Risk-Managed Technical Specifications (RMTS) Guidelines

Interim Development Report

Technical Report

Risk-Managed Technical Specification (RMTS) Guidelines

Interim Development Report

1002965

November 2003

EPRI Project Manager
F. Rahn

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.

Westinghouse Electric Company, LLC

ORDERING INFORMATION

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

CITATIONS

This report was prepared by

Risk Consulting Division
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

Principal Investigators
J. Liming
R. 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 Specification (RMTS) Guidelines: Interim Development Report, EPRI, Palo Alto, CA: 2003. 1002965.

REPORT SUMMARY

This report presents nuclear utilities with a technical framework and associated general guidance for implementation of risk-managed technical specifications (RMTS) as a partial replacement for existing conventional plant technical specifications. This interim report, intended for both Westinghouse and non-Westinghouse reactor plants and for future reference and application by the Nuclear Energy Institute (NEI), will probably be updated in the future as risk-informed applications technology continues to progress in the nuclear power industry.

Background

Since 1995, the methodology for applying probabilistic risk assessments (PRAs) to risk-informed regulation has been advanced by the publication of many reports. EPRI has 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), and *Risk-Informed Configuration-Based Technical Specifications (RICBTS) Implementation Guide* (1007321). NRC published its final policy statement on *Use of Probabilistic Risk Assessment Methods in Nuclear Activities* in the Federal Register, 60, pp 42622-42629, August 16, 1995, and has issued several regulatory guides and Standard Review Plan sections for risk-informed applications of nuclear power plant regulation, specifically, RG 1.177 providing guidance on risk-informed technical specifications programs. Finally, over the past four years, the NEI has formed the Risk-Informed Technical Specification Task Force (RITSTF) and the Technical Specifications Working Group to address specific issues associated with the process of "risk-informing" plant technical specifications. This report supplements the *PSA Applications Guide* and current RITSTF efforts and supports EPRI member utilities in effective and efficient development of RMTS implementation programs.

Objectives

- To provide utilities with an approach for developing and implementing nuclear power plant risk-managed technical specifications programs
- To complement and supplement existing PRA applications methodologies.

Approach

Using available industry and NRC documentation, experienced PRA practitioners developed an approach and methodology for implementing risk-informed technical specifications.

Results

This report presents a recommended approach and technical framework for an effective RMTS program and its implementation following NRC approval. The approach uses an appropriate blend of deterministic and probabilistic methods. The report includes a comprehensive list of references.

EPRI Perspective

This project shows that most nuclear power utilities can apply their current PRAs to develop risk-managed technical specifications for their plants. This interim report presents a general framework, not a specified method, for RMTS program development. The RMTS framework it describes is designed to be consistent with and build upon NEI maintenance rule guidance. NEI Initiative 4B pilot plant applications will help determine a more specific methodology for RMTS program implementation in the future. The methodology presented in the report may be phased in so that only "high-value" systems are chosen initially, thus front-loading the potential benefits of RMTS implementation. It is important to note that a RMTS program should not permit intentional, simultaneous disabling of all trains of any key safety function. EPRI acknowledges and thanks the STP Nuclear Operating Company (STPNOC) for its invaluable technical support of this project.

Keywords

Probabilistic risk assessment
Risk-informed applications
Probabilistic safety assessment
Technical specifications
Operations
NRC regulations
Licensing

ABSTRACT

In 1995, EPRI published the *PSA Applications Guide* (TR-105396) to help utilities that own and operate nuclear power plants use their probabilistic risk assessments (PRAs) to improve plant safety and resource allocation and *Guidelines for Preparing Risk-Based Technical Specifications Change Request Submittals* (TR-105867). In 2000, EPRI published the *Risk-Informed Integrated Safety Management Specification (RIISMS) Implementation Programs* report (1000893), describing the fundamental concepts of a RIISMS program, followed in 2001 by the *Risk-Informed Integrated Safety Management Specifications (RIISMS) Implementation Guide* (1003116), describing the details of RIISMS program implementation. In 2002, EPRI published its *Risk-Informed Configuration-Based Technical Specifications (RICBTS) Implementation Guide* (1007321). The purpose of this report is to supplement these preceding reports to provide specific guidance on how to implement risk management technical specification (RMTS) programs at existing and planned nuclear power plants. This report is organized and presented as follows:

- Section 1 is an overview of the history of 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.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

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 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. Early activities in integrating risk insights were used in resolving specific industry issues. These activities were sponsored to varying degrees by all Owners' Groups (References 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 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) (References 25, 26 and 27) became the pilot documents supporting the development of the Regulatory Guide governing risk informed changes to the Plant TS (Reference 13). As experience with risk informed regulation grew, additional Risk-Informed AOT extensions have been granted.

The impetus for a risk-managed Technical Specifications (RMTS) program was the NRC's "Maintenance Rule" (10 CFR 50.65) (Reference 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 Management Technical

Specifications (RMTS) initiatives. This report focuses on enabling conditions for the broad based initiative to replace the existing fixed AOTs/CTs with a flexible CT structure controlled within the plant's 10CFR50.65(a)(4) (Reference 2) Maintenance Rule. In a flexible CT structure, most equipment TS conditions allow the component outage time to be determined based on the actual plant state, maintenance needs, and relative risks. Specifically, the general features of the Nuclear Energy Institute (NEI) Technical Specification Task Force (TSTF) Initiative 4B are discussed, and specific risk informed processes that may be needed for successful implementation of this type of TS are identified. Initiative 4B is the industry effort to transition from existing fixed AOTs to flexible CTs. These processes will supplement an existing 10CFR50.65(a)(4) program and could be subsumed within that program. Inclusion of these supplementary processes within a plant's maintenance program will enable better integration, and support of the plant TS.

It is expected that implementation of RMTS will allow utilities to 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 (Reference 4) and NRC's Regulatory Guide 1.174 (Reference 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 NEI RITSTF Initiative 4B. Initiative 4B 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 NEI 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. These 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 structure of the maintenance rule. 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 RMTS features/processes to be integrated into a risk informed application of the (a)(4) risk management process include:

1. Identification of, and timely response to, emergent (unscheduled) risk-significant conditions.

2. Assessment of potential common cause failure risk associated with emergent failures.

3. Implementation of a formal Risk Informed Decision Process for plant shutdown/mode change.

4. Process for consideration of external events (Reference 20) and risk significant fire events.

The first feature is added to ensure that a delay in the risk assessment (up to the time of the front-stop) will not result in the emergence of a high-risk plant configuration. The second and third enhancements are defined to support the assessment that the "configuration is acceptable for continued operation" beyond the front-stop. The addition of a formal external events (Reference 20) risk assessment process is intended to ensure proper disposition of the risk informed decision.

It should be noted that many existing maintenance rule programs include one or more of the above features already. However, it is expected that some accommodations and enhancements may be required to existing maintenance rule applications for RMTS implementation. The addition of these processes to the existing 10CFR50.65(a)(4) (where they do not already exist) risk assessment process will facilitate the transition to flexible CTs.

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 informed maintenance actions, and may include the action to shutdown the plant. In practice, this program is transparent for all 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 management actions. Enhancements are associated with <u>emergent (unscheduled)</u> 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 affect a shutdown, as appropriate.

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-management 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, and its attendant Regulatory Guide (RG) 1.182. Risk informed front-stop times will be established based on single SSC outage guidelines of RG 1.177 or using the traditional non risk-informed standard Tech. Specs.. In addition, the overall use of the RMTS process will be periodically assessed to demonstrate compliance with RG 1.174 guidance for small risk impact plant modifications (i.e., yearly change < 10^{-5} per year).

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. The RICT will 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 RG 1.177. The back-stop CT limit of 30 days is judged to be a prudently conservative administrative limit for configuration risk management, as compared with the 10CFR50.59 design change criteria limit of 90 days. It is anticipated that application of RICTs for individual maintenance configurations 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 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 (RITS) will be similar to familiar traditional TS with the exception that actions will be provided to allow continued plant operation beyond the TS “front-stop”. 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 should be performed in accordance with the plant’s Maintenance Rule program and supported by a plant’s PRA and other risk management tools (e.g., plant safety monitor or risk monitor software, risk matrices, 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) and 10CFR50.59 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 (definition in Appendix A), and applies to both preventive and corrective maintenance.

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/their applicable safety function(s)) of the inoperability will be considered within the scope of the risk assessment. For example, HPSI inoperability may vary in risk significance, dependent on the degree of residual capability (capability to support required safety functions) of the system.

A target and maximum RICT would be calculated before the front-stop CT limit is reached. The target RICT would be used to track the success of the maintenance activity consistent with normal work controls. Consistent with NEI maintenance rule guidance (Reference 3), a target RMTS configuration risk would be a configuration incremental Core Damage Probability (ICDP) of 10^{-6} (as measured from the time the associated plant equipment goes out of service). For emergent conditions (or for forced, unscheduled extension of planned maintenance) a maximum RICT equivalent to an ICDP of 10^{-5} is identified. Under no circumstances is the RICT to exceed the ultimate back-stop CT limit of 30 days (as measured from the time of entry into the associated TS LCO front-stop CT). The use of administrative maintenance target risk values at levels significantly below the RICT will ensure adequate margin to unanticipated concurrent failures.

In an RMTS program, a RICT would only be calculated when the plant enters 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 front-stop CT. If, during application of a specified RICT, the plant transitioned to a different maintenance configuration (e.g., due to emergent conditions), then that RICT would be required to be recalculated and revised within a specified time period (24 hours, for example) after the change in configuration. It is important to note that this 24-hour re-assessment period is simply an example applied in this report. Case-specific re-assessment periods applied within a plant-specific RMTS program will need to be consistent with the application of associated front-stop CT requirements. 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. If a revised RICT were found to exceed a RMTS threshold, the plant would re-evaluate the impact and enter a plant shutdown decision process. If the revised RICT exceeds the upper-level RMTS threshold based on specified ICDP/ILERP limits (see Section 3, specifically Table 3-2), the plant would be required to take the actions required for "ACTION NOT MET" for the affected Technical Specifications. Note that, during the time period following the front-stop CT but before the expiration of the applicable RICT, plant actions will escalate to be commensurate with the projected risk during the maintenance configuration period, consistent with the current maintenance rule guidance (Reference 3).

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 more directly to the equipment's availability to support its intended risk mitigation function. Equipment functionality will generally be considered in a RMTS program when assessing risk for RICT calculation.

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 to 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 and other SSCs that have been determined to be of high safety significance via processes outlined in Reference 3.

The (a)(4) process uses PRA methods and risk insights in establishing and planning maintenance activities. The RMTS program recommended herein meets (a)(4) requirements by using existing (a)(4) guidance in many areas and by implementing a more rigorous 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 and considers the impact of external events (such as fire, seismic, flooding, high wind, and other initiating events defined as external events in Reference 20). Additional details of this process are contained in NUMARC-93-01 (Reference 3).

The RMTS process shall:

1. Be documented in plant procedures delineating appropriate responsibilities for (a)(4) related actions.

2. Include procedures for performing a risk assessment when the maintenance items are outside the scope of the quantitative risk assessment tool.

3. 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 risk matrix, a list of pre-calculated risk levels for specified maintenance configurations, etc.), or the tool is otherwise unavailable, qualitative methods may be used to assess risk and define appropriate actions to manage the risk increase.

4. Include guidance for using risk insights to manage overall plant risk.

In performing the RMTS assessment, the decision-making process will, where appropriate, include consideration of transition risks associated with mode changes. 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)

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 informed assessment. The structure of the proposed RMTS is illustrated in Table 3-1. 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 (Reference 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/qualitative risk assessment will provide the basis for continued plant operation. The assessment must consider the impact of common cause failures, external events (Reference 20) and flooding. In addition, the assessment may credit compensatory actions established during the period being evaluated.

2. Depending on the outcome of this assessment and assessment of alternative actions, 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 plant shutdown will reflect plant cumulative risks, the likelihood of repair and transition and shutdown risk considerations.

For emergent (unscheduled) conditions, the plant staff is expected to provide an expeditious assessment of the plant risk. Typically, such an assessment should be performed within 24 hours of an emergent condition. Quantitative risk assessments will be performed with an appropriately contemporaneous (as-built, as-operated) plant risk model, and PRA results should be based on PRAs with Level 1 and 2 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 extension.

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

1. Perform risk assessment and management in accordance with the Maintenance Rule (a)(4),

2. 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 RMTS guidance to determine the feasibility of continued power operation beyond the front-stop,

3. Based on the results of the risk assessment, the plant staff will take actions to manage risk by potentially expediting repairs, or by implementing contingency actions, including initiating a plant shutdown, and

4. Once the extended CT is entered, the RMTS risk assessment will be re-performed in accordance with the RMTS program when emergent conditions change the evaluated maintenance configuration. In the event of an emergent condition, the assessment should be performed within 24 hours following any plant maintenance configuration changes. The risk management program will be based on a risk informed application of 10CFR50.65(a)(4).

The risk 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. In addition, risk assessments will be performed to assess the incremental risk of the inoperable equipment associated with maintenance configuration addressed by the extended CT (RICT). These latter results will be tracked, trended, and periodically reviewed to ensure that the cumulative risk of the flexible TS is small (per RG 1.174). 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/equipment 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 in an approved plant procedure, and each assessment supporting implementation will be documented. 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 conducting, reviewing, and approving the assessment. In all cases where a RICT assessment cannot be performed (e.g., when the configuration risk cannot be adequately addressed via the CRMP and PRA), the normal front-stop CT(s) will be applied.

For plants implementing an RMTS program, it is generally a good practice to develop and maintain a "pre-analyzed" list of maintenance configurations with associated RICT values. 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. One [HPSI] subsystem inoperable.	B.1 Restore SI 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 (i.e., within 24 hours of a subsequent configuration change)
	AND	
	B.2.3 Restore subsystems SI to OPERABLE status.	30 days or acceptable completion time , whichever is less.

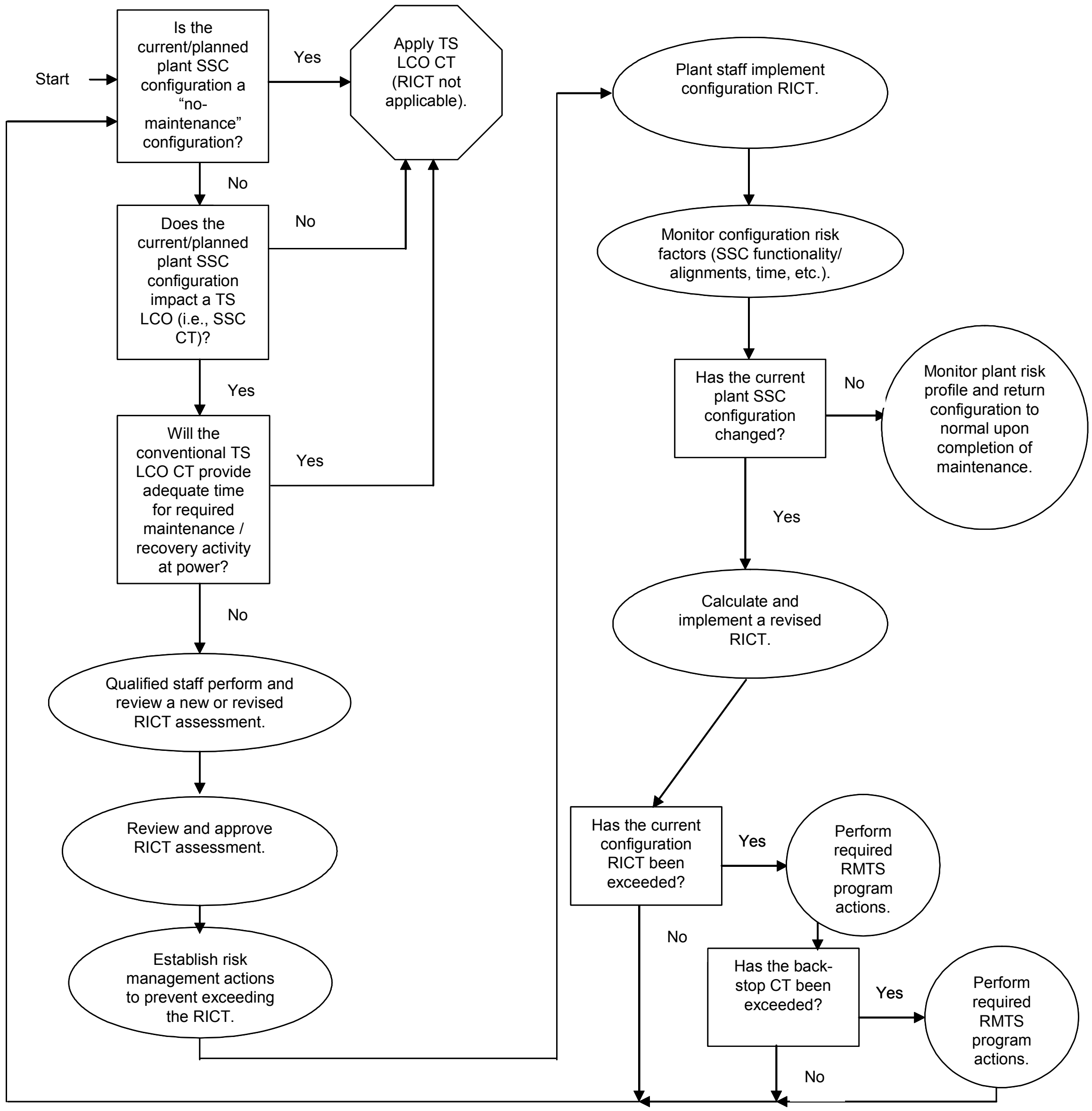

Figure 3-1
Example Process Flowchart for RMTS RICT Assessment and Implementation

3.2 General Guidance for the Assessment

1. Power Operating Conditions are defined as plant modes other than 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 may use quantitative approaches supported by qualitative approaches.

3. The quantitative assessment should be based on the plant Maintenance Rule 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 lower bound RICT calculated via an upper bound configuration risk yields ample time for maintenance implementation).

4. The assessment must consider:
   - Technical Specifications requirements
   - 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 (References 19 and 20) (as determined by each licensee, consistent with its obligation to manage maintenance-related risk)
   - Component and system dependencies that are affected
   - Significant performance issues for the in-service redundant SSCs
   - Significant industry experience related to the maintenance configuration of interest (Note that updating input information from industry experience should be consistent with Maintenance Rule (a)(4) assessment and PRA updates for the plant.)
   - Compensatory actions taken to mitigate the risks, e.g. alignment of cross-ties with other units, installation of temporary systems.

5. In determining the risk impact of the plant configuration, the assessment may also consider the following factors:
   - the risk impact of the configuration during shutdown versus performing the maintenance at power.
   - the impact of plant mode transition risk (the cumulative risk incurred during one or more associated plant mode changes) if the equipment outage would require one or more associated mode changes that would otherwise be unnecessary.
6. Assessments may be predetermined or performed on an as-needed basis.
7. 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.
8. 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.
9. 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).
10. Emergent conditions(or forced, unscheduled extension of planned maintenance) may require action prior to completing the assessment, or could change the conditions of a previously performed assessment. Examples include plant configuration or mode changes, additional SSCs out of service due to failures, or significant changes in external conditions e.g. weather, offsite power availability, etc.. The following guidance, consistent with Reference 3 guidance, 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. Procedural guidance must be provided in the plant’s RMTS program request submittal to specify the appropriate completion time for reassessing the risk. Based on the results of the assessment, ongoing or planned maintenance activities may need to be suspended, modified or rescheduled, and SSCs may need to be returned to service.
    - 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 (e.g., within 24 hours), the assessment need not be performed for purposes of supporting that maintenance activity. However, an evaluation should be considered in the plant's administrative program for controlling 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 effectively defines its scope of equipment maintenance configurations (see definition of "maintenance configuration" in Appendix A) to be those associated with SSCs that are included within the scope of current technical specifications LCOs, and therefore, have front-stop CT requirements, but excludes fundamental technical specifications 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 (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 (Reference 3).

The PRA used for the RMTS scope and risk assessment should have the following characteristics:

- The PRA should meet adequacy criteria such as industry standards for risk-management technical specification applications (see References 19, 20, and 21). Specifically, the PRA should meet ASME PRA standard (Reference 19) requirements for effective risk evaluation of all SSCs within the scope of the RMTS program. The NRC has recognized Reference 19 standards in DG-1122 (Reference 21).
- Some SSCs within the plant PRA scope may be determined to have low safety significance regardless of plant configuration. These SSCs need not be included in the scope of the risk assessments. Pre-existing analyses and/or expert panels may be used to facilitate these determinations.

- A process for assessing important large early release frequency (LERF) considerations (containment performance, release category frequencies, etc.) should be applied in addition to an acceptable Level 1 PRA.

3.4 Assessment Methods for Power Operating Conditions

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, requires 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 insights 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 plant configuration. Section 5 provides information on PRA attributes. 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

1. The quantitative assessment should be supplemented by a qualitative evaluation. 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.

2. 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 exposures.

3. 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 (References 19 and 20)
   - Involve a significant potential to cause a scram or safety system actuation
   - Result in significant complications to recovery efforts.

4. Depending on the level of anticipated configuration risk, risk impacts of equipment outages may be determined via approximate or bounding analyses.

5. Qualitative considerations may also be necessary to address external events (Reference 20), and SSCs not in the scope of the Level 1, internal events PRA (e.g., included in the assessment scope because of expert panel considerations).

6. 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).

7. External event (Reference 20) considerations involve the potential impacts of weather or other external conditions relative to the proposed maintenance evolution. In the assessment, weather, external flooding, and other external impacts need to be considered if such conditions are imminent or have a high probability of occurring during the planned out-of-service duration. An example where these considerations are appropriate would be the long-term removal of exterior doors, hazard barriers, or floor plugs.

8. Flooding considerations (from internal or external sources) should be addressed if pertinent. The assessment should consider the potential for maintenance activities to cause internal flood hazards, and for maintenance activities that expose SSCs to flood hazards that degrade their capability to perform key safety functions.

3.5 Managing Risk

Risk management uses the risk assessment in plant decision-making to control the risk impact. This process requires careful planning, scheduling, coordinating, monitoring, and adjusting of maintenance activities.

The objective of risk management is to control the temporary and aggregate risk increases from maintenance activities. This control is accomplished by using target and maximum limit RICT values (calculated based on the risk thresholds presented in Table 3-2) to plan and schedule maintenance such that the risk increases are limited, and to take additional actions beyond routine work controls to address situations where the temporary risk increase is above specified RMTS thresholds (see Table 3-2). These thresholds may be set on the basis of qualitative considerations (e.g., remaining mitigation capability), quantitative considerations (e.g., temporary increase in core damage frequency), or blended approaches using both qualitative and quantitative insights.

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.) Aggregate risk is controlled to a degree through maintenance rule guidance (Reference 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 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 (References 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.

The most fundamental risk management action is planning maintenance activities with the insights provided by the assessment. In conjunction with scheduling the sequence of activities, compensatory risk management actions may be taken that reduce the temporary risk increase. Since many of the risk management actions involve non-quantifiable factors, the risk reduction would not necessarily be quantified. The following sections discuss the establishment of thresholds for the use of risk management actions.

3.5.1 Establishing Action Thresholds Based on Qualitative Considerations

In accordance with Reference 3, risk management action thresholds (i.e., plant conditions and associated configuration risk levels determining when risk management actions are required) may be established qualitatively by considering the performance of key safety functions, or the remaining mitigation capability, given the out-of-service SSCs. Qualitative methods to establish 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 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 may be established quantitatively by considering the magnitude of the instantaneous core damage frequency (CDF_{inst}), incremental core damage frequency (ICDF), and the incremental large early release frequency (ILERF) for the maintenance configuration of interest. 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 probability 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 (Reference 3). When combined with the other elements of maintenance rule guidance, and other quantitative or qualitative measures, this guidance is acceptable for RICT implementation:

1. Maintenance configurations with a configuration-specific CDF_{inst} in excess of 10^{-3} per year should be carefully considered before voluntarily entering such conditions. If such conditions 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.

2. 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 (Reference 3). These risk acceptance guidelines should be considered with respect to establishing risk management actions.

Table 3-2
RMTS Quantitative Risk Acceptance Guidelines

Criterion		Risk Management Guidance
$CDF_{inst} > 10^{-3}$/yr		- Careful consideration before entering the configuration
ICDP	ILERP	
$>10^{-5}$	$>10^{-6}$	– Configuration should not normally be entered voluntarily
10^{-6} - 10^{-5}	10^{-7} - 10^{-6}	– Assess non-quantifiable factors – Establish risk management actions
$< 10^{-6}$	$<10^{-7}$	– Normal work controls

In a RMTS program the 10^{-6} and 10^{-7} thresholds for ICDP and ILERP, respectively, are referred to as "target" or "lower-level" RMTS thresholds, while the 10^{-5} and 10^{-6} thresholds for ICDP and ILERP, respectively, are referred to as "maximum limit" or "upper-level" RMTS thresholds.

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. Individual plants may choose to propose application of a similar risk management scheme based on absolute risk metrics versus incremental risk metrics.

Using this framework for risk management, the plant staff can calculate target and maximum risk-informed allowed outage times. 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) based on risk assessment, alternative actions and the impact of compensatory actions.

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 is to 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. One example of an acceptable plant administrative policy designed to effectively implement cumulative risk management is described in Reference 1. 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. The requirement to achieve acceptable long-term performance indicators provides 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 calculating configuration RICT values for plant-specific applications. However, the RICT quantitative acceptance guidelines established herein have the following fundamental basis. When RMTS-implementing plants apply PRAs of acceptable quality standards (see Section 5), application of PRA-calculated mean values (see definition in Appendix A) for configuration risk compared with the risk acceptance guidelines provided herein will meet acceptable uncertainty criteria for safe and prudent RICT implementation.

It is recommended that prior to implementation of the RMTS ("flexible CT"), a demonstration of the RI evaluation and control processes be performed. This demonstration may include limited post assessment of previous cycles' 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 should be evaluated. Results of these studies may be used to inform the utility and NRC staff of the plant's program for implementing the flexible CT.

3.5.2.2 External Events Consideration

Plants without external events (Reference 20) PRAs must apply the following logic to support maintenance activities beyond the front-stop:

1. They must be able to provide a reasonable technical argument that the configuration risk of interest is dominated by internal events, and that external events (Reference 20) are an insignificant contributor to configuration risk, or

2. They must be able to perform a reasonable bounding analysis of the external events (Reference 20) contribution to configuration risk 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 mitigation or contingency actions that, for the duration of the configuration of interest, enable them to provide a reasonable technical argument that external events (Reference 20) are an insignificant contributor to configuration risk.

It is the intent of the RMTS process to consider the total plant risk. Plants with full scope PRAs may be able to largely perform quantitative risk assessments. However, it is expected that many of the plants intending to utilize the flexible CT will have robust level 1 PRAs and qualitative risk insights associated with fire, seismic and external flooding assessments. Checklists may be used to identify components where external event (Reference 20) overlaps are not significant and to limit maintenance in areas when the component risks are dominated by external event contributions.

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. Some example actions are shown below:.

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 operating 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
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.

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 (is it 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. 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 under 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 to reduce the risk impact during a planned maintenance activity. The 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; however, the impact of the measures on plant safety functions should be considered as part of the risk evaluation. 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.

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.

4
PRA ATTRIBUTES

The PRA used for the (a)(4) and RMTS risk assessments is important for two aspects:

1. Determination of scope of SSCs to which the assessment applies.

2. Evaluation of risk impact of the maintenance configuration (or as the basis for the risk monitor, matrix, or other tool), if the assessment is performed quantitatively.

In general, the quantitative risk assessment should be based on the plant Maintenance Rule risk assessment program (Reference 3) supported by the plant PRA. An internal-events-only Level 1 PRA may be applied if the containment breech and external events (Reference 20) risk associated with the configuration of interest can be shown to be reasonably bounded or insignificant via a blend of qualitative arguments and quantitative calculations.

The PRA model attributes and quality assurance requirements for RMTS applications are designed to be consistent and compatible with NRC regulatory guidance for PRA technical adequacy (see Reference 21), and supported by the ASME and ANS PRA Standards (References 19 and 20, respectively). Guidance provided in References 5, 16, and 34 also applies.

All portions of the PRA that support RICT assessments for SSCs within the scope of the RMTS program should be consistent with ASME PRA standard (Reference 19) requirements, as discussed in NRC draft regulatory guide DG-1122.

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, July 1998.

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.

20. American Nuclear Society, “External Events PRA Methodology,” BSR/ANS-58.21-200x, a Proposed National Standard, Current Draft for Review.

21. USNRC, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Draft Regulatory Guide (DG-1122), November 2002.

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.

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 (generally less than) the average annual risk calculated via the PRA.
- *COMPLETION TIME (CT)*: [Same as allowed outage time (AOT)]
- *CORE DAMAGE FREQUENCY (CDF)*: expected number 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. <u>Weekly risk</u> is calculated for the 168-hour time period over each calendar week. <u>Configuration risk</u> is calculated for the anticipated and/or actual duration of a plant maintenance configuration. <u>Annual risk</u> is a 52-week rolling average, calculated week by week.

- *CUMULATIVE RISK*: same as "aggregate risk" defined above.
- *EMERGENT EVENT*: any 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.
- *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.
- *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. <u>Weekly risk</u> is calculated for the 168-hour time period over each calendar week. <u>Configuration risk</u> is calculated for the anticipated and/or actual duration of a plant maintenance configuration. <u>Annual risk</u> 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 (as defined in Reference 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. <u>Weekly risk</u> is calculated for the 168-hour time period over each calendar week. <u>Configuration risk</u> is calculated for the anticipated and/or actual duration of a plant maintenance configuration. <u>Annual risk</u> 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 include the full scope of those defined in References 19 and 20.
- *INSTANTANEOUS CORE DAMAGE FREQUENCY (*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*: 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 functional 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. When a limiting condition for operation of any process step in the system of a fuel reprocessing plant is not met, the licensee shall shut down that part of the operation 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 (Reference 3), the concept of

"maintenance configuration" also encompasses the existence of other activities or conditions (such as severe weather) that can materially affect plant risk. In the context of a RMTS program, some plants may wish to interpret a RMTS maintenance configuration definition to be generally limited to plant SSCs that have or could have associated technical specification LCOs (i.e., AOT or CT limits), and "functionality" is defined as "available to perform its associated safety function." A maintenance configuration definition can be expressed as a "truth table" for all appropriate SSCs that states the current state of functionality (yes or no) of each SSC. The universe of possible maintenance states includes the "no-maintenance" state where all SSCs are functional. See the following simple example of a maintenance configuration definition table:

PLANT SSC (TAG NUMBER)	FUNCTIONAL (AVAILABLE TO PERFORM ITS ASSOCIATED FUNCTION)
SSC00001	YES
SSC00002	NO
SSC00003	YES
. . .	. . .
SSCXXXXX	YES

In the context of this guide, there are two major types of maintenance configurations, planned and unscheduled maintenance. A planned maintenance configuration is one that is intentionally and deliberately pre-scheduled (i.e., in a weekly maintenance plan). An unscheduled 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 uncertainty analysis. This uncertainty analysis involves propagation of input data uncertainty through the PRA risk quantification process.

- *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).
- *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 $K_{effective} < 0.99$.

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. In practice, these limits were used to identify what level of maintenance would be done on those components. 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 (Reference 3) and has been endorsed by the NRC in RG 1.182 (Reference 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 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 (Reference 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) and the Technical Specifications Working Group 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 (Reference 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 transition 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 Increment al 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
	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

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 Increment al CDP (Hours)	Back-Stop CT (Hours)
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)
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)
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 HHC	5.99E-05	146.34	1463.44	720	Plants have diesel-driven startup feedwater pumps.
CE Later Design	CCA DGA EWA HHA HHC	1.99E-04	44.05	440.50	720	Plants have no PORV.
Westinghouse 2-Loop	CCA DGA EWA HHA HHC	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 HHC	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 EWC	4.98E-05	176.02	1760.24	720	Plants have diesel-driven startup feedwater pumps.
CE Later Design	AFD EWC	1.05E-04	83.49	834.86	720	Plants have no PORV.
Westinghouse 2-Loop	AFD EWC	1.33E-04	65.91	659.10	720	Plants have available non-safety equipment to support the auxiliary feedwater function.
Westinghouse 3-Loop	AFD EWC	1.01E-04	86.79	867.92	720	None.

Program:
Nuclear Power

About EPRI

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

EPRI. Electrify the World

Printed on recycled paper in the United States of America

1002965

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