DRAFT

Risk-Managed Technical Specifications (RMTS) Guidelines

Technical Update to EPRI Technical Update Report 1009674

August 2005

EPRI Project Manager
J. Gaertner

EPRI • 3412 Hillview Avenue, Palo Alto, California 94304 • PO Box 10412, Palo Alto, California 94303 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

ABSG Consulting Inc. (ABS Consulting)
300 Commerce Drive, Suite 200
Irvine, CA 92602-1305

Westinghouse Owners Group
Westinghouse Electric Company, LLC
2000 Day Hill Road
Windsor, CT 06095-0500

CITATIONS

This report was prepared by

ABSG Consulting Inc. (ABS Consulting)
300 Commerce Drive, Suite 200
Irvine, California 92602-1305

Principal Investigator
J. K. Liming

Westinghouse Owners Group
Westinghouse Electric Company, LLC
2000 Day Hill Road
Windsor, Connecticut 06095-0500

Principal Investigator
R. E. Schneider

This report describes research sponsored by EPRI.

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

Risk-Managed Technical Specifications (RMTS) Guidelines, EPRI, Palo Alto, CA: 2004. 1009674.

REPORT SUMMARY

The Electric Power Research Institute (EPRI) has assessed the role of probabilistic risk assessment (PRA) in the regulation of nuclear power plant technical specifications. This report presents nuclear utilities with one example of a technical framework and associated general guidance for implementation of risk-managed technical specifications (RMTS) as a partial replacement of existing conventional plant technical specifications. This report was prepared by EPRI with extensive technical input and review by the Nuclear Energy Institute (NEI) Risk-Informed Technical Specifications Task Force (RITSTF), which includes contributions from the Westinghouse Owner's Group. This report is a Technical Update to EPRI Report 1009674, which was published in December 2004 as an Interim Development Report. As this report is used as the basis for RMTS implementation and as it undergoes review by the Nuclear Regulatory Commission (NRC) staff, it will likely be updated and upgraded in the future.

Background

Since 1995, the methodology for applying PRAs to risk-informed regulation has been advanced by the publication of many reports. Related to the area of risk-informed Technical Specifications alone, EPRI has recently published the *PSA Applications Guide* (TR-105396), *Guidelines for Preparing Risk-Based Technical Specifications Change Request Submittals* (TR-105867), *Risk-Informed Integrated Safety Management Specifications (RIISMS) Implementation Guide* (1003116), *Risk-Informed Configuration-Based Technical Specifications (RICBTS) Implementation Guide* (1007321), and *Risk-Managed Technical Specifications (RMTS) Guidelines, Interim Reports* (1002965 and 1009674). NRC has issued Regulatory Guide1.177 and a Standard Review Plan providing guidance on risk-informed technical specifications programs. Over the past four years, the Nuclear Energy Institute (NEI) Risk-Informed Technical Specification Task Force (RITSTF) has addressed several generic initiatives to further risk-inform plant technical specifications. One of these initiatives, 4B, entitled Risk Managed Technical Specifications, is the subject of this report. Two pilot implementations of Initiative 4B have been submitted by utilities to NRC for their approval. An earlier version of this report, EPRI Report 1002965 was submitted to NRC with these pilot submittals. Based on NRC reviews, EPRI Report 1009474 was produced and docketed with NRC. This report is a further revision based on NRC review, industry and NRC workshops on the subject, and industry experience using the guidelines.

Objectives

- To provide utilities with an approach for developing and implementing nuclear power plant risk-managed technical specifications programs.

- To complement and supplement existing successful Configuration Risk Management applications such as Maintenance Rule (a)(4).
- To eventually serve as NRC-approved guidelines for widespread implementation of RITSTF Initiative 4B.

Approach

By using available industry and NRC documentation, experienced PRA practitioners, acting through the NEI RITSTF, developed an approach and methodology for implementing risk-informed technical specifications. The method uses the Maintenance Rule (a)(4) guidance contained in Section 11 of NUMARC 93-01 as a starting point, and this document is developed as a logical extension of that guidance to address the additional challenges of Risk Managed Technical Specifications. The primary enhancements to the (a)(4) process are 1) the calculation of a risk-informed completion time (RICT) as an alternative to the Allowed Out-of-service Times (AOTs) in current Technical Specifications, and 2) calculation of cumulative risk incurred through the use of these RICTs. Other enhancements to the (a)(4) process are associated with the elevation of the (a)(4) process to a higher regulatory significance through its incorporation into Technical Specifications. The process continues to evolve based on NRC review comments, the experience of the two proposed pilot implementations of Initiative 4B, and reviews by the members of the NEI RITSTF.

Results

This report presents a recommended approach and technical framework for an effective RMTS program and its implementation following NRC approval. This report is also intended, together with the ASME standards on PRA as modified by experience with NRC Regulatory Guide 1.200, to define of the requirements for PRA scope and capability for this RMTS application.

EPRI Perspective

This project is an important element of the nuclear industry's strategic objective to use more risk-informed regulations and operational decisions. It is a logical extension of traditional Technical Specifications that builds upon the current Configuration Risk Management (CRM) requirements of the NRC Maintenance Rule. All U.S. nuclear plants meet these requirements, and many have more extensive CRM programs to support work planning and scheduling, evaluation of events during operation, response to NRC inspection findings, and other day to day applications. These capabilities have proven to be risk-effective and cost-effective. Furthermore, their regular use has fostered a desirable risk management culture at well-run plants. EPRI expects to support this RMTS effort in the future as it continues through the regulatory approval process and through its early implementation. Furthermore, this project will interface with the related activities of the EPRI Configuration Risk Management Forum (CRMF), which addresses a wide range of CRM issues.

Keywords

Probabilistic risk assessment
Risk-informed applications

Technical Specifications
NRC regulations and Licensing

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

The purpose of this report is to provide specific guidance on how to implement RMTS programs at existing and planned nuclear power plants using configuration risk management tools and techniques. This report provides guidance for plants desiring to implement RMTS for a single system as well as those desiring to implement a global "whole plant" RMTS approach. This report is organized and presented as follows:

- Section 1 is an overview of the history preceding RMTS programs.
- Section 2 provides the RMTS process description overview.
- Section 3 presents the detailed RMTS guidance approach and methodology.
- Section 4 presents the attributes of a PRA that are required for RMTS implementation.
- Section 5 presents RMTS references.
- Appendices provide supporting RMTS program information.

10CFR50.36, "Technical Specifications," requires that the licensee identify Limiting Conditions of Operation (LCOs). These are the minimum functional capability or performance levels of equipment required for safe operation of the facility. When an LCO is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the Technical Specifications (TS) until the condition can be met. No specific timing requirements were included in the regulation. However, in practice, actions within an LCO are associated with one or more fixed time intervals. Within the context of the plant TS, these time intervals are termed the Allowed Outage Times (AOTs) or Completion Times (CTs). These time intervals were established at the time of plant licensing. In this document, we use the term CT to refer to completion time and/or allowed outage time.

In the 1980s and early 1990s, risk informed changes were approved for a number of plants including Millstone Units 2 and 3; Palo Verde Units 1, 2 and 3; and the South Texas Project Units 1 and 2 (e.g., the diesel generator 14-day AOT, etc.). Early activities in integrating risk insights were used in resolving specific industry issues. These activities were sponsored to varying degrees by all Owners' Groups [23 and 24]. In 1995, the NRC embarked on an initiative to improve regulatory efficiency and enhance public safety by considering risk insights in regulation. The effort resulted in the risk-informed changes to a wide range of regulatory activities including In-Service Testing (IST), In-Service Inspection (ISI), graded Quality Assurance (QA), and AOT and surveillance test interval (STI) extensions within the plant TS. The CEOG AOT extension efforts for the Safety Injection Tanks (SITs), Low Pressure Safety Injection (LPSI) System and Emergency Diesel Generators (EDG) [25, 26 and 27] became the pilot documents supporting the development of the Regulatory Guide governing risk informed

changes to the Plant TS [13]. As experience with risk informed regulation has grown, additional Risk-Informed AOT extensions have been granted.

One of the factors leading up to the development of a Risk-Managed Technical Specifications (RMTS) program was the NRC's "Maintenance Rule" (10 CFR 50.65) [2], specifically, 10 CFR 50.65(a)(4) which states:

> "Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to those structures, systems, and components that a risk-informed evaluation process has shown to be significant to public health and safety."

Following industry feedback from a 1998 stakeholders meeting, the NRC recommended that the industry consider an initiative to risk inform the plant TS. In response to that initiative, several public meetings were held to identify the aspects of the TS that are amenable to a risk informed treatment. Currently, the industry is sponsoring eight Risk Informed Technical Specifications (RITS) initiatives. These initiatives involve all the Owner's Groups and are coordinated through the NEI RITSTF. This report focuses on enabling conditions for the broad based RITSTF Initiative 4B, Risk-Managed Technical Specifications (RMTS), to replace the existing fixed AOTs/CTs with a flexible CT structure consistent with the plant's 10CFR50.65(a)(4) [2] Maintenance Rule program. In a flexible CT structure, most equipment TS conditions allow the component outage time to be determined based on the actual plant state and relative risks. Specifically, the general features of the RITSTF RMTS are discussed, and specific risk informed processes that may be needed for successful implementation of this type of TS are identified. RMTS is the industry effort to transition from existing fixed AOTs to flexible CTs. These processes will complement an existing 10CFR50.65(a)(4) program and could be subsumed within a future overarching risk management program. Inclusion of these supplementary processes within a plant's configuration risk management program will enable better integration and support of the plant TS and, in so doing, improve the methodology of today's TS.

It is expected that implementation of RMTS will allow utilities to more fully utilize risk-informed tools and processes in the management of plant maintenance. These TS enhancements will reduce plant risk by allowing flexibility in prioritization of maintenance activities, improving resource allocation, and avoiding unnecessary plant mode changes. The RMTS under development is specifically directed towards equipment outages and will not change the manner in which plant design parameters are controlled.

This guide essentially refines and supplements Nuclear Energy Institute guidance for implementation of the Maintenance Rule (see Section 11 of Reference 3). Additional key references include EPRI's PSA Applications Guide [4] and NRC's Regulatory Guide 1.174 [5].

Maintenance activities must be performed to provide the level of plant equipment reliability necessary for safety, and should be carefully managed to achieve a balance between the benefits and potential impacts on safety, reliability and availability.

The benefits of well managed maintenance conducted during power operations include increased system and unit availability, reduced equipment and system deficiencies that could impact operations, more focused attention on safety due to fewer activities competing for specialized resources, and reduced work scope during outages.

This report is a key part of RITSTF RMTS. RMTS is designed to be consistent with, and provide enhancement to, the guidance provided for maintenance rule risk management described in Reference 3. This section summarizes the enhancements that this initiative brings to prudent safety management.

It is not the intent of the RITSTF initiatives to modify the manner in which the maintenance rule requirements are met by various utilities. However, it is the intent of this report to provide the guidance for integrating risk managed technical specifications with the maintenance rule process. While the fundamental process to be used for the flexible TS is not different from the maintenance rule process, the proposed risk assessment process has an increased quantitative focus and requires a more formal mechanism for dispositioning maintenance decisions. RMTS features balance the flexibility in performing maintenance within a structural risk informed framework so as to adequately control the risk impact of plant maintenance decisions.

The RMTS process discussed in this report may be used within the current configuration risk management which implements the maintenance rule (a)(4) requirements. Specifically, this report describes a proposed integration of the present 10CFR50.65(a)(4) evaluation process with selected supplementary processes to create an enhanced process that will support the implementation of flexible CTs within the plant TS.

The integrated process is intended to provide a comprehensive risk informed mechanism for expeditious identification of risk significant plant conditions. This will include the implementation of appropriate risk management actions, and will retain the current TS action statement requirements, including the action to shutdown the plant. In practice, this program is consistent with 10CFR50.65(a)(4) maintenance planning conditions. That is, the program retains the current 10CFR50.65(a)(4) practice, which prohibits the plant from voluntarily entering high-risk conditions without proper evaluation of the concurrent risks and implementation of appropriate risk management actions. Enhancements are associated with emergent (unscheduled) maintenance states and are recommended to ensure that high-risk conditions associated with multiple component outages are identified early and that a risk-informed process exists to effect TS required actions, including plant shutdown, as appropriate. In addition, the guidance on the scope and quality of the risk-informed tool(s) used in performing the assessment are identified.

2
PROCESS DESCRIPTION

This document has been developed to provide the commercial nuclear power industry guidance on risk management issues associated with implementation of Risk-Managed Technical Specifications (RMTS) programs at their facilities. Specifically, this guide is designed to support the implementation of a risk-informed approach to the management of equipment "allowed outage time" (AOT) or maintenance "completion time" (CT) related to safety functions addressed by plant technical specifications. Henceforth, in this document, we will refer to AOT and/or CT simply as CT. See Appendix A of this guide for a glossary of key terms applicable to RMTS program development and implementation.

The RMTS process presented in this report integrates the appropriate regulatory guidance. The overall maintenance risk will be assessed via processes consistent with 10CFR50.65, its attendant Regulatory Guide (RG) 1.182, and NUMARC 93-01. Risk informed front-stop CTs for RMTS will be consistent with the currently-approved TS CTs, but may be revised outside the scope of RMTS via single SSC outage guidelines of RG 1.177.

Existing conventional technical specifications for nuclear power plants specify required maximum CT values for specific plant equipment related to the maintenance of key plant safety functions. Under the proposed RMTS concept, these CT values would be maintained and referred to as "front-stop" CT values. However, operation beyond the front-stop would be allowable provided the risk of continued operation can be shown to remain within established safety limits. The process for allowing continued operation will involve performance of risk assessments and definition of risk-informed CT (RICT) targets and limits. The RICT is the time from the initiation of a maintenance configuration until a risk threshold or limit (described in Section 3) is reached. Therefore, the RICT is a calculated value for each maintenance configuration. However, the RMTS RICT will also have an ultimate maximum CT limit (currently established at 30 days), referred to as the "back-stop" CT. The front-stop CT values may be either those that have historically been established via conventional deterministic engineering methods and judgment or those more recently justified via risk-informed methods in accordance with RG 1.177. The back-stop CT limit of 30 days is judged to be a prudently conservative administrative limit for configuration risk management, for example compared with the 10CFR50.59 design change criteria limit of 90 days. The 30-day back-stop CT was established based on the fact that some conventional technical specification front-stop CT limits are as long as 30 days, and because many nuclear plants would require up to this time period to complete some required complex corrective maintenance and testing for system function recovery. It is anticipated that application of RICTs for individual maintenance configurations (see definition of "maintenance configuration" in Appendix A) would realistically rarely exceed approximately two weeks. The front-stop CT, RICT, and back-stop CT taken in conjunction can be thought of as a type of "defense-in-depth" approach to maintenance configuration and

associated technical specification risk management. The proposed approach builds upon the recognized need that the maintenance of equipment in the nuclear power industry could benefit from the application of current "state-of-the-art" risk management methods, tools, and techniques.

In a RMTS program, the structure of the risk-informed technical specifications will be similar to familiar conventional TS with the exception that actions will be provided to allow continued plant operation beyond the TS "front-stop CT". Thus, if a need arises, plant operators would have an option of exceeding that CT provided a risk assessment confirms the risk is reasonably expected to remain within established safety limits. Guidance for continuing maintenance beyond the CT must be consistent with the Maintenance Rule Guidance, and the risk associated with this continued maintenance must be tracked. Risk assessments applied for RMTS RICT determination and implementation will be performed in accordance with this document and supported by the implementing plant's PRA and other configuration risk management tools (e.g., plant safety monitor or risk monitor software, lists of pre-analyzed maintenance configurations, PRA sensitivity studies, etc.) for specified hazards and operational plant states. These tools are typically applied in 10CFR50.65(a)(4) assessments and evaluations. The term "maintenance configuration" is defined in Appendix A and is simply the consolidated state of all plant equipment along with their states of functionality, i.e., either functional or non-functional, and applies to both preventive and corrective maintenance.

PRAs and associated configuration risk management (CRM) tools must be commensurate with the risk impact and scope of the application. Furthermore, the PRA aspects of the CRM tool will comply with NRC RG 1.200 requirements to the extent appropriate for the specific application. Throughout this guideline, scope and capability requirements specific to this PRA application type are further specified herein. These two documents (RG 1.200 and this guideline) address the requirements for PRA scope and capability for this PRA application type. For RMTS program application, CRM tools applied for RICT calculation must meet the same quality assurance requirements as their respective underlying PRAs approved for risk-informed applications via RG 1.200.

Risk-managed LCOs will be entered when the associated TS components are declared inoperable. The assignment of inoperability will follow current TS guidance. Once the LCO is entered, the functional impact (related to SSC availability to support its applicable safety function(s)) of the inoperability will be considered in the risk assessment for RICT determination. For example, system inoperability may vary in risk significance, dependent on the degree of residual capability (capability to support required safety functions) of the system.

To use the RMTS option for normal planned maintenance, two key time durations are calculated before the front-stop CT limit is reached: (1) a risk management action time (RMAT); and (2) a safety limit RICT. In a RMTS program, prior to reaching the RMAT, maintenance activity is performed consistent with normal work controls. After the RMAT but before the safety limit RICT has been reached, maintenance activity is performed in association with clearly specified risk management actions (RMAs). At or beyond the safety limit RICT, clearly specified actions in accordance with applicable TS LCO action statements, possibly including plant shutdown, would be required. Consistent with NEI maintenance rule guidance [3], the RMAT threshold

would be based on a configuration Incremental Core Damage Probability (ICDP) of 10^{-6} or Incremental Large Early Release Probability (ILERP) of 10^{-7} (as measured from the time the associated plant equipment is placed or is discovered to be out of service). A safety limit RICT threshold is established at an ICDP of 10^{-5} or an ILERP of 10^{-6}. Under no circumstances is the safety limit RICT to exceed the ultimate back-stop CT limit of 30 days (as measured from the time of entry into the associated TS LCO). Plants implementing a RMTS program are required to perform a RICT assessment whenever two or more separate equipment TS LCOs are simultaneously effective. In such cases, if the calculated RICT is less than one or more of the associated individual equipment front-stop CTs, the RICT will become effective, thus becoming more restrictive than the conventional front-stop CTs. In a RMTS program, a RICT exceeding the current front-stop CT cannot be applied in cases where all trains of a TS system function have been lost or are determined to be inoperable. RICT assessments do not allow credit to be taken for repair of the affected TS LCO equipment in a configuration-specific RICT calculation.

There are two important configuration risk concepts employed in the implementation of a RMTS program to manage risk, these are instantaneous risk and cumulative risk. Figures 2-1 and 2-2 illustrate these concepts, as they apply in a RMTS program. Figure 2-1 presents an example instantaneous core damage frequency (CDF_{inst}) profile for a calendar week. Figure 2-2 presents an incremental core damage probability (ICDP) profile for the same example week.

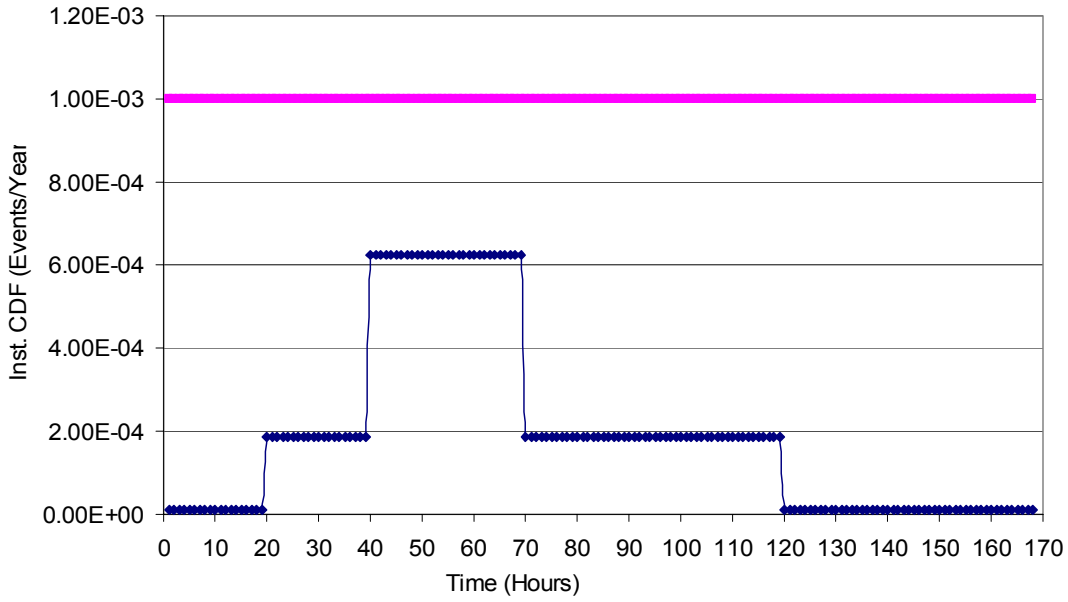

Figure 2-1
Configuration Risk Management – Instantaneous CDF Profile Example

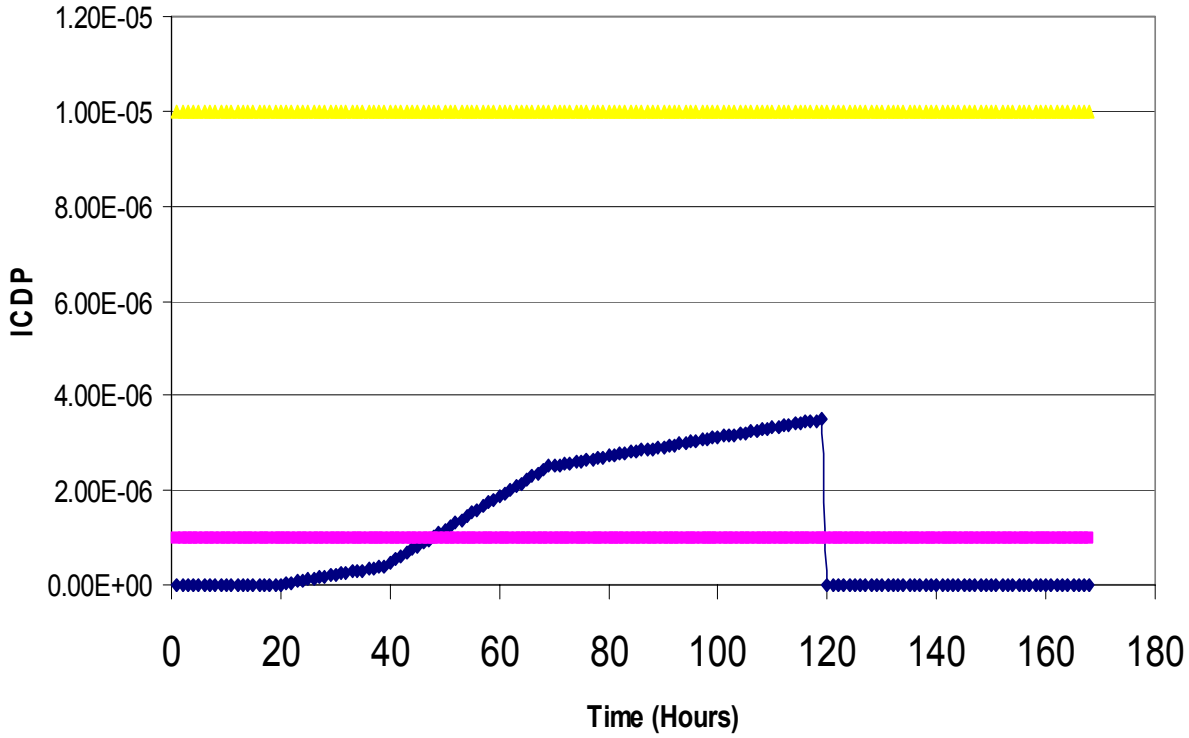

Figure 2-2
Configuration Risk Management – Incremental CDP Example

Figure 2-1 shows an example where the first step increase in instantaneous CDF, from the zero-maintenance state (see definition of "maintenance state" in Appendix A), at time = 20 hours is for a planned maintenance activity, and the second step increase in instantaneous CDF at time = 40 hours is due to an emergent unplanned failure discovered in another system. In this example, the emergent failure function is recovered at time = 70 hours, and the planned maintenance continues until time = 120 hours. It is important to note that before time = 20 hours and after time = 120 hours, the instantaneous CDF is not zero (as it may appear in this figure due to size resolution), but is equal to the zero-maintenance CDF for the plant (1.00E-05 in this example). The horizontal straight-line upper limit shown in Figure 2-1 is the instantaneous CDF safety limit threshold for RMTS (= 1.00E-03 events per year). A similar instantaneous LERF safety limit threshold for RMTS is established at 1.00E-04 events per year. It is also important to note that this is an example provided for concept communication only. It is likely that realistic plant-specific zero-maintenance CDFs will be lower, and that most realistic maintenance configurations will result in less risk accumulation over greater periods of time.

Figure 2-2 shows the same example maintenance configuration versus time profile for incremental core damage probability (ICDP). ICDP does equal zero whenever the zero-maintenance configuration is in effect, but begins to rise at time = 20 hours when the plant is placed in the originally planned maintenance configuration. When the plant transitions to the second maintenance configuration at time = 40 hours (when the emergent condition occurs or is discovered), the slope of the ICDP profile increases until the function of the emergent failure is

recovered at time = 70 hours, when the slope of the ICDP curve returns to its original value as it was under the original maintenance configuration at time = 20 hours. This profile continues until the plant is returned to the zero-maintenance configuration at time = 120 hours, at which point the ICDP profile returns to zero. Figure 2-2 shows two horizontal lines, the lower for the RMA threshold value (ICDP = 1.00E-06), and the higher for the safety limit threshold value (ICDP = 1.00E-05). In this example, the plant staff would be required to implement RMAs before the configuration risk ICDP profile increases above 1.00E-06 (at approximately time = 47 hours in this example). The concepts shown in Figures 2-1 and 2-2 are also applied to large early release probability (LERP) thresholds in RMTS. Additional guidance on RMTS thresholds and associated risk management is provided in Section 3.5 of this report.

In a RMTS program, a RICT would be calculated when the plant considers entering a TS LCO associated with a specific plant maintenance configuration (see definition in Appendix A), and it is determined that completion of maintenance allowing exiting that LCO would not be practicable within the associated front-stop CT. If, during application of a specified RICT, the plant transitions to a different maintenance configuration (e.g., due to emergent conditions), then that RICT is required to be recalculated. It is important to state that, in such situations, the operators would proceed to place the plant in a stable condition as they do under conventional TS, and not be restricted in these actions by the RMTS program. Plants implementing RMTS have configuration risk management tools, such as safety monitors, risk monitors, pre-solved configuration risk databases, etc., that can be applied to calculate configuration risk in a nearly real-time manner by the plant staff who are on-shift, or within relatively short periods of time following identification of the configuration. If the new configuration results in a TS 3.0.3 condition, then the timing for the RICT re-calculation will be determined by the required TS 3.0.3 action statement entry time.

When emergent conditions occur while a RICT is in effect, the plant would (1) take actions appropriate with managing risk in the current condition, and (2) assess the risk significance of the condition. The plant would then have up to a maximum time period of 12 hours to calculate a revised RICT. Plants exercising pre-solved configuration risk databases containing the configuration of interest meet the requirements for both preliminary and final RICT. This revised RICT would be effective from the time of implementation of the original RICT for the original maintenance configuration, and the associated maintenance "time-clock" would not be re-set to zero at the time of the modified configuration. In the RMTS framework, a RICT can be revised, occasionally many times, but not exited (or re-set to the remaining licensing period duration) until the plant satisfactorily exits all TS LCOs where the associated front-stop CT has been exceeded. In cases where the plant is found to have already exceeded the revised RMAT, the plant staff would re-evaluate the impact, implement compensatory measures or risk management actions as appropriate, and initiate a decision process to implement RMAs, including, as appropriate, transitioning the plant to a lower-risk configuration. In any case where a plant reaches or is found to have exceeded the safety limit RICT based on specified CDF/LERF/ICDP/ILERP limits (see Section 3, specifically Table 3-2), the plant would be required to take the most restrictive actions required for "ACTION NOT MET" for the affected Technical Specifications, including any associated requirement for plant shutdown implementation. Note that, during the time period following the front-stop CT but before the expiration of the applicable RICT, plants will normally implement progressively-phased risk

management actions commensurate with the projected risk during the maintenance configuration period. Additional information on establishing and implementing RMTS RICT values is presented in Section 3.5 of this report.

It is important to make clear that, when emergent conditions occur while operating under a RICT, additional equipment may not subsequently be electively or deliberately taken out of service for planned maintenance until an updated RICT has been approved that shows that such planned maintenance would not be predicted to cause the plant to exceed RMTS program risk management safety limits (see Section 3.5).

In a RMTS program, the conventional technical specification definition of equipment "operability" (see Appendix A) applies, just as it does under current existing plant technical specifications. Thus, equipment "operability" is applied by plant operating staffs to enter or exit TS LCOs. However, the issue of equipment "functionality" (see Appendix A) is broader and relates directly to the equipment's capability to support its intended safety or risk mitigation function as modeled in the plant PRA. Equipment PRA functionality will be considered in a RMTS program when assessing risk for RICT calculation. In any case where equipment declared as "inoperable" is being considered "functional" for purposes of RICT calculation, the reasoning behind such a consideration must be justified in the documentation of the RICT assessment.

3
GUIDANCE

This section describes an approach to support RMTS by estimating the overall risk of potential plant configurations and by providing information to plant personnel so that they can take appropriate actions to control it.

10CFR50.65(a)(4) requires that a risk assessment be performed prior to performing maintenance. The scope of the RMTS generally includes, at a minimum, SSCs modeled in a Level 1 PRA that have a quantifiable effect on CDF or LERF and that have been determined to be of high safety significance.

The (a)(4) process uses PRA methods and risk insights in establishing and planning maintenance activities. The RMTS program recommended herein compliments or exceeds (a)(4) requirements by using existing (a)(4) guidance in many areas and by implementing a more rigorous supplemental application in the remaining areas. The following guidance would replace the existing (a)(4) guidance for plants implementing RMTS.

3.1 Assessment Process, Control, and Responsibilities

10CFR50.65 paragraph (a)(4) states that "before performing maintenance activities (including but not limited to surveillances, post-maintenance testing, and corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities." Risk assessments are not limited to temporarily inoperable equipment but can include equipment troubleshooting, hazard barrier removal, erection of scaffolding, lifting electrical leads and installing electrical jumpers. The scope of the assessment may be limited to SSCs that a risk-informed evaluation process has shown to be significant to public health and safety. Furthermore, the (a)(4) plant maintenance evaluation is required for all plant operating modes.

The RMTS RICT evaluation process shall:

1. Be documented in plant procedures delineating appropriate responsibilities and related actions.

2. Define a process so that when the plant configuration is outside the scope of the RMTS quantitative calculation tool (e.g., risk or safety monitor software, a list of pre-calculated risk levels for specified maintenance configurations, etc.), or the tool is otherwise unavailable, quantitative approaches (e.g., bounding analyses) supplemented by qualitative methods may be used to assess risk and define appropriate actions to manage the risk increase over the duration of the maintenance configuration.

3. Use risk insights to manage overall plant risk.

In performing the RMTS RICT assessment, the decision-making process will, where appropriate, include consideration of transition risks associated with mode changes, if a mode change is required or if the condition occurs when the plant is in a non-power generating operating mode. Consideration of mode transition risk is appropriate when a mode transition is actually involved in the implementation of maintenance, and when the calculation of the maintenance configuration risk would not be bounded (as an upper bound) by a calculation of the steady-state at-power risk for the configuration of interest.

Implementation of the RMTS risk assessment process requires integration into the plant-wide work control process. The process then requires identification of the current plant maintenance configuration and performance of a risk assessment applicable to that configuration. Appropriate actions to manage the risk impacts shall then be determined and implemented.

The remainder of this report assumes that the plant is fully compliant with 10CFR50.65(a)(4). It is further assumed that the plant risk assessments integrate PRA results and PRA-derived risk insights into the process. The supplementary processes discussed in this report are intended to enhance the existing (a)(4) process in order to allow it to accommodate a greater plant control function. The primary intent of these processes is to ensure that selected desirable attributes of the current TS are pragmatically retained in the RMTS structure in a risk informed format. These attributes include:

1. Current (conventional) TS Structure

2. Reliance on defined time interval limits (i.e., front-stop CT, RICT, and back-stop CT)

3. Reference to defined actions in an LCO

The RMTS is intended to replace the fixed CT and the prescriptive actions of the current TS with an action statement to conduct a risk assessment. The structure of the proposed RMTS is illustrated in Table 3-1. Table 3-1 shows an example structure for one system only, but this structure would be repeated for other SSCs within the scope of a plant's RMTS. Note that the proposed TS references three time intervals: the front-stop CT, the 30-day (or "back-stop") CT, and the acceptable risk informed time interval (the RICT) calculated in accordance with the RMTS thresholds (see Table 3-2). The front-stop is the plant's TS CT as justified via design basis considerations or TS CT as modified via an approved RG 1.177 analysis. The 30-day completion time is provided to ensure the plant design basis is retained (that is, no permanent plant changes are made associated with this TS). The 30-day interval is not risk informed, but rather represents a deterministic limit. The level of acceptable risk beyond the front-stop is established via a risk-informed application of maintenance rule guidance [3] as follows:

1. Prior to exceeding the front-stop CT, the plant must perform a configuration risk assessment to confirm that the risk of continued operation in the existing configuration is acceptable. A quantitative risk assessment supported, by qualitative risk insights will provide the basis for continued plant operation. The RICT assessment must consider the impact of common cause failures and external events (see definition in Appendix A), including contributions from

internal fires and flooding. In addition, the assessment may credit compensatory risk management actions established during the period being evaluated.

2. Depending on the outcome of this assessment and assessment of alternative actions as appropriate, risk management actions will be defined and the plant will either continue operation beyond the front-stop CT or take other action in accordance with TS. The timing of the associated plant TS actions, to include plant shutdown, will reflect plant configuration cumulative risks.

For emergent (unscheduled) conditions, the plant staff is expected to provide an expeditious assessment of the plant risk, but in a way such as not to interfere with operator actions to control the condition. Typically, such an assessment should be performed within the front-stop CT action statement time duration associated with an emergent condition. Quantitative risk assessments will be performed with an approved plant risk model, and PRA results should be based on Level 1 PRA and LERF attributes (adequate for the assessment of maintenance configuration impacts on CDF and LERF) compatible with the associated risk informed application. Fire, seismic and/or flood risks must also be considered when establishing the duration of a proposed CT extension.

Conceptually, the implementation of the flexible CT is simple. For entries into the RMTS, the licensee will:

1. Prior to the expiration of the TS front-stop CT, a risk assessment of the maintenance configuration resulting from the inoperable equipment will be performed by using the plant CRMP containing RMTS guidance to determine the feasibility of continued power operation beyond the front-stop,

2. Based on the results of the risk assessment, the plant staff will take actions to manage risk by returning equipment to service or by implementing compensatory risk management actions, take actions in accordance with plant TS up to and including initiating a plant shutdown, and

3. Once the RICT has been entered, the RMTS risk assessment will be re-performed in accordance with the RMTS program when any emergent conditions changes the evaluated maintenance configuration. In the event of an emergent condition, a conservative screening assessment must be performed to determine if the emergent maintenance configuration represents a loss of function. This screening assessment should be performed expeditiously. If continued plant operation is expected, a quantitative screening assessment will be performed within 12 hours following any plant maintenance configuration change.

The RICT assessment process will focus on the entire maintenance evolution and will utilize the quantitative action thresholds of Section 11.3.7.2 of Reference 3. RICT risk assessments will be performed to assess the incremental risk of the inoperable equipment associated with maintenance configurations targeted for RICT implementation. These latter results will be tracked, trended, and periodically reviewed to ensure that the cumulative risk of the flexible TS is small [5]. Furthermore, this process will reduce the potential for performing higher risk maintenance beyond the front-stop. For conditions where risk consideration alone would result

in a very long RICT, restoration of low risk, design basis configurations will be ensured by the back-stop CT.

The process for conducting and using the result of the risk assessment in plant decision-making will be documented (see Section 3.7). An example general process flowchart for RMTS risk assessment and implementation is presented in Figure 3-1. The procedures should specify the plant functional organizations and personnel, including operations, engineering, and risk assessment (PRA) personnel, responsible for each step of the procedures. The procedures should also clearly specify the process for crediting RMAs, conducting, reviewing, and approving the assessment. In cases where a RICT assessment cannot be performed (e.g., when the configuration risk cannot be adequately addressed via the CRM program and PRA), the normal front-stop CT(s) will be applied.

For plants implementing a RMTS program, the development and maintenance of a "pre-analyzed" list of maintenance configurations with associated RICT values is recommended. This list does not necessarily need to address all SSCs affected by TS LCOs, but should address reasonable combinations of disabled safety function equipment trains and instrument channels.

Table 3-1
Generic Risk-informed CTS with a Back-stop: Example Format

Actions Condition		Required Action		Completion Time
B.	Subsystem inoperable.	B.1	Restore subsystem to OPERABLE status.	72 hours
		OR		
		B.2.1	Determine that the completion time extension beyond 72 hours is acceptable in accordance with established RMTS thresholds.	72 hours
			AND	
		B.2.2	Verify completion time extension beyond 72 hours remains acceptable.	In accordance with the RMTS Program.
		AND		
		B.2.3	Restore subsystem to OPERABLE status.	30 days or acceptable completion time, whichever is less.

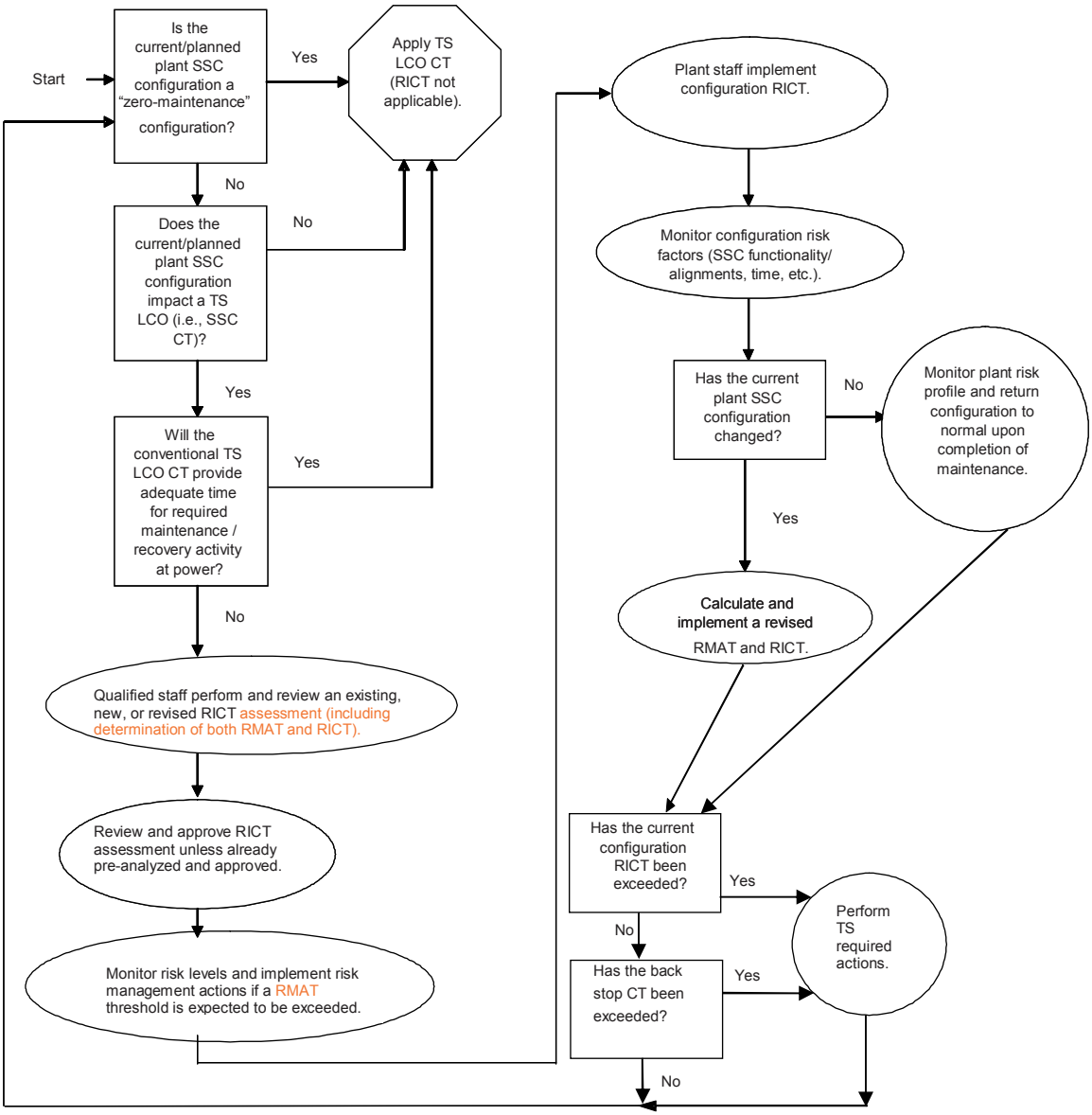

Figure 3-1
Example Process Flowchart for RMTS RICT Assessment and Implementation

3.2 General Guidance for the RICT Assessment

1. Power Operating Conditions are defined as plant modes other than hot shutdown, cold shutdown, refueling, or defueled. Section 3.3 describes the scope of SSCs subject to the assessment during power operations.

2. The risk assessment method for RICT determination must use quantitative approaches, but can also be supported by qualitative approaches.

3. The quantitative assessment should be based on the plant Maintenance Rule (a)(4) risk assessment program supported by the plant PRA. In specific instances, bounding assessments may be appropriate (i.e., in cases where a simplified bounding risk assessment is convenient and can show that a RICT calculated via an upper bound configuration risk yields ample time for maintenance implementation).

4. The RICT assessment should consider the following:
    - Availability of other equipment to perform the safety function(s) served by the out-of-service SSC
    - Potential for common cause failure of redundant equipment
    - The anticipated duration of the out-of-service or testing condition
    - The likelihood of an initiating event or accident (including both internal and external events as defined in References 19 and 20) that would require performing the affected safety function
    - The likelihood that the plant maintenance configuration will significantly increase the frequency of a risk-significant initiating event [19 and 20] (as determined by each licensee, consistent with its obligation to manage maintenance-related risk)
    - Component and system dependencies that are affected
    - The degree of reliance on Maintenance rule components with (a)(1) status
    - Compensatory risk management actions taken to mitigate the risks, e.g., alignment of cross-ties with other units, installation of temporary systems.

5. Assessments may be pre-determined (i.e., performed prior to an actual need), or they may be performed on an as-needed basis.

6. The degree of depth and rigor used in managing risk should be commensurate with the complexity of the planned configuration and the level of expected risk.

7. Maintenance may involve altering the facility or procedures for the duration of the maintenance activity. Examples of such alterations include jumpering terminals, lifting leads, placing temporary lead shielding on pipes and equipment, removing barriers, and using temporary blocks, bypasses, scaffolding and supports. The assessment should include

consideration of the impact of these alterations on plant safety functions qualitatively or quantitatively depending on the significance of the alteration.

8. For surveillance testing or situations where the maintenance activity has been planned in such a manner to allow for prompt restoration of SSC functions, the assessment may take into account the likelihood and restoration time of out-of-service SSCs being promptly restored to service in response to emergent conditions. In this context, the terms "prompt" and "promptly" mean that the restoration of SSC function occurs prior to its associated demand for risk mitigation, given the occurrence of a predicted emergent condition or event sequence that affects plant safety (and risk).

9. Emergent conditions (see definition in Appendix A) may require action prior to completing the assessment, or could change the conditions of a previously performed assessment. Examples include plant maintenance configuration or mode changes, additional SSCs out of service due to failures, or significant changes in external conditions (e.g., weather and offsite power availability). The following guidance, consistent with Reference 3, applies to such situations:

    - The safety assessment should be performed (or re-evaluated) to address the changed plant conditions on a reasonable schedule commensurate with the safety significance of the condition.
    - Performance (or re-evaluation) of the assessment should not interfere with, or delay, the operator and/or maintenance crew from taking timely actions to restore the equipment to service or take compensatory actions.
    - If the plant configuration is restored prior to the required re-evaluation risk assessment the assessment need not be performed for purposes of supporting that maintenance activity. However, an accounting of the maintenance configuration should be included in the plant's administrative program for controlling long-term cumulative or aggregate risk (see Section 3.5.2).

3.3 Scope of RMTS and RMTS Assessment

The NRC Maintenance Rule requirements for plant maintenance configuration risk assessment are stated in 10 CFR 50.65(a)(4). 10 CFR 50.65(a)(4), states "The scope of the Systems, Structures and Components (SSCs) to be addressed by the assessment may be limited to those SSCs that a risk-informed evaluation process has shown to be significant to public health and safety." Thus, the scope of SSCs subject to the RMTS assessment provision may not include all SSCs that meet sections (b)(1) and (b)(2) maintenance rule scoping criteria.

From a practical standpoint, a RMTS program defines the scope of equipment that will be used to define maintenance configurations (see definition of "maintenance configuration" in Appendix A). Generally, equipment included within a maintenance configuration are those associated with SSCs that are included within the scope of current technical specifications LCOs and included in a plant's CRMP. Therefore, they have front-stop CT requirements, and can be evaluated via the RMTS-supporting PRA and CRMP, but exclude design-related technical

specifications, such as safety limits and limiting safety system settings (e.g., reactivity control, power distribution parameters, etc.).

The PRA provides an appropriate primary mechanism to define the RICT assessment scope, as the PRA scope considers dependencies and support systems; and, through definition of top events, cut sets, and recovery actions, includes those SSCs that could, in combination with other SSCs, result in significant risk impacts. Thus, the risk informed assessment scope may be limited to the following scope of SSCs:

1. Those SSCs included in the scope of the plant's Level 1 and LERF (or Level 2 if available), internal (and, if available, external) events PRA, and;

2. SSCs in addition to the above that have been determined to have high safety significance through the process described in Section 9.3 of NUMARC 93-01 [3].

3.4 Assessment Methods for Power Operating Conditions

Unless the plant employs a full scope (all important internal and external initiators) CRM program with results appropriately aggregated to a total CDF, ICDP, and ILERP; removal of a single SSC from service for longer than its front-stop CT, or simultaneous removal from service of multiple SSCs for longer than the most limiting front-stop CT, may require an assessment using blended (quantitative supported by qualitative) methods consistent with Reference 3 guidance. Sections 3.4.1 and 3.4.2 provide guidance regarding quantitative and qualitative considerations, respectively.

3.4.1 Quantitative Considerations

1. The assessment process shall be performed via a tool or method that considers quantitative frequencies from the PRA. Acceptable tools include the PRA model, safety/risk monitor, risk matrix, or pre-analyzed list derived from the PRA insights. To properly support the assessment, the PRA must have certain attributes, and it must reasonably reflect the actual plant configuration. Section 3.5.2 provides guidance on various approaches for using the output of a quantitative assessment to manage risk.

2. If the PRA does not directly model the SSC to be removed from service (e.g., the SSC is part of the RPS system, diesel generator, etc. which has been modeled as a "single component"), the assessment should consider the impact of the out of service SSC on the safety function of the modeled component. SSCs are considered to support the safety function if the SSC is significant to the success path for function of the train or system (e.g., primary pump, or valve in primary flow path). However, if the SSC removed from service does not contribute to the unavailability of the associated train or system safety function (e.g., indicator light, alarm, drain valve), the SSC would not be considered to support the safety function.

3.4.2 Qualitative Considerations

RMTS is fundamentally based on the ability to calculate a RICT. Qualitative assessments may be used, if necessary, to supplement the quantification. The purpose of the qualitative assessment is to confirm that the aspects not comprehensively addressed in the quantitative assessment do not have a significant effect on the calculated RICT. If the qualitative assessment cannot provide this assurance, then the evaluation should do one of the following prior to extending the CT:

- enhance the quantification, or
- identify appropriate risk management actions

The quantitative assessment should be supplemented, if necessary, by a qualitative evaluation designed to address issues that may not be comprehensively addressed in the quantitative assessment. For example, the impact of the maintenance activity upon key safety functions may be addressed as follows:

- Identify key safety functions affected by the SSC planned for removal from service.
- Consider the degree to which removing the SSC from service will impact the key safety functions.
- Consider degree of redundancy, duration of out-of-service condition, and appropriate compensatory measures, contingencies, or protective actions that could be taken, if appropriate, for the activity under consideration.

1. For power operation, key plant safety functions are those that ensure the integrity of the reactor coolant pressure boundary, ensure the capability to shut down and maintain the reactor in a safe shutdown condition (see definition in Appendix A), and ensure the capability to prevent or mitigate the consequences of accidents that could result in potentially significant offsite radiation exposures.

2. The key safety functions are achieved by using systems or combinations of systems. The configuration assessment should consider whether the maintenance activity would:
    - Affect the likelihood of a PRA initiating event [19 and 20]
    - Involve a significant potential to cause a scram or safety system actuation
    - Result in significant complications to recovery efforts.

3. Depending on the level of anticipated configuration risk, risk impacts of equipment outages may be determined via approximate or bounding analyses. Guidance on bounding analyses for PRA applications is provided, for example, in the industry guidance [36] for implementation of 10 CFR 50.69.

4. Qualitative considerations may also be necessary to address external events (see definition in Appendix A), including internal fires, and SSCs not in the scope of the Level 1, internal events PRA (e.g., SSCs included in the assessment scope because of Maintenance Rule expert panel considerations).

5. The assessment may need to consider actions that could affect the ability of the containment to perform its function as a fission product barrier. With regard to containment performance, the assessment should consider:
    - Whether new containment bypass conditions are created, or the probability of containment bypass conditions is increased
    - Whether new containment penetration failures that can lead to loss of containment isolation are created
    - Whether redundant or diverse containment safeguards should be available, if maintenance is performed on SSCs of the containment systems (or SSCs upon which containment functions are dependent).

6. External event, including internal fires and floods, (see definition in Appendix A) considerations involve the potential impacts of weather and other external conditions relative to the proposed maintenance evolution.

3.5 Managing Risk

Risk management uses the risk assessment in plant decision-making to control the risk impact. This process involves coordination with planning, scheduling, monitoring, maintenance, and operations activities.

The objective of risk management is to manage the temporary and aggregate risk increases from maintenance activities. This control is accomplished by using target RMAT values to plan and schedule maintenance such that the risk increases are identified and managed. As RMATs are approched, the plant staff will take additional actions beyond routine work controls and endeavor to maintain adequate margin between the actual maintenance configuration duration and the RICT. RICT values for a specific maintenance configuration are calculated simply by dividing the appropriate associated cumulative risk limit in Table 3-2 by its configuration instantaneous risk frequency.

Management of risk also considers aggregate risk impacts. (Aggregate risk is the collective risk impact over time. Aggregate risk is also known as cumulative risk, but, within the context of a RMTS program, refers to time periods longer than those associated with specific plant maintenance configurations. Aggregate risk is most effectively tracked via one or more standard time periods associated with plant operation (e.g., one calendar year, one refueling cycle, a rolling 52-week period, etc.). Aggregate risk is controlled to a degree through maintenance rule guidance [3] requirements to establish and meet SSC performance criteria. These requirements include considering the risk significance of SSCs in establishing performance goals. Plants that implement RMTS should develop measures to assess the aggregate risk relative to the average risk. This assessment could be accomplished through a periodic assessment of previous out-of-service conditions, such as the annual accounting of configuration risk assessments required by 10CFR50.65(a)(3). Such an assessment may involve quantitatively estimating cumulative risks or may involve qualitatively assessing the risk management approach employed.

The PRA provides valuable insights for risk management, because it relates events and systems. Risk management can often be effectively supported by using qualitative insights from the PRA, rather than sole reliance on quantitative information. Removing equipment from service may alter the significance of various risk contributors from those identified via a typical PRA designed to calculate average annual risk. Specific configurations can result in increased importance of certain initiating events [19 and 20], or of systems and equipment used to mitigate accidents. Evaluating specific configurations can identify "low order" cut sets or sequences that may not be important in the "annual average" risk analysis but become important for a specific configuration. These considerations are very important to risk management within a RMTS program.

A key risk management activity is assessing the risk impact of planned maintenance. In conjunction with scheduling the sequence of activities, compensatory risk management actions may be taken that reduce the temporary risk increase, if determined to be necessary. Since many of the risk management actions involve non-quantifiable factors, the risk reduction would not necessarily be quantified. The following sections discuss approaches for the establishment of thresholds for the use of risk management actions.

3.5.1 Qualitative Considerations Supporting Action Thresholds

RMTS risk management action thresholds (i.e., plant conditions and associated configuration risk levels determining when risk management actions are required) must be established quantitatively, but they should also be supported qualitatively by considering the performance of key safety functions, or the remaining mitigation capability, given the out-of-service SSCs. Qualitative methods to support risk management actions would generally be necessary to address SSCs not modeled in the PRA. This approach typically involves consideration of the following factors in the assessment:

- Duration of out-of-service condition, since longer duration results in increased exposure time to initiating events
- The type and frequency of initiating events that are mitigated by the out-of-service SSC, considering the sequences for which the SSC would normally serve a safety function
- The impact of the plant configuration on the initiating event frequencies
- The number of remaining success paths (redundant systems, trains, operator actions, recovery actions) available to mitigate the initiating events
- The likelihood of proper function of the remaining success paths

The above factors can be used as the basis for establishing a matrix, or list of configurations and associated applicable risk management actions.

3.5.2 Establishing Action Thresholds Based on Quantitative Considerations

3.5.2.1 Quantitative Risk Action Thresholds

The thresholds for risk management actions should be established quantitatively by considering the magnitude of the instantaneous core damage frequency (CDF_{inst}), instantaneous large early release frequency ($LERF_{inst}$), incremental core damage frequency (ICDF), and the incremental large early release frequency (ILERF) for the maintenance configuration of interest. It is important to note that these incremental frequency values are measured from their respective "no-maintenance" or "zero-maintenance" baseline frequencies as determined via the plant PRA (see definitions of terms in Appendix A). Plants should consider factors of duration in setting the risk management acceptance guidance. Duration may be either a particular out-of-service condition or a specific defined work interval (e.g., shift, day, week, etc). The product of the configuration ICDF or ILERF and the effective duration of the associated configuration is expressed as a configuration incremental core damage probability ($ICDP_{config}$) or configuration incremental large early release probability ($ILERP_{config}$) respectively.

Guidance for evaluating temporary risk increases by considering configuration-specific CDF_{inst}, as well as $ICDP_{config}$ and $ILERP_{config}$ is provided in NUMARC 93-01, Revision 3 [3]. When combined with the other elements of maintenance rule guidance, and other quantitative or qualitative measures deemed appropriate by the plant staff and described in a plant's RMTS program request submittal, this guidance is acceptable for RICT implementation:

- Maintenance configurations with a configuration-specific CDF_{inst} in excess of 10^{-3} per year or a configuration-specific $LERF_{inst}$ in excess of 10^{-4} per year must be carefully considered by the plant staff before operators voluntarily enter such configurations. If such configurations are entered, it should be for very short periods of time and only with a clear detailed understanding of which events dominate the risk level.
- Quantitative risk acceptance guidelines using $ICDP_{config}$ and $ILERP_{config}$ for a specific maintenance configuration are presented in Table 3-2. The quantitative risk acceptance guidelines presented in Table 3-2 are consistent with NEI Maintenance Rule (a)(4) guidance [3]. Applicable RICT values are calculated simply by dividing the incremental cumulative risk probability values in Table 3-2 by their associated instantaneous incremental configuration risk frequency parameters (e.g., (ICDP limit)/(ICDF) or (ILERP)/(ILERF), converted to hours). These risk acceptance guidelines should be considered with respect to establishing risk management actions and, when appropriate, taking TS-required actions, including, where specified by applicable TS, plant shutdown.

Table 3-2
RMTS Quantitative Risk Acceptance Guidelines

Criterion		Maintenance Rule Risk Management Guidance	RMTS Risk Management Guidance
CDF_{inst}	$LERF_{inst}$		
$>10^{-3}$ events/year	$>10^{-4}$ events/year	- Careful consideration before entering the configuration (none for $LERF_{inst}$)	- Implement most restrictive actions required for "ACTION NOT MET" for the affected Technical Specifications
ICDP	ILERP		
$>10^{-5}$	$>10^{-6}$	– Configuration should not normally be entered voluntarily	- Implement most restrictive actions required for "ACTION NOT MET" for the affected Technical Specifications
10^{-6} - 10^{-5}	10^{-7} - 10^{-6}	– Assess non-quantifiable factors – Establish risk management actions	– Assess non-quantifiable factors – Establish risk management actions
$<10^{-6}$	$<10^{-7}$	– Normal work controls	– Normal work controls

This guide provides a risk management scheme based on incremental risk metrics as supported by application of Reference 3, Reference 4, 10 CFR 50.65(a)(4), and related maintenance configuration risk management policies currently in effect. In a RMTS program the 10^{-6} and 10^{-7} thresholds for ICDP and ILERP, respectively, are referred to as RMA time (RMAT) RMTS thresholds, while the 10^{-5} and 10^{-6} thresholds for ICDP and ILERP, respectively, are referred to as "safety limit" RICT, or simply RICT, RMTS thresholds. These thresholds are deemed appropriate for RMTS programs because they relate to integrated plant (versus single system) risk impacts that are occasional and temporary in nature (versus permanent).

3.5.2.2 RICT Calculation and Application

Using this framework for risk management, the plant staff can calculate target RMATs and safety limit risk-informed allowed outage times or RICTs. For planned maintenance, target outage times should be established at low risk levels and should be accompanied by normal work controls. The process to manage the risk assesses the rate of accumulation of risk in plant configurations and determines acceptability of continued plant operation (beyond the front-stop CT) based on risk assessment, alternative actions and the impact of compensatory risk management actions. As the plant approaches the RMAT threshold, associated risk management actions (RMAs) should be considered and, where deemed appropriate by plant operators, implemented. These RMAs may be quantified to determine revised RICT values, but this

quantification of RMAs is neither expected nor required, as omission of this RMA quantification results in conservatively short RICT values. It is generally in a plant's best interest to quantify RMAs, if practicable, to determine realistic RICT values. For a plant to be eligible to quantify RMAs for RICT credit, it must be able to determine the associated RMA risk impacts on and from the following: SSC functionality; new configurations of existing PRA basic event cut sets; new temporary equipment functions; and new or modified human actions. If the plant chooses to quantify RMAs, it must apply a pre-existing documented and approved process (including associated procedures and administrative controls) for this purpose, and it must meet NRC Regulatory Guide 1.200 and applicable ASME standards. As the plant approaches safety limit RICT values, it must take action to transfer to a safer maintenance configuration. If the plant meets or exceeds safety limit RICT values, it must implement the associated most restrictive TS-required actions for "ACTION NOT MET" for the affected Technical Specifications LCOs. These actions may include plant shutdown, where required by current TS. Plants implementing a RMTS program are required to perform a RICT assessment whenever two or more separate equipment TS LCOs are simultaneously effective. In such cases, if the calculated RICT is less than one or more of the associated individual equipment front-stop CTs, the RICT will become effective, thus becoming more restrictive than the conventional front-stop CTs. In a RMTS program, a RICT exceeding the current front-stop CT cannot be applied in cases where all trains of a TS system function have been lost or are projected to be inoperable. RICT assessments do not allow credit to be taken for repair of the affected TS LCO equipment in a configuration-specific RICT calculation.

As stated in Section 2, when emergent conditions occur that change the plant maintenance configuration, and thus, the associated configuration risk profile for the plant, the RICT must be re-evaluated. When such emergent conditions occur while a RICT is in effect, the plant would have a maximum of 12 hours to perform a revised RICT assessment. If the plant has a previously approved safety function determination program (SFDP) for plant SSCs, this RICT determination should be consistent with the determinations and resulting actions of that program. This revised RICT would be effective from the time of implementation of the original RICT for the original maintenance configuration, and the associated maintenance "time-clock" would not be re-set to zero at the time of the modified configuration. In the RMTS framework, a RICT can be revised, occasionally many times, but not exited (or re-set to the remaining licensing period duration) until the plant satisfactorily exits all TS LCOs where the associated front-stop CT has been exceeded. It is important to note that this RICT re-evaluation process is required whenever emergent conditions change the configuration risk profile of the plant, even when only non-TS equipment functions are involved in the emergent conditions. By including this requirement, it is readily evident that a RMTS program can result in lower cumulative risk over time for the RMTS-implementing plant as compared to a conventional TS safety management process for the same plant.

The application of a configuration-specific RICT is strictly a "configuration-based" risk management activity. That is, a specified RICT is directly associated with an "off-normal" plant SSC configuration that is considered temporary. The RICT must be used in concert with "aggregate" or longer-term "cumulative" risk management policies, based on qualitative and quantitative criteria described in References 4 and 5. However, this longer-term cumulative risk would be managed via an administrative process incorporated within the plant RMTS program,

and, unlike the RICT implementation described in Table 3-2, would not be directly linked to TS required actions. An example of an acceptable general administrative cumulative risk management process could be encompassed within the plant's 10CFR50.65(a)(3) evaluation and documentation practices. In this evaluation and documentation scheme, the plant would be required to document maintenance configurations where a RICT has been applied. Another example of an acceptable general administrative cumulative risk management process could be tracking cumulative risk via a 52-week rolling average that is updated weekly to account for incremental risk above the zero-maintenance baseline risk. Alternatively, the plant could meet this requirement by documenting the zero-maintenance baseline risk for the plant along with the changes or "deltas" from that baseline, or just quantify the "deltas" from the baseline on an annual basis. The administrative process for aggregate or cumulative risk management must be described in the plant's RMTS program request submittal to the NRC. This administrative process for aggregate risk management should include a requirement to document specific corrective actions for returning to operation within Regions II or III of Figures 3 or 4 of NRC Regulatory Guide 1.174, if the plant aggregate risk tracking shows an actual or imminently potential excursion into Region I of either of these figures due to RMTS-related RICT implementation. The RMTS program implementation request submittal to the NRC should clearly describe how aggregate risk tracking and associated "triggers" for self-assessment and corrective action will be implemented within the plant-specific RMTS program. Application of the risk assessment to manage allowed time in different plant configurations is complemented by the station's programs to monitor performance indicators for long-term availability of risk-significant components under the maintenance rule. The requirements to achieve acceptable long-term performance indicator goals and to maintain operation within Regions II or III of Regulatory Guide 1.174, Figures 3 and 4 provide an appropriate disincentive to the plant staff for regularly extending front-stop CT values to the detriment of safety risk and safety function availability.

RMTS-implementing plants must appropriately consider the issue of uncertainty when determining configuration RICT values for plant-specific applications (see Reference 37 for guidance on treatment of uncertainty in PRAs). However, the RICT quantitative acceptance guidelines established herein have the following fundamental basis. RMTS-implementing plants must have PRAs of acceptable quality and capability yielding zero-maintenance CDF and LERF probability distributions meeting established criteria applicable to 10CFR50.65(a)(4) applications. Specifically, the implementation of plant-approved configuration risk management models must satisfy Reference 19 Capability Category 2 requirements (as modified by RG 1.200) and the associated uncertainty analysis requirements therein. Therefore, application of PRA-calculated mean values (see definitions in Appendix A) for configuration risk compared with the risk acceptance guidelines provided herein should meet acceptable uncertainty criteria for safe and prudent RICT implementation. It is important to note that unquantified RMAs tend to counter any non-conservative risk quantification uncertainty when implementing RICTs, and therefore, may be applied to aid in addressing uncertainty issues.

It is recommended that prior to NRC approval and plant implementation of the RMTS RICT, a demonstration of the risk informed evaluation and control processes be performed. This demonstration may include a limited post assessment of a previous refueling cycle's maintenance, or assessment of past NOEDs and a demonstration of how such situations would be

handled when the RMTS process is instituted. In addition, a set of pre-defined failures of TS components can be postulated in the process of a normal maintenance schedule and the impact of delayed repair on plant risk and actions can be evaluated. Results of these studies may be used to inform the utility and NRC staff of the plant's program for implementing the RICT (see Appendix C).

3.5.2.3 External Events Consideration

Plants with external events PRAs, including internal fires, will apply them in the RMTS RICT assessment process. Plants without external events PRAs must apply the following logic to support maintenance activities beyond the front-stop CT:

1. They must be able to provide a reasonable technical argument (to be documented prior to the implementation of the associated RICT) that the configuration risk of interest is dominated by internal events, and that external events, including internal fires, are an insignificant contributor to configuration risk, or

2. They must be able to perform a reasonable bounding analysis of the external events, including internal fires, contribution to configuration risk (to be documented prior to the implementation of the associated RICT) and apply this upper bound external events risk contribution along with the internal events risk contribution in calculating the configuration risk and the associated RICT, or

3. They must identify and implement risk management actions that, for the duration of the configuration of interest, enable them to provide a reasonable technical argument (to be documented prior to the implementation of the associated RICT) that external events, including internal fires, are an insignificant contributor to configuration risk.

Combination of Items 2 and 3 above are also acceptable. The "reasonable bounding analyses" identified in Item 2 above must be case-specific and technically verifiable, and they must be shown to be conservative from the perspective of RICT determination (i.e., result in conservatively-low RICT values). An example of an acceptable bounding analysis method for screening fire risk in a RMTS program is presented in Reference 38. It is the intent of the RMTS process to consider the total plant risk. Plants with full scope PRAs will be able to perform integrated quantitative risk assessments to support their RMTS programs. However, it is expected that many of the plants intending to utilize the flexible CT will have robust Level 1 and LERF PRAs and qualitative risk insights associated with fire, seismic and external flooding assessments. Previously documented and approved checklists may be used to identify components where external events, including internal fires, overlaps are not significant and to limit maintenance in areas when the component risks are dominated by external event contributions. PRA capability requirements must be commensurate with the guidelines presented in Section 4.

3.5.2.4 Common Cause Failure Consideration

As previously stated in this report, common cause failure must be considered when evaluating maintenance configuration RICT values. In general, it is anticipated that the PRA applied to support RMTS programs will incorporate a relatively robust treatment of common cause failure (CCF). RICTs calculated via these PRAs automatically incorporate conditional probabilities of common cause component group failures. In practice, when emerging conditions associated with one train of a common cause component group occur and are discovered, the licensed operators must make the determination as to whether or not common cause failures could exist in one or more of the remaining functional trains of the common cause group of interest. If they determine that CCF exists (e.g., that more than one common cause group functional train is affected), then they are usually required to take expeditious action via conventional TS (e.g., TS 3.0.3). Therefore, in virtually all cases for most plants, the operators will determine if a component failure mode could exist in other functional trains of the same systems. This activity is performed prior to any RICT being calculated or implemented. In these cases, the RICT can be calculated applying the independent failure probability of the SSC discovered to be failed.

In cases where a common cause group SSC has been determined to have failed, but the operators require a delay in the determination of operability and functionality of the remaining SSCs in the common cause group, the RICT may optionally be calculated by applying a PRA SSC model alignment that considers the emergently-failed equipment out of service. This will automatically incorporate CCF for the remaining trains in the common cause group, if the model is correctly developed. Similarly, some plant staffs can apply this modified CCF logic in their PRA models by setting the emergently-failed equipment to "failed" or "true" in the associated PRA logic model basic event(s), and then calculating the associated RICT. For the time period after discovery of the initial common cause group SSC failed, but before determination of the operability and functionality of the remaining common cause group SSCs, a RICT may be determined via the PRA by setting the remaining common cause group train composite failure probability to be equal to its global conditional probability of failure (this is equal to the common cause "beta" factor in most simple two-train PRA models). This process would yield a RICT shorter than the associated normal independent failure RICT that could be implemented in the RMTS program until a more definitive determination of the existence or extent of CCF could be made by the plant staff. In any case, CCF must be incorporated into the RICT calculation based on operator knowledge of the extent of SSC functional condition, commensurate with the risk significance of the known failed component. The plant-specific process for incorporating CCF consideration into its RMTS RICT calculation process must be described in its RMTS program request submittal to the NRC.

3.5.3 Risk Management Actions

Determining actions, individually or in combinations, to control risk for a maintenance activity is specific to the particular activity (or maintenance configuration), its impact on risk, and the practical means available to control the risk. Normal work controls would be employed for configurations having predicted risk levels within RMTS lower-level thresholds (risk-informed safety criteria) presented in Table 3-2. This guidance means that the normal plant work control

processes are followed for the maintenance configuration, and that no additional actions to address risk management are necessary.

Risk management actions, up to and including plant shutdown, should be implemented for plant configurations whose instantaneous and cumulative risk measures are predicted to approach or exceed lower-level RMTS thresholds. The benefits of these actions may or may not be easy to quantify. These actions are aimed at providing increased risk awareness of appropriate plant personnel, providing more rigorous planning and control of the maintenance activity, and taking steps to control the duration and magnitude of the increased risk. Examples of risk mitigation/management actions are as follows:

1. Actions to provide increased risk awareness and control:
    - Discuss planned maintenance activity and the associated maintenance configuration risk impact with operations and maintenance shift crews and obtain operator awareness and approval of planned evolutions
    - Conduct pre-job briefing of maintenance personnel, emphasizing risk aspects of planned maintenance evolutions
    - Request/require that system engineer(s) be present for the maintenance activity, or for applicable portions of the activity
    - Obtain plant management approval of the proposed activity
    - Identify return-to-service priorities
    - Identify important remain-in-service priorities
    - Place warning signs or placards in the entry ways to protect other in-service risk significant equipment
2. Actions to reduce duration of maintenance activity:
    - Pre-stage required parts and materials accounting for likely contingencies
    - Walk-down the anticipated associated system tagout(s) and key equipment associated with the specified maintenance activity(ies) prior to conducting actual system tagout(s) and performing the maintenance
    - Develop critical activity procedures for risk-significant configurations, including identification of the associated risk and contingency plans for approaching/exceeding the RICT target.
    - Conduct training on mockups to familiarize maintenance personnel with the activity prior to performing the maintenance
    - Perform maintenance around the clock rather than “day-shift only”
    - Establish contingency plan to restore key out-of-service equipment rapidly if and when needed

3. Actions to minimize the magnitude of risk increase:
    - Minimize other work in areas that could affect related initiating events (e.g., reactor protection system (RPS) equipment areas, switchyard, diesel generator (D/G) rooms, switchgear rooms) to decrease the frequency of initiating events that are mitigated by the safety function served by the out-of-service SSC
    - Identify remain-in-service priorities and minimize work in areas that could affect other redundant systems (e.g., HPCI/RCIC rooms, auxiliary feedwater pump rooms), such that there is enhanced likelihood of the availability of the safety functions at issue served by the SSCs in those areas
    - Establish alternate success paths (provided by either safety or non-safety related equipment) for performing the safety function of the out-of-service SSC
    - Establish other compensatory measures as appropriate
    - A final action threshold (i.e., a cumulative risk threshold) should be established such that plant staffs are discouraged from routinely and repeatedly entering risk significant configurations voluntarily.
    - Return equipment to service to reduce risk levels.
    - Postpone maintenance activities, if appropriate, to maintain or reduce risk levels.

Technical specifications LCO required actions, up to and including controlled plant shutdown, should be considered for plant configurations where instantaneous and cumulative risk measures are predicted to exceed upper-level RMTS thresholds presented in Table 3-2. The plant RMTS program should include a clear decision process for determining when plant shutdown should be implemented as a result of maintenance configuration risk. An RMTS program shutdown decision process should include the following considerations:

- Evaluation of the projected integrated maintenance configuration risk (e.g., is risk unacceptably high based on Table 3-2 thresholds?)
- Evaluation of the projected maintenance configuration duration and complexity (short and simple versus long and complex)
- Evaluation of the potential challenges to maintenance-affected SSCs imposed by a plant shutdown
- Evaluation of the alternative risk imposed by shutting the plant down (does the difference in integrated plant risk projected as a result of shutting down represent a significant "risk benefit" over the increased operational risk projected as a result of remaining at power?)

In this process, risk is "acceptable" when it is projected to remain within the upper-level RMTS thresholds (safety limit criteria) presented in Table 3-2.

3.6 Regulatory Treatment of Compensatory Measures

Using compensatory measures is discussed in several sections of this guide and in Reference 3. These measures may be employed, either prior to or during maintenance activities, to mitigate risk impacts. The following guidance discusses the applicability of 10 CFR 50.65 (a)(4) and 10 CFR 50.59 to the establishment of compensatory measures (also called risk management actions in this guide). There are two circumstances of interest:

1. The compensatory measures are established to address a degraded or nonconforming condition, and will be in effect for a time period prior to conduct of maintenance to restore the SSC's condition. Per NRC Generic Letter 91-18, Revision 1 (and NEI 96-07, Revision 1), the compensatory measures should be reviewed under 10 CFR 50.59. If the compensatory measures are put into effect prior to performance of the maintenance activity, no immediate assessment is required by 10 CFR 50.65 (a)(4), however an assessment would be required prior to performing maintenance to address a degraded or nonconforming condition.

2. The compensatory measures are established as a risk management action (RMA) to reduce the risk impact during a planned maintenance activity. The 10 CFR 50.65 (a)(4) assessment should be performed to support the conduct of the corrective maintenance, and those compensatory measures that will be in effect during performance of the maintenance activity. The compensatory measures would be expected to reduce the overall risk of the maintenance activity. The impact of the measures on plant safety functions may, but are not required to, be considered quantitatively as part of the risk evaluation and RICT determination (see Section 3.5.2.1). Since the compensatory measures are associated with maintenance activities, no review is required under 10 CFR 50.59, unless the measures are expected to be in effect during power operation for greater than 90 days (far greater than the RMTS back-stop CT of 30 days).

3.7 Documentation

The following are guidelines for documentation of the risk assessment:

1. Similar to 10 CFR 50.65 paragraph (a)(4) of the maintenance rule, the purpose of the RMTS program RICT assessment is to assess impacts on plant risk or key safety functions due to maintenance activities. This purpose must be affected through establishment of plant procedures that address process, responsibilities, and decision approach. It may also be appropriate to include a reference to the plant (a)(4) procedures and other appropriate plant procedures that govern planning and scheduling of maintenance or outage activities in the RICT assessment documentation. The RICT assessment process itself will be documented.

2. Also similar to (a)(4), it is not necessary to document the basis of each RICT assessment for removal of equipment from service as long as the RICT assessment process is followed. However, risk assessments and risk management actions for each entry into RMTS that exceeds the associated conventional technical specification "front stop" CT must be documented. A checklist approach may be applied in the documentation of individual

applications of a RMTS RICT. Specific documentation requirements for RICT evaluation and implementation must be clearly described in each plant's submittal to the NRC requesting implementation of a RMTS program.

3. Documentation of RICT implementation must be adequate for regulatory inspectors to verify the assumptions and results of the configuration risk management process applied for RICT determination.

It is recommended that plants include, or make available, the following information in their RICT assessment documentation:

1. Reason for initially not meeting the TS LCO.
2. Reason for extended operation beyond the front stop CT.
3. Estimated CDF and LERF upon not meeting the TS LCO.
4. Concurrent component outages.
5. Actual CDP and LERP experienced during the associated maintenance configuration.
6. Time of entry into the portion of the RICT that is beyond the front stop CT.
7. Time of exit from the TS action statement, if entered.
8. Resolution/treatment of potential common cause failure conditions (for emergent failures only) via the Operability Determination Process.
9. Compensatory measures or RMAs implemented by the plant to manage risk of the associated maintenance configuration.
10. Documentation of the post-maintenance review.

Also, the RMTS program establishment request submittal to the NRC must describe the process for long-term cumulative or aggregate risk management applied in the plant-specific RMTS program. As stated in Section 3.5, an example of an acceptable general administrative cumulative risk management process could be encompassed within the plant's 10CFR50.65(a)(3) evaluation practices. In this evaluation scheme, the plant would be required to document maintenance configurations where a RICT has been applied. Another example of an acceptable general administrative cumulative risk management process could be tracking and documenting cumulative risk via a 52-week rolling average that is updated weekly. Alternatively, the plant could meet this requirement by documenting the zero-maintenance baseline risk for the plant along with the changes or "deltas" from that baseline, or just quantify the "deltas" from the baseline on an annual basis. The administrative process for aggregate or cumulative risk management must be described in the plant's RMTS program request submittal to the NRC. This administrative process for aggregate risk management should include a requirement to

document specific planned and implemented corrective actions for returning to operation within Regions II or III of Figures 3 or 4 of NRC Regulatory Guide 1.174, if the plant aggregate risk tracking shows an actual or imminently potential excursion into Region I of either of these figures due to RMTS-related RICT implementation. The RMTS program implementation request submittal to the NRC should clearly describe how aggregate risk tracking and associated "triggers" for self-assessment and corrective action will be implemented within the plant-specific RMTS program. This aggregate risk management documentation process may be accomplished via the plant's existing corrective action system, but RMTS-associated corrective actions must be clearly identified in this documentation.

4
PRA AND CONFIGURATION RISK MANAGEMENT TOOL ATTRIBUTES

The RMTS program requires the determination of a RICT. The RICT requires a quantitative risk estimate. The basis for these risk estimates is the quantitative configuration risk management (CRM) Tool, which is a derivative of the plant PRA. For some operating modes and some initiating events (initiators) detailed below, bounding CRM methods can be used in addition to or instead of the CRM Tool. This section describes the attributes of the PRA, the CRM Tool, and Bounding CRM Methods that are necessary to support the RMTS program.

4.1 PRA Attributes

In general, the quantitative risk assessment (plant PRA for RMTS) should be based on the plant Configuration Risk Management Program supported by the plant PRA calculations. At a minimum, the PRA applied in support of a RMTS program must include a Level 1 PRA with LERF capability. The scope of this PRA must include credible internal events and should consider, as appropriate, all or some of the following external events: fire, flood, seismic hazard, and severe weather. It is preferred that these impacts be modeled such that they are explicitly included in the calculation of a RMTS RICT. However, where prior evaluation can demonstrate that one or more of the challenges is not significant to the site or the application, quantitative modeling may be omitted. In any case, the scope of the PRA to be used for RMTS should address Modes 1 and 2 of reactor plant operation. Where the PRA is to be used to extend CTs that originate in lower modes, the PRA scope may be extended to include those applicable modes, or a technically-based argument for application of the Mode 1 and 2 model to other operating modes must be provided (e.g., it must provide assurance that risk associated with other modes addressed in the RMTS is bounded by the Modes 1 and 2 PRA event sequences). The PRA must have an update process clearly defined by plant procedures or instructions.

The PRA model attributes and technical adequacy requirements for RMTS applications must be consistent and compatible with established ASME and ANS standards requirements, as modified by NRC Regulatory Guide 1.200. PRA peer review findings should be resolved or otherwise dispositioned. It is expected that, in general, the PRA which supports RMTS will meet Capability Category 2 requirements of Reference 19, and that any exceptions to meeting those requirements will be justified. For limited scope applications, the PRA capability should be appropriate to the TS system(s) of concern.

4.2 CRM Tool Attributes

The following specific CRM tool attributes are recommended as being necessary for RMTS implementation:

- Initiating events accurately model external conditions and effects of out-of-service equipment
- Model truncation levels are adequate to maintain associated decision-making integrity
- Model translation from PRA to CRM tool is appropriate; and CRM fault trees are traceable to the PRA
- Dependent human actions are modeled and quantified
- Configuration of the plant is correctly mapped from real time activities to CRM parameters
- Each CRM application tool is verified to adequately reflect the as-built, as-operated plant including risk contributors which vary by time of year or time in fuel cycle
- Common cause treatment in the CRM model conforms to RMTS guidance
- New key uncertainties introduced in the CRM model are identified and evaluated prior to use
- CRM application tools and software are accepted and maintained by an appropriate quality program

While these CRM attributes may be implemented in various ways at RMTS-implementing power plants, these attributes should be verifiable via the approved RMTS programs at these plants. Guidance and recommendations for each of these attributes is provided as follows:

1. Initiating events accurately model external conditions and effects of out-of-service equipment - CRM tools should explicitly model external conditions, such as weather impacts, or a process to adequately address the impact of these external conditions exists. The impacts of out-of-service equipment should be properly reflected in CRM initiating event models as well as system response models. For example, if a certain component being declared inoperable and placed in a maintenance status is modeled in the PRA, the entry of that equipment status into the CRM must accommodate risk quantification to include both initiating event and system response impact.
2. Model truncation levels are adequate to maintain associated decision-making integrity – Model truncation levels applied in the CRM should be such that they have no significant impact on associated RMTS decisions. In general, this means that the truncation levels are such that, for a specific RICT calculation, the RICT calculated via the truncated model would not vary significantly from that calculated via an associated un-truncated model and that important model elements have not been removed from the PRA through truncation. Reference 39 provides a reasonably rigorous set of criteria for managing PRA model truncation for adequate decision-making support.
3. Model translation from PRA to CRM tool is appropriate; and CRM fault trees are traceable to the PRA - No time-averaging features of the model that could lead to configuration-specific errors, such as equipment train asymmetries and treatment of possible alternate configurations, should be included in the CRM Tool. Time-averaging features of the basic event data that could lead to configuration-specific errors should be excluded in the CRM

Tool database. Conversely, changes to the model and data should correctly reflect configuration-specific risk. In cases where the CRM tool is simply a configuration risk database cataloguing parameters calculated via the approved PRA, then spot checks of these parameters for conformance with the approved PRA should be performed in accordance with approved station procedures. In cases where the CRM tool actually performs PRA logic model reduction and/or risk calculations directly, quality assurance checks of the model and quantification results translation from the underlying approved PRA should be performed at regular intervals and should show model translation. These technical adequacy checks should show satisfactory traceability from the CRM to the approved PRA.

4. Dependent human actions are modeled and quantified - RICT calculations should appropriately account for, and quantify, the impacts of human action dependence relative to plant configurations and conditions analyzed. This is particularly important in cases where credit for RMAs implemented within the RMTS program is taken in the RICT calculation. Human action dependence analysis should be documented in plant procedures applied for RMTS implementation.
5. Configuration of the plant is correctly mapped from real time activities to CRM parameters - 1) any pre-analysis translation tables from plant activities to CRM Tool basic events or model conditions should be accurate and controlled, 2) effective written process should be in place to apply the translation tables and/or generate the CRM Tool inputs corresponding to plant activities, and 3) training of personnel who apply or review the tool should be performed.
6. Each CRM application tool is verified to adequately reflect the as-built, as-operated plant including risk contributors which vary by time of year or time in fuel cycle - CRM tools should reflect as-built, as-operated plant conditions. The application process should assure that design changes, alternative alignments, and indirect effects of work activities should be considered by plant staff before the RICT is determined. The CRM tools should be updated in accordance with approved PRA update procedures.
7. Common cause treatment in the CRM model conforms to RMTS guidance - The CRM Tool and its implementation process should be adequate to follow the guidance for treatment of common cause failure provided in Section 3.5.2.4 of this document.
8. New key uncertainties introduced in the CRM model are identified and evaluated prior to use - Uncertainty should be addressed in RMTS CRM tools in accordance with Section 3.5.2.2 of this document and consider recommendations in Reference 37.
9. CRM application tools and software are accepted and maintained by an appropriate quality program . CRM application tools and associated software applied for RMTS implementation should meet the same level of quality assurance as the underlying approved PRA software and application tools.

It is recommended that RMTS implementation procedures require that confirmatory checks of RICT assessments and associated calculations by appropriately-qualified plant staff members be part of the RMTS process. Additionally, plant personnel applying CRM tools to perform and approve RICT assessments must be adequately trained and qualified in accordance with plant TS implementation procedures.

5
REFERENCES

1. "Risk-Informed Configuration-Based Technical Specifications (RICBTS) Implementation Guide," EPRI, Palo Alto, CA: 2002. 1007321.

2. U.S. Government, Title 10 of the Code of Federal Regulations, Part 50, Section 10 CFR 50.65, "The Maintenance Rule."

3. Nuclear Energy Institute, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," NUMARC 93-01, Revision 3, July 2000.

4. "PSA Applications Guide," EPRI report TR-105396, August 1995.

5. USNRC, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, Revision 1, November 2002.

6. USNRC, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," *Federal Register,* Vol. 60, p. 42622 (60 FR 42622), August 16, 1995.

7. USNRC, "Risk-Informed Regulation Implementation Plan," SECY-00-0213, October 16, 2000, updated December 5, 2001 (SECY-01-0218).

8. USNRC, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," Draft Revision 1 of Chapter 19 of the Standard Review Plan, NUREG-0800, June 2001.

9. USNRC, "Addressing PRA Quality in Risk-Informed Activities," SECY-00-0162, July 28, 2000.

10. USNRC, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," *Federal Registe*r, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986.

11. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing," Regulatory Guide 1.175, August 1998.

12. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance," Regulatory Guide 1.176, August 1998.

13. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications," Regulatory Guide 1.177, August 1998.

14. USNRC, "An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Inspection of Piping," Regulatory Guide 1.178, September 1998.

15. W.T. Pratt et al., "An Approach for Estimating the Frequencies of Various Containment Failure Modes and Bypass Events," NUREG/CR-6595, January 1999.

16. Nuclear Energy Institute, "Probabilistic Risk Assessment (PRA) Peer Review Process Guidance," NEI 00-02.

17. Nuclear Energy Institute, "Guidelines for Industry Actions to Assess Shutdown Management," NUMARC 91-06.

18. Nuclear Energy Institute, "Guidelines for 10 CFR 50.59 Evaluations," NEI 96-07.

19. American Society of Mechanical Engineers, "Probabilistic Risk Assessment for Nuclear Power Plant Applications," ANSI/ASME RA-S-2002, April 5, 2002 (including Addenda ASME RA-Sa-2003, December 5, 2003).

20. American Nuclear Society, "External Events PRA Methodology Standard," ANSI/ANS-58.21-2003.

21. USNRC, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Regulatory Guide 1.200 (For Trial Use), February 2004.

22. Combustion Engineering Owners Group, "Implementing Guidance for Application to Risk Managed Technical Specifications," WCAP-15971, Current Draft, November 2002.

23. CEN-327-A, "RPS/ESFAS Extended Test Interval Evaluation," May 1986.

24. WCAP-10271-P-A, "Evaluation of Surveillance Frequencies and Out of Service Times for the Reactor Protection Instrumentation System," May 1986.

25. CE-NPSD-994, "Safety Injection Tanks AOT," CEOG Task 836, May 1995.

26. CE-NPSD-995, "Low Pressure Safety Injection System AOT," CEOG Task 836, April 1995.

27. CE NPSD-996, "Emergency Diesel Generator AOT," CEOG Task 836, April 1995.

28. USNRC, "Assessing & Managing Risk before Maintenance Activities at Nuclear Power Plants," Regulatory Guide 1.182, May 2000.

29. U.S. Government, Title 10 of the Code of Federal Regulations, Part 50, Section 10 CFR 50.36, "Technical Specifications."

30. CE-NPSD-1208, "Justification of Risk Informed Modifications to Selected Technical Specifications for Conditions Leading to Exigent Plant Shutdown", December 2000 Westinghouse, Inc.

31. CEOG Certification, "Standard for Probabilistic Risk Assessment for Nuclear Power Plants," Revision 14A, ASME, May 11, 2001.

32. U. S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance," Standard Review Plan Chapter 19, NUREG-0800.

33. U. S. Nuclear Regulatory Commission, "Risk-Informed Decisionmaking: Technical Specifications," Standard Review Plan Chapter 16.1, NUREG-0800.

34. American Nuclear Society, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications: Low-Power and Shutdown PRA," a Proposed National Standard, Current Draft for Review.

35. "Risk-Managed Technical Specifications (RMTS) Guidelines: Interim Development Report," EPRI, Palo Alto, CA: 2003. 1002965.

36. Nuclear Energy Institute, "10 CFR 50.69 SSC Categorization Guideline," NEI 00-04, Final Draft R2, October 2004.

37. "Guideline for the Treatment of Uncertainty in Risk-Informed applications: Technical Basis Document," EPRI 1009652, Palo Alto, CA, December 2004.

38. "Methodology for Fire Configuration Risk Management," EPRI report [Draft XXXXXXX], April 2005.

39. Cepin, Marko, "Method for Setting up the Truncation Limit of Probabilistic Safety Assessment," International Conference on Probabilistic Safety Assessment and Management (PSAM 7 – ESREL '04) paper 0602, June 2004.

A
GLOSSARY OF TERMS

Key terms used in this guide are defined in this appendix. These definitions are intended to be consistent with existing plant technical specifications and associated regulatory and industry guidance. In any case where a plant's technical specifications definitions differ from those provided herein, the plant technical specifications definitions take precedence.

action – that part of a plant technical specification that prescribes remedial measures required under designated conditions.

aggregate risk – the cumulative risk integrated over time accounting for variations in instantaneous risk; generally measured in terms of cumulative CDP and/or LERP (see definitions below).

allowed outage time (AOT) – the duration that an SSC specified in the plant technical specifications can be out of service (non-operational) during plant at-power operation before formal action is required via technical specification limiting conditions for operation.

average risk – the average annual risk calculated via the plant PRA, accounting for the "average" or "typical" maintenance profile of the plant throughout the year. This is different from (generally greater than) the baseline "no-maintenance" risk of the plant.

back-stop completion time – the ultimate maintenance completion time or allowed outage time limit for a specified maintenance configuration. While 10CFR50.59 indicates that this limit may be reasonably established at 90 days, this guide has conservatively recommended a back-stop completion time of 30 days. The back-stop completion time limit for licensee action takes precedence over any risk-informed completion time calculated to be greater than 30 days.

baseline risk – the "no-maintenance" or "zero-maintenance" risk calculated via the plant PRA. This is different from (less than) the average annual risk calculated via the PRA.

completion time (CT) – [Same as allowed outage time (AOT)]

configuration core damage probability (CCDP) – the value equal to the configuration instantaneous core damage frequency multiplied by the actual (or expected) duration of the configuration.

configuration large early release probability (CLERP) – the value equal to the configuration instantaneous large early release frequency multiplied by the actual (or expected) duration of the configuration.

configuration risk management program (CRMP) – the plant program designed to apply the approved PRA to support prudent risk management over the plant life cycle. This program is designed to support the planning and execution of plant maintenance, testing, and inspection activities, as well as other risk-impacting evolutions.

core damage frequency (CDF) – the likelihood of core damage events per unit of time.

core damage probability (CDP) – the integral of CDF over time; the classical cumulative probability of core damage (i.e., instantaneous core or fuel damage frequency integrated over a specified duration), over a given period of time. CDP is unit-less. Weekly risk is calculated for the 168-hour time period over each calendar week. Configuration risk is calculated for the anticipated and/or actual duration of a plant maintenance configuration. Annual risk is a 52-week rolling average, calculated week by week.

cumulative risk – same as "aggregate risk" defined above.

emergent event or emergent condition – any event or condition, which is NOT in the planned work schedule, which renders station equipment non-functional or extends non-functional equipment scheduled outage time beyond its planned duration.

error factor (EF) – [Same as the more common uncertainty term "*RANGE FACTOR*" defined below.]

external events – seismic, flooding, high wind hazard, and other initiating events defined as external events in Reference 20 or similar industry PRA guidance documents and fire hazards events.

front-stop completion time – the maintenance completion time or allowed outage time for plant equipment specified in the conventional (pre-RMTS) plant technical specifications.

functional – SSC is capable of performing its intended function for both normal and emergency operations required to mitigate plant risk as modeled in the plant-specific PRA.

high-risk configuration – a maintenance configuration yielding a plant instantaneous CDF > 1.00E-03 or LERF > 1.00E-4.

incremental configuration core damage probability (ICCDP) – the value equal to the mathematical difference determined by the configuration instantaneous CDF minus the instantaneous zero-maintenance CDF multiplied by the actual (or expected) duration of the configuration.

incremental configuration large early release probability (ICLERP) – the value equal to the mathematical difference determined by the configuration instantaneous LERF minus the instantaneous zero-maintenance LERF multiplied by the actual (or expected) duration of the configuration.

incremental core damage frequency (ICDF) – the frequency above a "no-maintenance" baseline CDF (generally expressed in terms of events per calendar year) that one can expect a reactor fuel core-damaging event to occur for a nuclear power plant of interest.

incremental core damage probability (ICDP) – the integral of ICDF over time; the classical cumulative probability of incremental core damage over a given period of time. ICDP is unit-less. Weekly risk is calculated for the 168-hour time period over each calendar week. Configuration risk is calculated for the anticipated and/or actual duration of a plant maintenance configuration. Annual risk is a 52-week rolling average, calculated week by week.

incremental large early release frequency (ILERF) – the frequency above a "no-maintenance" baseline LERF (generally expressed in terms of events per calendar year) that one can expect a large early release of radioactivity [4] from a reactor core-damaging event to occur for a nuclear power plant of interest.

incremental large early release probability (ILERP) – the classical cumulative probability of incremental large early release of radioactivity over a given period of time. ILERP is unit-less. Weekly risk is calculated for the 168-hour time period over each calendar week. Configuration risk is calculated for the anticipated and/or actual duration of a plant maintenance configuration. Annual risk is a 52-week rolling average, calculated week by week.

initiating event – any event either internal or external to the plant that perturbs the steady state operation of the plant, if operating, thereby initiating an abnormal event such as transient or LOCA within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could potentially lead to core damage or large early release. The scope of initiating events addressed in this guide includes the full scope of those defined in References 19 and 20.

instantaneous core damage frequency (*$\mathbf{CDF_{inst}}$*) – the instantaneous expected core damage frequency resulting from continued operation in a specific plant mode and a given plant configuration (generally presented with units of events/year). In the context of a RMTS, this parameter would likely be calculated continuously and reported hourly or upon a change in value. This term is very similar to the "core damage frequency" term defined above, but the focus here is on a single point in time, and not on longer term averages typically applied when reporting CDF.

instantaneous large early release frequency (*$\mathbf{LERF_{inst}}$*) – the instantaneous expected large early release frequency resulting from continued operation in a specific plant mode and a given plant configuration (generally presented with units of events/year). In the context of a RMTS, this parameter would likely be calculated continuously and reported hourly or upon a change in value.

key safety function – any safety function of equipment included within the scope of technical specifications limiting conditions for operation.

large early release frequency (LERF) – expected number of large early releases per unit of time.

large early release probability (LERP) – the classical cumulative probability of large early release of radioactivity (i.e., instantaneous large early release frequency integrated over a specified duration), over a given period of time. LERP is unit-less. Weekly risk is calculated for the 168-hour time period over each calendar week. Configuration risk is calculated for the anticipated and/or actual duration of a plant maintenance configuration. Annual risk is a 52-week rolling average, calculated week by week.

limiting condition for operation (LCO) – Limiting conditions for operation are the lowest operable capability or performance levels of equipment required for safe operation of the facility. When a limiting condition for operation of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the technical specifications until the condition can be met.

A technical specification limiting condition for operation of a nuclear reactor must be established for each item meeting one or more of the following criteria:

(A) *Criterion 1*. Installed instrumentation that is used to detect, and indicate in the control room, a significant abnormal degradation of the reactor coolant pressure boundary.

(B) *Criterion 2*. A process variable, design feature, or operating restriction that is an initial condition of a design basis accident or transient analysis that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.

(C) *Criterion 3*. A structure, system, or component that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.

(D) *Criterion 4*. A structure, system, or component which operating experience or probabilistic risk assessment has shown to be significant to public health and safety.

maintenance configuration – the consolidated state of all plant SSCs with their associated individual states of functionality (i.e., either functional or non-functional) and alignment (including surveillance inspections and testing alignments) identified. Consistent with the maintenance rule and associated NEI guidance [3], the concept of "maintenance configuration" also encompasses the existence of other activities or conditions that can materially affect plant risk.

In the context of this guide, there are two major types of maintenance configurations, planned and emergent maintenance. A planned maintenance configuration is one that is intentionally and deliberately pre-scheduled (i.e., in a weekly maintenance plan). An emergent maintenance configuration results from an unintentional, emergent situation (i.e., discovery of failure or significant degradation of an SSC within the scope of the RMTS program or a forced, unscheduled extension of previously-planned maintenance).

operable and operability – a system, subsystem, train, component or device shall be operable or have operability when it is capable of performing its specified function(s), and when all necessary attendant instrumentation, controls, electrical power, cooling and seal water, lubrication and other auxiliary equipment that are required for the system, subsystem, train,

component, or device to perform its function(s) are also capable of performing their related support function(s).

operational mode or mode – an operational mode (i.e., mode) shall correspond to any one inclusive combination of core reactivity condition, power level, and average reactor coolant temperature specified in plant technical specifications.

PRA-calculated mean value: the mean value of a probability distribution for a key risk measure, such as CDP or LERP, calculated via the PRA.

probabilistic risk assessment (PRA) – a qualitative and quantitative assessment of the risk associated with plant operation and maintenance that is measured in terms of frequency of occurrence of risk metrics, such as core damage or a radioactive material release and its effects on the health of the public (also referred to as a probabilistic safety assessment, PSA).

range factor (RF) – in performing uncertainty analysis, this is a measure of the range or width of the probability distribution for an underlying risk parameter, such as CDF or CDP. Conventionally, the range factor, sometimes called the "error factor" of a probability distribution is defined and calculated as the square root of the quotient result from the 95^{th} percentile value divided by the 5^{th} percentile value of the distribution of interest. For lognormal distributions, this is the same as the quotient result from the 95^{th} percentile divided by the 50^{th} percentile, which is also the same as the quotient result from the 50^{th} percentile divided by the 5^{th} percentile value of the distribution of interest.

risk-informed completion time (RICT) – a plant-specific SSC maintenance configuration CT or AOT calculated based on maintaining plant operation within allowed risk thresholds or limits (presented in Section 3 of this report) and applying a formally approved configuration risk management program and associated probabilistic risk assessment.

risk-management technical specifications (RMTS) – a plant-specific set of configuration-based technical specifications, based on a formally approved configuration risk management program and associated probabilistic risk assessment, designed to supplement previous conventional plant technical specifications.

safe shutdown condition – the plant shutdown condition in any defined (known) plant shutdown mode where the reactor $K_{effective} < 0.99$.

zero-maintenance CDF – the calculated CDF for the zero-maintenance configuration.

zero-maintenance configuration – the plant configuration where no planned or emergent maintenance is being performed (including any risk-impacting testing or inspection actions) and PRA components remain functional.

zero-maintenance LERF – the calculated LERF for the zero-maintenance configuration.

B
BACKGROUND

B.1 The Maintenance Rule – Technical Specification Nexus

Plant Technical Specifications were intended to provide time limits on inoperability of design basis components during various plant modes. These times were designated as Allowed Outage Times (AOTs) or Completion Times (CTs) within TS action statements. As refueling outages became shorter, these times were used to help establish the "at power" maintenance durations for design basis and safety related components. While a few selected high-risk maintenance combinations were prohibited by the TS (namely maintenance on redundant trains of the same system), no limitations were provided on non-TS components and most plant configurations were not directly restricted. In some instances, on-line maintenance was primarily based on compliance with the TS CTs, and at times implementing TS required actions resulted in operation in less than desirable plant configurations.

In an effort to improve plant maintenance practices in the nuclear industry, the NRC issued the Maintenance Rule (10CFR50.65) as its first risk informed performance based regulation. The regulation required the licensee to assess and manage risk, including the important contribution of Balance of Plant (BOP) non-safety systems. At the initial issuance of the rule, performance of a risk informed assessment was not required. In November 2000, the Maintenance Rule was amended with the addition of paragraph (a)(4). Paragraph (a)(4) of 10CFR50.65 explicitly required that plants assess and manage risk in the conduct of maintenance operations. This rule requires that a "risk assessment" be performed prior to voluntary entry into a maintenance configuration, or as soon as practical, upon entry into a non-voluntary maintenance condition. The guidance for satisfying the requirements of this rule provision is defined in Section 11 of NUMARC 93-01 [3] and has been endorsed by the NRC in RG 1.182 [28]. These guidance documents were built, in part, on the Configuration Risk Management program developed as part of the CEOG pilot for RG 1.177. A companion risk-informed rule (10CFR50.59) change associated with evaluating "permanent" plant changes, became active in January 2001.

As a result of the difference in intent of the TS and the Maintenance Rule, the control of plant maintenance could be inconsistently treated. For example, the Maintenance Rule provides for a risk assessment prior to voluntary entry into a maintenance configuration, with the emergent (unplanned) work being evaluated as soon as practical. On the other hand, while the TS requires no risk assessment, operation within certain plant configurations is explicitly restricted, require defined actions including plant shutdown, and is subject to rigid time restrictions. Furthermore, unlike the TS, the Maintenance Rule is silent on identification of plant conditions requiring plant shutdown.

The RMTS intends to meld the two processes together by supplementing the fixed interval CTs and prescribed actions in the current TS with a risk-informed alternative. This alternative establishes flexible CTs with a backstop CT controlled by the Maintenance Rule, and shutdown/mode change actions established from a risk assessment process. Thus, TS actions will explicitly consider the contemporaneous plant risks in managing the plant configuration and while conducting restorative actions. The process for assessing plant risks will represent a blending of quantitative information and qualitative considerations.

B.2 Historical Evolution

10CFR50.36 [29] requires that the plant's design basis be maintained and that when the plant is outside that design basis, actions be taken to restore that design basis. Plant shutdown is included among the actions to be considered. The regulation has no explicit requirement or process for establishing allowable times for these actions or the associated restorative actions. As the TS evolved, deterministic insights, simplified risk insights, and judgment were used to establish CTs and actions. However, for the most part, the forced plant shutdown was considered a safe action if design basis compliance could not be restored. Therefore, a forced plant shutdown would be required, even when continued plant operation is the lower risk alternative. Later, the TS became increasingly standardized, culminating in the development of the Improved Standard TS (ISTS). The goal of the ISTS was to simplify the TS structure and clarify the TS language. In addition, the ISTS sought to remove conflicts that existed among TS actions and to rationalize some specific TS by integrating risk insights into the associated actions. While the ISTS resolved many of the initial problems with earlier TS, the actions and allowed outage times (or completion times) remained largely deterministically driven.

In 1993, the Electric Power Research Institute (EPRI) began development of the *PSA Applications Guide* (EPRI report TR-105396) to help utilities that own and operate nuclear power plants use their PRAs to improve plant safety and resource allocation. The *PSA Applications Guide* was completed in August 1995. In December 1995, with support from industry owners groups, EPRI published its *Guidelines for Preparing Risk-Based Technical Specifications Change Request Submittals* (EPRI report TR-105867). Also, in 1995, the NRC published its final policy statement on *Use of Probabilistic Risk Assessment Methods in Nuclear Activities* in the Federal Register. In 1997, the NRC developed draft regulatory guides (reg. guides) and associated draft standard review plan (SRP) sections related to risk-informed applications of nuclear power plant regulation. These draft reg. guides and SRP sections were reviewed, revised, and published as final reg. guides and SRP sections during the 1997-1999 time frame. Specifically, NRC reg. guide 1.177 provides NRC guidance on risk-informed technical specifications programs. Throughout the 1990s, the nuclear power industry has also developed and implemented 10 CFR 50.65, the "Maintenance Rule," and more recently implemented 10 CFR 65(a)(4), the maintenance configuration risk management portion of the Maintenance Rule (see Section 1). Also, over the past four years, the Nuclear Energy Institute (NEI) has formed the Risk-Informed Technical Specification Task Force (RITSTF) to work closely with the Technical Specifications Task Force (TSTF), which is responsible for maintaining and improving on OGS ITS NUREGs, to address specific issues associated with the process of "risk-informing" plant technical specifications. This risk management guide was developed to supplement the *PSA Applications Guide* and current RITSTF efforts, and support

utilities in effective and efficient development of risk-management technical specifications (RMTS) implementation programs.

Following industry feedback from a 1998 stakeholders meeting, the NRC recommended that the industry consider an initiative to risk inform the plant TS. In response to that initiative, several public meetings were held to identify the aspects of the TS that are amenable to a risk informed treatment. Based on these meetings, the NRC and industry have embarked upon an effort to globally risk inform several aspects of the current TS. The product to emerge from this effort is the RMTS. This effort is an outgrowth of the emergence of a "risk conscious" regulatory environment at the NRC and several years of regulatory experience in evaluating and implementing risk informed changes to the current generation of TS. As with the existing generation of TS, the criteria for entry into the associated TS will be defined inoperabilities of a TS System, Structure or Component (SSC). Retention of this structure will ensure that the RMTS is fully compatible with the requirements of 10CFR50.36 [29]. However, it is envisioned that, once fully implemented, the maintenance related actions for non-TS SSCs will also follow the same risk assessment process.

C
RISK PROFILE EXAMPLES

This appendix provides some realistic examples of risk-versus-time profiles for a typical nuclear power generating unit. These examples have been developed via the STPNOC CRMP risk calculation and monitoring tool, the STPEGS Risk Assessment Calculator (RAsCal). Table C-1 shows some realistic plant risk-versus-time data for three typical nuclear power plant maintenance configuration profile examples.

Table C-1
Example STPEGS Risk Profile Data

Example Number	Maintenance Configuration	Start Time (Year 2003)	End Time (Year 2003)	Technical Specification Front-Stop CT (Hours)	Applicable Technical Specification Action	Instantaneous Incremental CDF (Events/Year)	Time to 1E-06 Incremental CDP (Hours)	Time to 1E-05 Incremental CDP (Hours)	Back-Stop CT (Hours)
1	CCA DGA EWA HHA	03/31 00:00	04/01 00:00	168	Restore CCA, EWA, and HHA to OPERABLE status within 7 days; restore DGA to OPERABLE status within 14 days; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	5.15E-05	170.12	1701.18	720
	CCA DGA EWA HHA HHC	04/01 00:00	04/01 01:00	1	Restore HHA or HHC to OPERABLE status within 1 hour; otherwise be in HOT STANDBY within 6 hours, HOT SHUTDOWN within the following 6 hours, and COLD SHUTDOWN within the subsequent 24 hours.	1.52E-04	57.84	578.43	720
	CCA DGA EWA HHA	04/01 01:00	04/02 12:00	168 Minus Elapsed Time (25 here) = 143	Restore CCA, EWA, and HHA to OPERABLE status within 7 days; restore DGA to OPERABLE status within 14 days; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	5.15E-05	170.12	1701.18	720
2	EWC	03/31 00:00	04/05 00:00	168	Restore EWC to OPERABLE status within 7 days; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	3.92E-05	223.51	2235.10	720

Example Number	Maintenance Configuration	Start Time (Year 2003)	End Time (Year 2003)	Technical Specification Front-Stop CT (Hours)	Applicable Technical Specification Action	Instantaneous Incremental CDF (Events/Year)	Time to 1E-06 Incremental CDP (Hours)	Time to 1E-05 Incremental CDP (Hours)	Back-Stop CT (Hours)
	AFD EWC	04/05 00:00	04/06 00:00	72	Restore AFD to OPERABLE status within 72 hours; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	1.35E-04	65.07	650.74	720
	AFD	04/06 00:00	04/06 22:00	72 Minus Elapsed Time (24 here) = 48	Restore AFD to OPERABLE status within 72 hours; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	1.33E-05	660.00	6599.96	720
3	EWC	03/31 00:00	04/04 00:00	168	Restore EWC to OPERABLE status within 7 days; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	3.92E-05	223.51	2235.10	720
	AFD EWC	04/04 00:00	04/05 00:00	72	Restore AFD to OPERABLE status within 72 hours; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	1.35E-04	65.07	650.74	720
	EWC	04/05 00:00	04/05 12:00	168 Minus Elapsed Time (120 here) = 48	Restore EWC to OPERABLE status within 7 days; otherwise be in HOT STANDBY within 6 hours and HOT SHUTDOWN within the following 6 hours.	3.92E-05	223.51	2235.10	720

A brief description of the maintenance configuration designators applied in Table C-1 is provided in Table C-2.

Table C-2
Maintenance Configuration Designator Descriptions for Table C-1

Maintenance Configuration Designator	Description of Inoperable Equipment
AFD	Turbine-driven auxiliary feedwater pump (and unique function-supporting components)
CCA	Component Cooling Water pump/heat exchanger train A (and unique function-supporting components)
DGA	Standby diesel generator train A (and unique function-supporting components)
EWA	Essential Cooling Water ventilation fan train A (and unique function-supporting components)
EWB	Essential Cooling Water ventilation fan train B (and unique function-supporting components)
EWC	Essential Cooling Water ventilation fan train C (and unique function-supporting components)
HHA	High head safety injection pump train A (and unique function-supporting components)
HHB	High head safety injection pump train B (and unique function-supporting components)
HHC	High head safety injection pump train C (and unique function-supporting components)

Listing multiple designators for one configuration simply means that the corresponding system functions/trains are simultaneously unavailable during that configuration.

Example 1 in Table C-1 indicates that the plant had planned maintenance for CCA, DGA, EWA, and HHA initially, and had entered that configuration, but that subsequently, an emergent condition developed wherein, during the planned maintenance configuration, the HHC function also became unavailable. In this example, the HHC function was recovered first; then planned maintenance for CCA, DGA, EWA, and HHA was completed, subsequently. Similarly, in Example 2 in Table C-1, maintenance was planned for EWC, but during that planned maintenance activity, the AFD function became unavailable, as an emergent condition. In this case, though, the plant was able to complete maintenance on the EWC function prior to recovering the AFD function. In effect, this action placed the plant in a safer configuration such that more time was available to address the emergent problem with the AFD function before any administrative or regulatory safety limits were breached. Finally, in Example 3 in Table C-1,

maintenance was planned for EWC, and during that planned maintenance activity, the AFD function became unavailable, as an emergent condition, as in Example 2. However, in this case, the plant staff was able to quickly restore the AFD function, thus placing the plant in a safer condition to continue with the planned EWC maintenance.

Note that in Table C-1, the eighth column simply indicates how long, in hours, it will take to reach an incremental CDP value of 1.00E-05. As this time is based on the constant instantaneous incremental CDF value presented in column five of Table C-1, one can calculate the time to reach other values of incremental CDP (e.g., 1.00E-06) based on simple factor relationships. For example, if we wish to know how long it would take to reach an incremental CDP value of 1.00E-06 for the first configuration of Example 1, we simply calculate one tenth of the time shown to reach 1.00E-05 (in this case, approximately 170 hours).

The Westinghouse Owners Group has calculated maintenance risk profiles for example scenarios 1 and 2 in Table C-1 for some typical generic pressurized water reactor designs. The results of these calculations for the most limiting maintenance configuration of these two scenarios are presented in Tables C-3 and C-4 for example scenarios 1 and 2, respectively. Tables C-1, C-3, and C-4 show that, for typical, but challenging, maintenance configurations, reasonable time periods are available to plant staffs for prudent risk management action based on the RMTS quantitative risk acceptance guidelines presented in Table 3-2 of this report.

Table C-3
Example Scenario 1 Risk Profile Data for Generic Pressurized Water Reactor Types

Generic Plant Type	Maintenance Configuration (see Table C-2)	Instantaneous Incremental CDF (Events/Year)	Time to 1E-06 Incremental CDP (Hours)	Time to 1E-05 Incremental CDP (Hours)	Back-Stop CT (Hours)	Plant Design Remarks
CE Early Design	CCA DGA EWA HHA HHB	5.99E-05	146.34	1463.44	720	Plants have diesel-driven startup feedwater pumps.
CE Later Design	CCA DGA EWA HHA HHB	1.99E-04	44.05	440.50	720	Plants have no PORV.
Westinghouse 2-Loop	CCA DGA EWA HHA HHB	2.21E-04	39.67	396.65	720	Plants have available non-safety equipment to support the auxiliary feedwater function.
Westinghouse 3-Loop	CCA DGA EWA HHA HHB	6.82E-04	12.85	128.53	720	None.

Table C-4
Example Scenario 2 Risk Profile Data for Generic Pressurized Water Reactor Types

Generic Plant Type	Maintenance Configuration (see Table C-2)	Instantaneous Incremental CDF (Events/Year)	Time to 1E-06 Incremental CDP (Hours)	Time to 1E-05 Incremental CDP (Hours)	Back-Stop CT (Hours)	Plant Design Remarks
CE Early Design	AFD EWA	4.98E-05	176.02	1760.24	720	Plants have diesel-driven startup feedwater pumps.
CE Later Design	AFD EWA	1.05E-04	83.49	834.86	720	Plants have no PORV.
Westinghouse 2-Loop	AFD EWA	1.33E-04	65.91	659.10	720	Plants have available non-safety equipment to support the auxiliary feedwater function.
Westinghouse 3-Loop	AFD EWA	1.01E-04	86.79	867.92	720	None.