The first five of these attributes particularly relate to analyses of risk from outages of multiple components in a PM schedule.

- System models should be constructed so that reconfiguration of component states during testing and maintenance can be taken into account efficiently in computations.

- Common-cause failure modelling should retain the component designator so that dependency is accounted for appropriately in different plant configurations with specific components down and available components potentially susceptible to common-cause failures.

- Errors in operator recovery actions modelled in accident sequences may need to be reviewed to assure their applicability in different plant configurations.

- PSA models should be able to quantify plant risk levels (e.g., core damage frequency) for different plant configurations where the status (available, unavailable, or reconfigured) of multiple components can be changed.

- There should be negligible error due to truncation of minimal cut sets. This is important because the status of multiple components is changed to "True" or "False" or to a different intermediate unavailability for a given configuration.

- Quantitative capabilities should include evaluations of accumulated risk for a given duration of a configuration and for the expected number of configuration occurrences over a given operating period.

- For a given configuration, priorities can be identified for checking alternate success paths (by checking other components to assure they are operable).

- For an on-line configuration management system with features to evaluate risk levels in real or near-real time, a time-dependent component unavailability model is a useful feature. It allows the effect of specific times at which tests are performed to be incorporated directly.

- For an on-line configuration management system, component unavailability models and initiating event frequency should allow updating of the parameters when accumulated data show that it is necessary, or at specific intervals desired by the user.

- For an on-line configuration management system and real time evaluations, risk levels and other information should be calculated in a timely fashion (e.g., 3 to 5 minutes).

- Calculation of risk levels, other information features, and the decision implementations achieved through the system should be stored and documented in such a manner that auditing can be performed effectively.

APPENDIX B CALCULATION OF CONDITIONAL CDF FOR AOT AND STI EVALUATIONS

The analyses of risk contributions associated with AOT evaluations and some STI evaluations involve calculating conditional CDFs using a standard PSA for the plant. Usually, the conditional CDF is calculated to estimate the CDF when one or more component is down either due to failure or for preventive maintenance. These calculations are performed using PSA computer codes and involve modifying input parameters (or data) to represent the downed condition. In this appendix, we discuss the modification of the PSA input parameters and the care that should be taken in calculating these conditional CDFs.

Conditional CDF for failure of a component

To calculate the conditional CDF when a component is failed (typically represented by R_1 in this handbook), the component unavailability is changed to the "True" or "T" state. However, the component unavailability may be modeled in terms of many contributors: random failure, maintenance downtime, test downtime, and common-cause failure. The common-cause failure (CCF) term represents the failure probability of two or more redundant components which include the failed component in question. The CCF term is modeled as a product of multiple terms, e.g., using the β-factor model for two redundant components, the CCF term is β times the component unavailability from random failures, but may be represented by one parameter.

Consider a component Q in train A of a safety system, letting QLA, QMA, and QTA, respectively, represent the component's unavailability from random failures, maintenance downtimes, and test-downtimes. Also, let QC($=\beta$.QL) be the CCF term for CCF of the redundant components in trains A and B, where QL is numerically equal to QLA and represents QLA or QLB. QLB is the unavailability of a component in train B from random failure. Usually, the terms QLA, QMA, QTA, and QC will be part of the PSA input data.

To calculate the conditional CDF given the component is failed, the component unavailability should be represented by the "T" state. This means that QLA, QMA, and QTA should be changed to the "T" state and QC should be divided by QLA since the component is down because of failure. In principle, out of the three conditions (QLA, QMA, QTA) changing one of them to "T" state should suffice. However, in many cases, truncated cutsets are used to calculate the conditional CDF, and changing all three will assure that the failed state of the component is represented. For this example, QC will be changed to β, which represents the conditional failure probability of the redundant component. When QC represents the failure of more than two components, e.g., three components, then QC will be converted to the failure probability of the remaining components, i.e., in this case, two components.

Conditional CDF when a component is down (but not failed) for PM

To calculate the conditional CDF when a component is taken down for PM (R_1 for PM analyses), the CCF term needs to be treated differently than that described above for the failure of the component.

Considering the same example as above, the down state of the component is represented by changing QLA, QMA, and QTA to "T" and by changing QC to QL, which is numerically the same as QLB or QLA. The CCF term is changed to represent the unavailability of the remaining component and not β, since the initial component is already down for PM and is not down due to failure. If the redundant component is successfully tested before taking the component down for PM, then QC can be equated to zero for a short-duration PM (i.e., when the duration of PM is much less than the test interval).

Conditional CDF when the component is not down for maintenance or is tested operable

The conditional CDF is reduced when the component is not down for maintenance or it has just successfully been tested. The calculation of AOT and STI risk contributions involve calculating this conditional CDF (R_0). For evaluating the AOT risk contribution, R_0 signifies that the component is not down for test or maintenance, and this condition is represented by setting test and maintenance downtime unavailabilities to "False" or "F" state. In our example, this means that QMA and QTA should be changed to the "F" state. For STI evaluations, R_0 signifies that the component is up, which is known from the test and is represented by setting its unavailability to "False." In our example, this means that QLA, QMA, and QTA should be changed to the "F" state. In many cases, the reduction in CDF from the baseline CDF is negligible.

Conditional CDF when multiple components are involved

To calculate conditional CDFs (R_1 and R_0), when multiple components are involved, the corresponding terms relating to each of the components should be changed to the "T" or "F" state. For each component, the corresponding terms relating to random failures, common-cause failures, test- and maintenance-downtimes should be converted, as discussed above. When all the components modeled by a common-cause term are failed, then this term changes to "T" state for calculating R_1. Otherwise, it is modeled as discussed above, representing the unavailability of the remaining components. In many PSA computer codes, the CCF term does not retain the specific component designator, i.e., for example, a unique notation identifying the specific component involved may not be part of the name of the CCF term, and the relevant term cannot directly be identified searching the names of the input parameters of the PSA. The description of the CCF terms modeled in the PSA may need to be examined to identify the relevant term or the input parameter.

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)
NUREG/CR-6141
BNL-NUREG-52398

2. TITLE AND SUBTITLE
Handbook of Methods for Risk-Based Analyses of Technical Specifications

3. DATE REPORT PUBLISHED
MONTH: December
YEAR: 1994

4. FIN OR GRANT NUMBER
A3230

5. AUTHOR(S)
P. K. Samanta, I. S. Kim/Brookhaven National Laboratory
T. Mankamo/Avaplan Oy
W. E. Vesely/Science Applications International Corporation

6. TYPE OF REPORT
Technical

7. PERIOD COVERED *(Inclusive Dates)*

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

Brookhaven National Laboratory
Upton, NY 11973

Avaplan Oy
Itainen rantatie 17
FIN-02230
Espoo, Finland

Science Applications International Corporation
655 Metro Place South, Suite 745
Dublin, OH 43017

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

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

10. SUPPLEMENTARY NOTES

11. ABSTRACT *(200 words or less)*

Technical Specifications (TS) requirements for nuclear power plants define the Limiting Conditions for Operation and Surveillance Requirements to assure safety during operatio In general, these requirements are based on deterministic analysis and engineering judgments. Experiences with plant operation indicate that some elements of the requirements are unnecessarily restrictive, while a few may not be conducive to safety. Inproving these requirements involves many considerations and is facilitated by the availability of plant-specific Probabilistic Safety Assessments and development of related methods for analyses. This handbook summarizes the risk- and reliability-based methods to improve TS requirements. The scope of the handbook includes reliability- and risk-based methods for evaluating allowed outage times, scheduled or preventive maintenances, action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals, and management of plant configurations resulting from outages of systems, or components. For each topic, the handbook summarizes analytic methods with data needs, outlines the insights to be gained, lists additional references, and gives examples of evaluations.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Technical Specification, Probabilistic Risk Assessment, Probabilistic Safety Assessment, Standard Technical Specifications, Risk-Based Technical Specifications, Allowed Outage Times, Surveillance Requirements, Limited Condition for Operation, Risk Assessment, Reactor Operation, Reactor Safety, System Failure Analysis, BWR Type Reactors-Engineered Safety Systems, PWR Type Reactors-Engineered Safety Systems, BWR Type Reactors-Specifications, PWR Type Reactors-Specifications, Preventive Maintenance, Technical Specification Action Statements.

13. AVAILABILITY STATEMENT
Unlimited

14. SECURITY CLASSIFICATION
(This Page)
Unclassified
(This Report)
Unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

SPECIAL FOURTH-CLASS RATE
POSTAGE AND FEES PAID
USNRC
PERMIT NO. G-67