BNL-NUREG-63139

CONF-960912--4

# HANDBOOK OF METHODS FOR RISK-BASED ANALYSIS OF TECHNICAL SPECIFICATIONS[a]

Pranab K. Samanta,
and Inn S. Kim[b]
Brookhaven National
Laboratory
Building 130
P.O. Box 5000
Upton, New York
11973-5000
(516)344-4948

Tuomas Mankamo
Avaplan Oy
Itainen Rantatie 17
FIN-02230 Espoo
FINLAND
358-0-400-3364

William E. Vesely
Science Applications
International
Corporation
655 Metro Place South
Dublin, Ohio 43017
(614)793-7600

## ABSTRACT

Technical Specifications (TS) requirements for nuclear power plants define the Limiting Conditions for Operations (LCOs) and Surveillance Requirements (SRs) to assure safety during operation. In general, these requirements are based on deterministic analyses and engineering judgements. Improvements in these requirements are facilitated by the availability of plant-specific Probabilistic Risk Assessments (PRAs).

The use of risk and reliability-based methods to improve TS requirements has wide interest because these methods can:

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

The United States Nuclear Regulatory Commission (USNRC) Office of Research sponsored research to develop systematic, risk-based methods to improve various aspects of TS requirements. A handbook of methods summarizing such risk-based approaches has been completed in 1994. It is expected that this handbook will provide valuable input to NRC's present work in developing guidance for using PRA in risk-informed regulation.

The handbook addresses reliability and risk-based methods for evaluating allowed outage times (AOTs), action statements requiring shutdown where shutdown risk may be substantial, surveillance test intervals (STIs), managing plant configurations, and scheduling maintenances. For each topic, the handbook summarizes the methods of analysis and data needs, outlines the insights to be gained, lists additional references, and presents examples of evaluations.

## I. INTRODUCTION

Technical Specifications (TS) requirements for nuclear power plants (NPPs) define the limiting conditions for operation (LCOs) and Surveillance Requirements (SRs) to assure safety during operation. In general, these requirements are based on deterministic analyses and engineering judgments. As probabilistic risk assessments (PRAs) of NPPs are increasingly used in plant safety management and in defining safety regulations, increased attention is being paid to improve/modify TS using Risk-based or PRA-based analyses. In fact, improvement of TS is considered by many to be among the first applications of risk-informed regulation.

To move towards risk-informed TS from existing TS requirements, acceptable PRA-based methods to address various aspects of TS should be available. Recognizing the need, the United States Nuclear Regulatory Commission (USNRC), Office of Research, sponsored research to develop systematic risk-based methods for evaluating TS requirements and a handbook has been completed.[1] In this paper, we discuss the handbook, its use and scope, and present an overview of the methods and applications included in the handbook. The handbook does not imply regulatory requirements; it summarizes information learned from research and case evaluations.

---

[a]Work performed under the auspices of the U.S. Nuclear Regulatory Commission. The views expressed are those of the authors and do not necessarily reflect any position or policy of the U.S. NRC.
[b]Currently with Korea Atomic Energy Research Institute, Taejon, Korea.

This paper is organized as follows: Section 2 presents an overview of the role of the handbook in analyzing TS changes, Section 3 describes the objectives, uses, and structure of the handbook, and Section 4 summarizes each application area presented in the handbook. Additional areas for risk-based TS applications are discussed in Section 5. The paper concludes with summary remarks.

## II. ANALYSES AND CONSIDERATIONS IN CHANGING TSs AND THE ROLE OF THE HANDBOOK

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

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

A broad spectrum of assessments and experiences are used in evaluating changes to TS that involve deterministic analyses, lessons learned from previous changes, engineering judgments, and risk implications of the change. The probabilistic risk assessment of a NPP provides a tool for quantitatively assessing the risk contributions of TS requirements, and the risk impact of a change. The handbook focusses on applying PRAs to assess the risk contributions associated with the requirements and the proposed changes.

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

The handbook also focusses on analyses of TS requirements during power operation, although there also are TS requirements when the plant is shut down. In principle, the methods discussed can be applied to shutdown periods using the corresponding PRA model for the shutdown stages. However, the specific conditions and parameters for shutdown analyses vary because different activities and requirements then should be taken into consideration.

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

## III. OBJECTIVE, USES, AND STRUCTURE OF THE HANDBOOK

The basic objective of the handbook is to summarize risk-based methods for analyzing various aspects of the TS. The primary focus is to enable USNRC reviewers to assess whether proper evaluations have been made in using risk-based analysis to change the TS requirements. Therefore, for each aspect of the TS, the handbook summarizes:

- the issues to be addressed,
- the methods and steps to be followed in a PRA-based application, and
- gives illustrative examples and insights for seeking changes to the TS requirements.

The handbook is expected to have several uses:

a) It can be used for USNRC reviews of risk-informed analysis to TS requirements submitted by the licensee,

b) The licensees can use the handbook in preparing their submittals to the USNRC,

c) Individual Plant Evaluations (IPEs) can be applied to analyze TS requirements, and

d) The handbook will help to ensure consistency in the analysis and in the review process.

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

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

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

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

## IV. RISK-BASED ANALYSES OF TS REQUIREMENTS

In this section, a brief overview is given of each of the application areas presented in the handbook; they correspond to Chapters 3 to 8.

### A. Allowed Outage Time (AOT)[2,3]

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

The intent of an AOT is to provide adequate time to repair a failed component without incurring undue risk because of loss of function of the component. A long AOT implies a relatively larger risk to be incurred, but a shorter AOT may result in inadequate repair and/or unnecessary plant shutdown, both of which have risk implications.

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

The chapter on AOT specifically discusses:

a) risk contributions associated with an AOT,

b) evaluations of two different types of risk contributions associated with an AOT, namely, single-event AOT risk and yearly AOT risk,

c) interactions of the risk contributions from several AOTs,

d) basic formula for, and the use of, PRAs to evaluate the AOT risk contribution,

e) specific steps in conducting AOT evaluations,

f) data needs for AOT evaluations,

g) example evaluations of AOT risk contributions for selected requirements in a NPP, and

h) risk strategies involving AOT risks.

B. Preventive Maintenance (PM)[4]

Components in the safety systems of NPPs require preventive maintenance (PM) to assure their reliability. Increasingly, PMs are being scheduled during power operation. The PMs are performed using the LCO requirements defined in the plant's TS (i.e., the AOTs discussed earlier). These requirements originally were intended for repairing failures, but are used to voluntarily declare an equipment inoperable to perform a PM. Thus, the duration of the PM is limited by the AOT, and also, LCO requirements are followed, limiting simultaneous outages of redundant trains in a system.

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

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

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

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

The risk implications of such practices during power operation can be summarized as follows:

a) The impact on core-damage frequency (CDF) of simultaneous outages of multiple components can be significant,

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

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

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

The chapter on PM addresses:

a) methods for analyzing the risk impact of PM on a single component (differences from AOT risk measures),

b) methods for evaluating the risk impact of maintenance schedules,

c) risk-based comparisons (based on impacts on core-damage frequency) of scheduling maintenance during power operation vs. shutdown,

d) examples of each of the above three types of applications, and

e) insights on scheduling PM.

C. Surveillance Test Interval (STI)[3,5]

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

The primary purpose of surveillance testing is to assure that the components of standby safety systems will be operable when they are needed in an accident. By testing these components, failures can be detected that may have occurred since the last test, or the time when the equipment was last known to be operational. However, the number of surveillance tests required by Technical Specifications is enormous, requiring the nuclear industry and the regulatory agency to spend substantial resources on planning, conducting, and verifying them.

By extending the STI, the resources spent on testing can be reduced. However, an important disadvantage here is that the fault-exposure time, i.e., the time during which the component will be subject to failures during standby (strictly speaking, standby time-related failures), will correspondingly increase as the STI increases.

The evaluation of STIs considers the STI risk contribution that arises from the failures that may occur between tests and are detected by the test; or, in other words, the risk contribution that may be limited by defining an STI. The undesirable or adverse effects of testing and their risk contributions are discussed next. The method presented is applicable to a large portion of surveillance testing whose adverse effects are negligible. The handbook discusses how the STI for these tests can be systematically evaluated, based on the STI risk contribution

that arises from the failures occurring between tests and neglecting the adverse effects of testing.

The chapter on STI includes:

a) risk contributions associated with an STI,

b) basic formula for test-limited risk for a tested component,

c) use of PRA to determine test-limited risk contributions,

d) special considerations for evaluating multiple test-limited risk contributions,

e) considerations in separating the component failure rate into time-related and demand-related contributions,

f) considerations in accounting for test scheduling in computing the test-limited risk,

g) steps involved in systematic STI evaluations,

h) data needs for an STI evaluation,

i) example STI evaluations using test-limited risks, and

j) risk-strategies involving STIs.

D. Adverse Effects of Surveillance Testing[5]

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

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

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

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

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

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

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

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

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

To evaluate the surveillance test interval including adverse effects of testing, the handbook discusses:

a) risk contributions caused by the tests,

b) risk effectiveness of testing considering test-caused and test-limited contributions,

c) basic formula, steps, and an example evaluation of the risk impact of test-caused transients,

d) basic formula, assumptions, and an example evaluation of the risk impact of test-caused wear,

e) data needs for evaluating test-caused risks, and

f) interpretation of results for defining STIs.

E. Action Statements Requiring Shutdown

Previously, methods were discussed for analyzing AOTs focussing on controlling the risk during power operation. This partly addresses action requirements because the actions are applicable at the end of the AOT. These action requirements primarily are directed towards minimizing the risk during power operation, assuming that shutting down the plant is relatively safe; namely, the risk of shutdown is assumed to be negligible. This is not necessarily a reasonable assumption for a system that removes decay heat. When such a system is inoperable or degraded at power, shutting down the plant may not necessarily reduce risk, compared to continuing power operation and giving priority to completing the repairs. A comparative analysis of risk impacts of action alternatives

can be used to address these failure situations. The chapter devoted to this type of application discusses:

a) basic concepts of the comparative analysis of LCO operating and shutdown risks,

b) basic method and formulas for evaluating LCO risks,

c) risk quantification for the basic operational alternatives,

d) sensitivity analysis to identify operational policy alternatives,

e) data needs for quantifying risk of shutting down,

f) example applications comparing risk of shutdown vs. continued operation, and

g) insights in defining action requirements for systems where risk of shutting down is substantial.

F. Managing Plant Configuration[7]

During the operation of a NPP, multiple components across systems may be simultaneously unavailable, disabling multiple trains of different safety systems. The LCOs in TS contribute to the management of plant configuration in the following ways:

a) assuring that repair of individual component failure is performed in the allotted period, i.e., within the defined AOT for individual failures,

b) requiring that the plant be shutdown for failure of redundant trains within a safety system.

Many other combinations of component outages are not explicitly addressed in the TS which imply that simultaneous outages of these combinations are not forbidden. Typically, these combinations can result from outages of components in different safety systems.

Unless specific measures are taken, simultaneous outages of multiple components are likely because of the many test and maintenance activities carried out at a plant. Realizing that simultaneous outages cannot be completely avoided, the management of plant configuration can help to avoid the occurrence of risk-significant configurations. Specifically, by identifying risk-significant ones, precautions can be taken such that deliberate actions, e.g., test and maintenance, do not contribute to their occurrence. At the same time, configurations with minimal risk implications can be allowed when it is advantageous for carrying out test and maintenance.

The evaluation of risks associated with management of plant configuration is applicable in the following areas:

- Scheduling of Preventive Maintenance: In many cases, preventive maintenance (PM) is routinely performed during power operation where multiple components are simultaneously taken out-of-service. PRAs can be used to assess the risk implication of the PM schedules and decide on an acceptable schedule that avoids large peaks in risk.

- Extensions of AOTs: When extensions to AOTs are considered, there is an increased likelihood that, because of them, multiple components may be simultaneously unavailable. The risk implications of likely combinations of components for which AOTs may be extended can be assessed to assure that the probability remains low of having large CDF peaks from plant configurations as a result of these extensions.

- Control of Risk-Significant Plant Configurations: In general, PRAs can be used to identify specific risk-significant configurations so that activities, e.g., tests and maintenance, are designed or organized to avoid these configurations. This type of evaluation can have three uses. First, specific configurations with risk implications, not forbidden in the TS, can be identified, and LCO action requirements can be defined, e.g., plant shutdown. Second, a hierarchy of important plant configurations can be defined for personnel involved in carrying out test and maintenance activities, and third, relaxed requirements can apply for those configurations forbidden in TS but which have low risk impact.

The handbook covers the following aspects for evaluating the risk of plant configurations:

a) definition and uses of different configurations - risk measures,

b) calculations of configuration risk using PRAs,

c) example analysis of configuration risk at a plant,

d) strategy and framework for a risk-based configuration control system, and

e) insights on managing plant configurations.

## V. ADDITIONAL AREAS FOR RISK-BASED TS APPLICATIONS

The handbook covers major aspects of TS requirements that may need modifications and are amenable to risk-based analyses. As mentioned earlier, risk-based evaluations can be extended to some additional aspects. The following are specific areas for which risk-based methods can be developed:

a) allotted time to accomplish mode changes,

b) end state for an LCO shutdown,

c) minimum requirements for equipment operability during plant transitions from power operation to shutdown and during shutdown, and

d) requirements relating to external event initiators, e.g., fire, seismic activity.

Additionally, risk-based approaches can be further developed to decide one-time extension/exemption requests, as opposed to permanent changes, and to define requirements for plant upgrades using technological advances, e.g., introduction of digital instrumentation and control systems. A more direct application of risk-based approaches will be to use on-line systems measuring plant risk levels, and to define conditions for operation and surveillances within acceptable bounds based on engineering and deterministic considerations.

## VI. SUMMARY

A handbook was developed to present methods for the risk-informed analysis of Technical Specification requirements in nuclear power plants. The scope of the handbook includes reliability and risk-based methods for evaluating allowed outage times (AOTs), action statements requiring shutdown where shutdown risk may be substantial, surveillance requirements (SRs), including the adverse effects of surveillance testing, managing the outage configuration of equipment, and scheduling maintenances. The handbook is expected to result in consistency both in the application of risk-informed methods to improve TS, and in the review of such analyses.

## VII. REFERENCES


1. P.K. Samanta, I.S. Kim, T, Mankamo, and W.E. Vesely, "Handbook of Methods of Risk-Based Analyses of Technical Specifications," NUREG-CR-6141, BNL-NUREG-52398, December 1994.

2. W.E. Vesely, "Evaluation of Allowed Outage Time (AOTs) From a Risk and Reliability Standpoint," NUREG/CR-5425, BNL-NUREG-52213, August 1989.

3. P.K. Samanta, S-M. Wong, and J. Carbonaro, "Evaluation of Risks Associated With AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, August 1988.

4. P.K. Samanta, I. Kim, S. Uryasev, J. Penoyar, and W. Vesely, "Emergency Diesel Generator: Maintenance and Failure Unavailability, and Their Risk Impacts," NUREG/CR-5994, BNL-NUREG-52363, November 1994.

5. I.S. Kim, S. Martorell, W.E. Vesely, and P.K. Samanta, "Quantitative Evaluation of Surveillance Test Intervals Including Test-Caused Risks," NUREG/CR-5775, BNL-NUREG-52296, February 1992.

6. T. Mankamo, I. Kim, and P.K. Samanta, "Technical Specification Action Statements Requiring Shutdown: A Risk Perspective with Application to the RHR/SSW Systems of a BWR," NUREG/CR-5995, BNL-NUREG-52364, November 1993.

7. P.K. Samanta, W.E. Vesely, and I.S. Kim, "Study of Operational Risk-Based Configuration Control," NUREG/CR-5641, BNL-NUREG-52261, August 1991.