

OECD

NEA

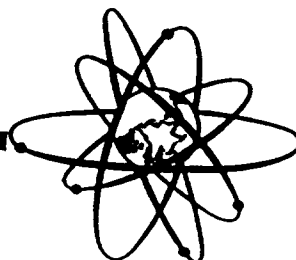
RESTRICTED
NEA/CSNI/R(92)16

***PSA APPLICATION TO TECHNICAL
SPECIFICATIONS***

*Edited by
José I. Calvo
Consejo de Seguridad Nuclear, Spain*

*CSNI Principal Working Group N° 5
on Risk Assessment*

October, 1992



**COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS (CSNI)
OCDE NUCLEAR ENERGY AGENCY
Le Seine Saint-Germain - 12, boulevard des Iles
92130 Issy-les-Moulineaux, France**



C S N I

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers. It was set up in 1973 to develop and coordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries.

CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the coordination of work in different Member countries including the establishment of co-operative research projects and international standard problems, and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on nuclear power plant incidents.

In implementing its programme CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
1.0 INTRODUCTION	1
1.1 Objectives	2
1.2 Organization of the Report	2
2.0 CURRENT APPLICATION OF PSA TECHNIQUES TO TECHNICAL SPECIFICATIONS	3
2.1 PSA Applications to Technical Specifications in the United States	3
2.2 PSA Applications to Technical Specifications in the Nordic Countries	8
2.3 Application of PRA Techniques to Technical Specifications in England	8
3.0 FUTURE APPLICATIONS	12
3.1 Line Item Improvements	12
3.2 Reliability Based Surveillance Test Intervals	13
3.3 Development of a Real Time Risk Monitor	15
3.4 Shutdown Configuration Application	17
4.0 CONCLUSIONS	18
5.0 REFERENCES	19

LIST OF TABLES

<u>Table</u>	<u>Page</u>
Table 1. USNRC Topical Report Reviews on STI/AOT Extensions	4

1.0 INTRODUCTION

To ensure safe operation of nuclear power plants, operating limits and conditions consistent with the plant safety analyses are established for each individual plant. These operating limits and conditions essentially define a safe envelope of operability for each individual plant and are referred to as technical specifications in the United States.

Technical Specifications in the United States and similar requirements in other countries have been an effective tool for controlling plant operational risk. However, in recent years there has been a growing concern about the philosophy, scope, bases, and content of current technical specifications. Most of these concerns are related to how well current technical specifications control individual plant's operational risk. For example, the Allowed Outage Time (AOT) defined as the maximum amount of time a component can be out of service before the plant has to shutdown is based on engineering judgement. Eventhough in the large majority of cases these limits are reasonable, in many plant-specific situations they might not account for the risk-significance of the component. This could result in plant shutdowns where the safety significance of the component and the plant status doesn't warrant such an action. Furthermore, in case of unavailability of components or systems that are necessary during shutdown, staying at power might be a preferred and safer state than a forced shutdown.

On the other hand current technical specifications requirements, in general, only address individual component outages based on engineering judgement. Multiple outage of components that could result in a much more degraded plant state compared to individual component outages are usually not addressed, and are governed by the technical specification for the single component with the most restrictive AOT.

Thus, current technical specifications could potentially allow plant operation with multiple component outages corresponding to a high risk level. Alternatively, technical specifications could require a plant shutdown due to unavailability of a component where the risk significance of the component would not warrant such a action, or prevent a utility from taking additional components out for preventive maintenance thereby reducing plant operational flexibility.

There are similar concerns about the Surveillance Test Intervals (STI) requirements. Surveillance Test Intervals are defined as the maximum amount of time between consecutive tests of standby equipment. These intervals are currently based on engineering judgement and manufacturer's recommendations. However, the optimum test interval for each standby component depends on relative contributions of the demand stress (created by frequent tests) vs. standby stress (created by long inactive intervals). Both of these factors strongly depend on the characteristics of the component and its environment.

All these examples point toward the need for a more comprehensive plant-specific risk-based approach to setting technical specifications. In such an approach the primary measure

of a component or parameters' importance is its risk significance, and the bases for all technical specification requirements is the plants' operational risk.

With the advancement of the Probabilistic Risk Assessment (PRA) techniques, there is a growing effort to use these techniques to supplement the engineering judgement in setting technical specification's requirements.

1.1 Objectives

The objectives of this report are to discuss the current applications of the PRA techniques to improve technical specifications around the world, and provide recommendations for future work in the area of risk-based technical specifications.

1.2 Organization of the Report

In the next section, an overview of the latest activities in application of PRA techniques to improve technical specifications will be provided. This section will focus on countries with active programs on application of risk and reliability techniques to technical specifications. This will be followed in Section 3.0 by our recommended future activities on application of PSA techniques to improve the effectiveness of technical specifications. Section 4.0 provides the overall conclusions of this study. All references cited in this report are included in Section 5.0.

2.0 CURRENT APPLICATION OF PSA TECHNIQUES TO TECHNICAL SPECIFICATIONS

Risk and reliability techniques are increasingly being used to improve and optimize technical specifications. In a recent International Atomic Energy Agency (IAEA) sponsored conference on this subject some 22 papers from 18 countries were presented. Among these, programs in the United States, Nordic Countries, and England are most mature and are summarized below.

2.1 PSA Applications to Technical Specifications in the United States

In the United States both the Nuclear Regulatory Commission (NRC) and the nuclear industry have several active programs to apply risk and reliability techniques for optimization of technical specifications. These programs fall into two major categories of short term programs where PSA techniques are used for immediate technical specifications changes, and long term programs which are oriented more toward research and development of major technical issues that could lead to a totally new approach to setting technical specifications. Majority of the short term program have been focused on line item improvements where PSA techniques are used to optimize AOTs and STIs associated with different components. Most of these applications are performed by the utility owners groups whereby the target of optimization are a set of components or parameters that apply to a whole class of power plants.

Table 1. shows a list of the line item improvements that have been submitted to the NRC and have been reviewed and approved by the NRC. In addition to this, individual utilities have occasionally requested technical specifications changes for individual items based on risk and reliability analyses. These requests are evaluated by the NRC on individual bases.

Another application of PSA techniques to improve Technical Specifications have been directed toward the new Standard Technical Specifications (STS).

Over the past several years a coordinated effort between the NRC and the utility industry has been underway to improve the content, format and style of the current technical specifications. The first step in this process was development of a set of criteria that would define what requirements should be included in the technical specifications. Application of these criteria to the current technical specifications resulted in removal of approximately 40% of the requirements to other licensee-controlled documents. In addition, the content and style of the remaining technical specifications were changed. These changes include some new AOTs and STIs using engineering judgement. However, PSA techniques were used on selective basis to assess the reasonableness of these new AOT and STI requirements (1). This application resulted in confirmation of some of the proposed AOTs and STIs and changes to others. The results of these probabilistic analyses were used as an input for setting the final requirements.

Table 1. USNRC Topical Report Reviews on STI/AOT Extensions*

-
1. **B & W Topical Report BAW-10167 For RPS - (Complete)**
 2. **CE Topical Report CEN-327 For RPS And ESFAS - (Under Review)**
 3. **GE Topical Report NEDC-30851 For BWR RPS - (Complete)**
 4. **GE Topical Report NEDC-30851, Supp 1 For BWR Rod Block Instruments - (Complete)**
 5. **GE Topical Report NEDC-30851, Supp 2 For BWR Isolation Instruments Common to RPS and ECCS - (Complete)**
 6. **GE Topical Report NEDC-30956, Part 1 For WR ECCS Actuation Instruments - (Complete)**
 7. **GE Topical Report NEDC - 30936, Part 2 For BWR ECCS Actuation Instruments - (Complete)**
 8. **W Topical Report WCAP-10271, Supp 1 For RPS - (Complete)**
 9. **W Topical Report WCAP-10271, Supp 2 For ESFAS (This Mtg.)**

*** Most STI Extensions Are From 1 To 3 Months, With A Variety Of AOT Extensions**

In addition to the above activities, there are several ongoing long term programs to assess the feasibility of a risk-based approach to technical specifications. The first program is sponsored by the NRC office of Nuclear Reactor Regulation (NRR). The initial phase of this study concentrated on identification of alternative risk-based approaches that could improve current technical specifications, and assessment of the characteristics and advantages/disadvantages of each approach (2).

Four alternative risk-based approaches for improving the technical specifications were identified. These are: 1) a risk-based approach, 2) a reliability goal-oriented approach, 3) a data-oriented approach, and 4) a configuration-control-oriented approach.

Based on detailed analysis of each approach, it was concluded that a risk-based approach to technical specifications is the most promising approach for bringing greater risk perspective to technical specifications. This conclusion is based on the fact that this approach utilizes the most comprehensive plant risk model currently available, and as such it accurately accounts for the level of redundancy, diversity, and importance of various components and systems.

The primary characteristics of a risk-based approach to technical specifications is that the decisions on plant operations are based on the effect of plant configuration changes on plant's instantaneous risk. The impact of configuration changes on plant instantaneous risk can be made in real time, if a fast response software for analysis of the plant risk model is developed, or in semi-real time using plant risk model and currently available PC-based software. In either case, the plant risk model can be used for planning of routine daily activities such as surveillance tests or preventive maintenance activities, or in response to unplanned component outages for setting Allowed Outage Times (AOTs). Using either approach, the AOTs for different components are based on the importance of the component to plant risk and the plant configuration at the time a component is declared inoperable. Thus, contrary to current technical specifications, the AOTs for different components are not fixed, rather they are calculated in real time based upon the current configuration of the plant, i.e., based upon what other components or systems that are available at the time a particular component is declared inoperable.

Following this conclusion a second study was initiated to study major technical and institutional issue associated with this approach and assess the feasibility of implementing a pilot program to look into detailed characteristics of such an approach to technical specifications. To do this a working group consisting of the NRC, SAIC, Brookhaven National Laboratory (BNL), and three utilities namely Pacific Gas and Electric (PG&E), Southern California Edison (SCE), and the Philadelphia Electric Company (PECo) was formed to consider all technical and practical issues associated with implementation of a pilot study (3).

In addition, to gain insights into operational experience with the current technical specifications, each utility was requested to collect data on the changes to plant

configuration as components are taken out of service due to test, maintenance, or failures. These data on plant configuration changes was then used by each utility in their plant - specific PRA to calculate the corresponding changes in plant core melt frequency. This information combined with an analysis of the results of the Accident Precursor (ASP) Study (4, 5), formed the basis for insights into the effect of current technical specifications on plant operational risk and the potential for improvement through the use of a risk-based approach to technical specification.

The technical and institutional issues analyzed as a part of this study included: 1) characteristics of the required plant risk model, 2) requirements of the proposed software for calculating real time changes in plant risk due to plant configuration changes 3) approach for setting risk-based criteria, 4) Technical Specifications for components not included in the PRA, 5) elements of a reliability - centered surveillance concept for setting STIs, and b) major elements of cost associated with implementation of a pilot program.

Considering major technical and practical issues associated with this approach, it was concluded that at this time there do not appear to be any technical or institutional obstacles that prevent initiation of a pilot program to assess the characteristics and effectiveness of a real time risk-based approach to technical specifications for controlling plant operational risk (6). The NRC is currently discussing potential pilot programs with several volunteer utilities.

The second long term program is the Procedures for Evaluating Technical Specifications (PETS) sponsored by the NRC office of Nuclear Regulatory Research (RES) and performed by the BNL. PETS program has studied a large number of technical issues associated with use of risk and reliability techniques for improving technical specifications. Some of these topics include: a) expected risk contributions associated with present technical specifications (7), b) maximum risk contributions allowed by present technical specifications (8), c) proper evaluation of the risk contributions associated with technical specifications (9, 10), d) effect of PSA uncertainties on evaluating risk contributions from technical specifications, and numerical criteria to asses acceptability of risk associated with technical specifications (11).

Another NRC RES program is focused on detailed analysis of standby component failure data to differentiate between the standby stress and demand stress contribution to each component failure (12). Such an analysis can be used to optimize different components STIs and would also provide a more accurate model for standby component failures in PRAs.

The Electric Power Research Institute (EPRI) has also led several utility-sponsored programs to optimized technical specifications requirements. In one project, EPRI developed an approach and a computer code to assess application of risk and reliability techniques for optimizing AOTS and STIs (13). Another EPRI-sponsored program is the development and demonstration of Reliability Centered Maintenance program which can

be used to optimize STIs (14). Finally, EPRI has an on-going program to identify the major problems with current technical specifications based on extensive interviews with the plant operating staff, and development of a configuration control approach to technical specifications where commitment for certain forms of reliability monitoring can be used in exchange for change or relaxation of technical specifications.

In addition to the formal programs described above, many utilities internally have initiated programs to control plant operational risk regardless of technical specifications requirements. One example of such program at SCE is the analysis of plant core melt profile. In this program, on regular basis (such as once every quarter) the core melt profile of each plant is developed using actual changes to plant configuration and a plant-specific PRA. For those situations that core melt frequency is higher than a utility set limit without violating any technical specifications, lessons are drawn and directives are sent to various operation or maintenance departments to avoid similar situations.

Another example of a utility-initiated program is at PECO. In this utility, a corporate unavailability goal is set for component outages during maintenance. This corporate unavailability goal consists of an instantaneous unavailability limit due to one or more components and a cumulative goal for the whole fuel cycle. Both of these limits are a percentage of the plant's total core melt frequency. In this way, regardless of technical specifications requirement, the utility maintenance staff have to plan component maintenance schedules so that maintenance unavailability goals are not violated. These are only two examples of utility-initiated programs for monitoring plant system availability and plant risk profile. Many other utilities have instituted similar programs on volunteer basis. These point to the fact that a risk-based approach to setting technical specifications for controlling plant operational risk is a natural extension of each plants' desire to be able to plan their activities such that high risk configuration are avoided.

Finally, recent events during shutdown in the United States has focused a lot of attention to the plant risk during shutdown mode. An NRC task force is currently studying the past events during shutdown and analyzing various options for lowering plant risk during shutdown. One of the areas for potential improvement is a more comprehensive set of technical specifications that include risk and reliability insights and are more reflective of the different operating modes associated with shutdown and refueling.

2.2 PSA Applications to Technical Specifications in the Nordic Countries

Application of PSA techniques to technical specifications in Nordic Countries has focused on specific LCO and STI requirements that either appear to be non-optimum with respect to plant safety or overly restrictive in allowing plant operational flexibility (15). One of the major development in these studies has been the use of shutdown risk as a measure to decide to shutdown the plant given unavailability of one or more components, or stay at power (16). Analysis has shown that plant operational risk goes through a spike during shutdown before risk is reduced as the power is reduced. Comparison between the plant

risk profile due to unavailability of one or more components, with the shutdown risk if the plant is forced to shutdown, can be used as a decision input on whether to stay at power and continue to work on restoring a failed component. This approach is specially useful when the unavailable component(s) might be required during shutdown.

In addition to development and use of this approach for setting AOTs for selective components, Nordic countries have also used PRA techniques for optimization of preventive maintenance in their 4 loop 50% capacity standby safety systems design. Finally, work is also underway to improve the effectiveness of surveillance test procedures and schemes for standby equipment.

2.3 Application of PRA Techniques to Technical Specifications in England

One of the most comprehensive risk-based approaches to technical specifications is the Essential Systems Status Monitor (ESSM) code developed by Nuclear Electric (formerly a part of Central Electricity Generating Board (CEGBs)), which is currently being used at the Heysham B Nuclear Power Stations (17). The ESSM is a real-time risk-based computer code that is designed to assist the plant's operating staff in the assessment of the plant's status when one or a combination of several components is out of service. This assistance is provided in two separate modes. In the first mode, which is a real-time application of the code, the plant operators use the code to assess potential violations of technical specification requirements when one or more components are declared inoperable, both from deterministic and probabilistic points of view. In the second mode, the plant maintenance personnel use this program, on a daily basis, to schedule planned surveillance tests to make sure that planned outages will not violate any technical specification requirements or put the plant in an unnecessarily high risk area.

The code models the plant by using the plant-specific PRA. In its first application, the code has been used to model Heysham 2 nuclear power plant which is a 660 MWe Advanced Gas Reactor (AGR). The plant model in ESSM is as detailed as the PRA, i.e., it is down to the component level. For Heysham 2, some 2000 components have been modeled. The actual plant model used in ESSM is in the form of a master fault tree with the top event being the ultimate undesirable event, i.e., a large release. Thus, this master fault tree combines the traditional event trees and fault trees used in PRAs.

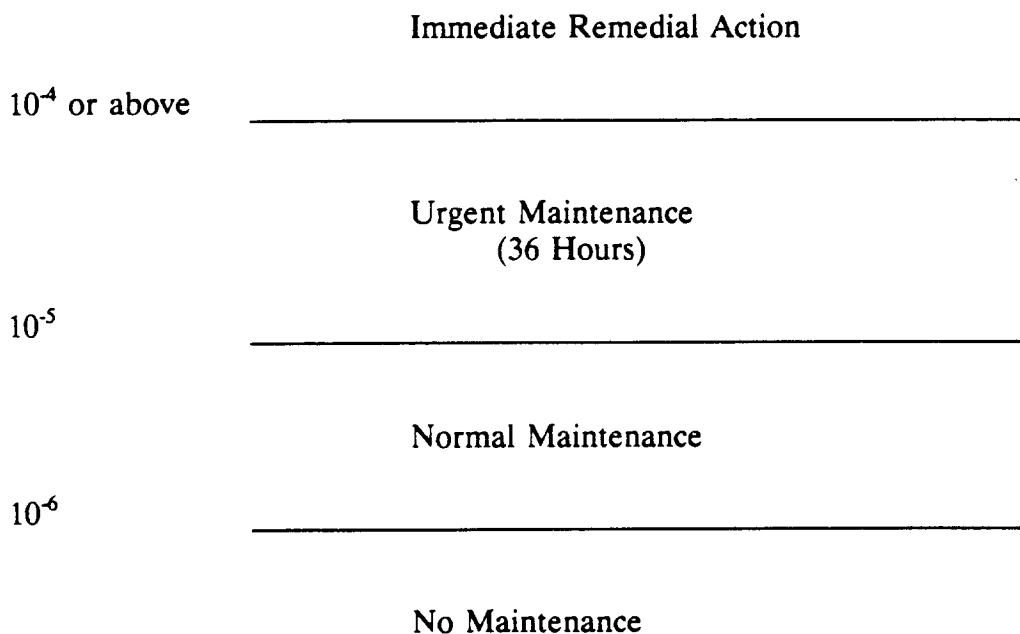
The code manipulates the Boolean equation for the fault tree and generates minimal cutsets. Currently, the code can run any case from all components available to cases with multicomponents out of service in less than 3 minutes. In fact, a 3 minute limit has been one of the design requirements of the code from the beginning. The code at the Heysham plant is run on a Honeywell DPS 6 minicomputer with 4 MB RAM and 67 MB disk storage.

At Heysham 2 plant, ESSM is located in the control room with the screen right above turbine system control panels. To make this program and its use acceptable to plant personnel, the code was designed to include both the currently used deterministic criteria

referred to as "back stop rules" and a new set of probabilistic criteria. During the start of a shift, the operator as a part of his routine activities checks the status of a ESSM. The code will indicate which components are out of service and, as a result, what is the status of the plant.

The status of the plant can be categorized in one of four states. The safest state is when all components are operable and there is no maintenance in progress. The next state is when one or more components that are not very important to safety are out of service and the plant is in normal maintenance, which implies no time limits for completion of maintenance. The next state is when one or more components important to safety are out of service and the plant is entered into "urgent maintenance," which implies that the plant should be out of this state within 36 hours or the plant must be shut down. Finally, the highest risk state of the plant is when "immediate remedial action" must be taken, which implies the plant should immediately be taken out of this state or it has to shut down. These states originally had been defined deterministically based on unavailability of one or more components. At Heysham 2, the division between normal maintenance and urgent maintenance is now based on probabilistic criteria. Correspondingly, a set of probabilities have been assigned to each of these states as shown below. It is important to note that the plant operators never see any probabilistic number. The only information provided to the operators is the plant state due to unavailability of one or more component.

Frequency of
Large Release
(Per Year)



The frequency of a large release is essentially the same as core melt probability since AGRs do not have a containment that could take any kind of pressure following a core meltdown. On the screen the plant operator never sees any probabilistic numbers, only one of the four plants states.

Following our earlier example, let us assume that at the beginning of a shift the plant operator checks the status of the plant and it is indicated that one or more components that are not important to safety are out of service and the plant is in normal maintenance state. During the shift, if the operator gets a call that indicates another components is inoperable, he will enter this in the ESSM and the code first checks the deterministic rules and would indicate to the operator if any of the back stop rules are violated. If none of the back stop rules are violated, he will know that he should not be in the immediate remedial action condition. Next the code performs a probabilistic analysis and indicates to him if he is in normal maintenance or urgent maintenance. If it is indicated that the plant is in urgent maintenance, then the plant is allowed 36 hours to get out of this mode or the plant has to shut down.

ESSM also provides the operator with several options for reconfiguring the plant or returning the equipment to service to try to get out of the urgent maintenance state. The selection of a particular option is made by the operator, not ESSM. This selection is based on what the operator perceives as the easiest way to get the plant out of this state and thereby lower the plant risk.

The plant operational personnel have easily accepted the program and, in fact, both the plant management and the operators have found ESSM extremely useful. The consensus is that this program helps the operator to quickly know whether taking components out of service results in a violation of any of the back stop rules. Thus, instead of the operator trying to use a set of deterministic rules with the potential for error, this code provides him with the necessary information in a short period of time. In addition, the code helps the operator to get out of an urgent maintenance state as fast as possible by identifying possible maintenance combinations to restore the most important components.

From a risk and reliability point of view, the probabilistic portion of the code can provide several important benefits. First, even though care is taken in developing deterministic back stop rules that cover all combinations of important components whose availability would result in an unsafe plant condition requiring immediate remedial action, there are no guarantees about completeness. The probabilistic analysis ensures this completeness by comparing the plant's instantaneous risk against a preset criteria. This will guarantee that the plant's level of risk is always controlled and the plant is not inadvertently in a very high risk level.

From an availability point of view, some of the deterministic back stop rules have been set very conservatively. Thus, strict adherence to these rules results in an unnecessary number of immediate remedial actions. The probabilistic analysis should identify these conservative

cases and help to increase plant availability by avoiding unnecessary immediate remedial actions.

In addition to the real time uses of code in the control room, the plant maintenance staff uses the code for planning purposes on a daily basis. In this mode, before taking any equipment out of service, the ESSM is used to assess the effect of the planned outage on the plant risk, including consideration of the current status of the plant. This will help the maintenance crew to plan their activity without any action that could potentially result in violation of a back stop rule or cause an undue increase in plant risk level.

Nuclear Electric is currently contemplating application of this code to other nuclear power plants in England including the new PWRs.

3.0 FUTURE APPLICATIONS

There are several approaches that involve use of risk and reliability techniques to improve the effectiveness of the technical specification requirements. These are briefly summarized in this section.

3.1 Line Item Improvements

As discussed previously there has been considerable activities in the United States and other countries to apply PSA techniques to change individual technical specifications requirements. Most of these activities have been initiated by either individual utilities or owner groups, with the regulatory bodies reviewing the requests. The motivation behind most of these applications have been to request relaxation of overly restrictive AOTs or overly frequent STIs.

In the majority of cases in the United States, the request for technical specifications relaxation have been based on calculation of the effect of the change on the plants core damage frequency. In all cases, it is shown that the impact of such a change result in a very small (few percentage increase) in core damage frequency.

The major difficulty that the regulatory bodies face with these types of requests is the lack of an overall risk-based criteria for assessment of acceptability of these requests. Usually the requests are reviewed in detail for technical accuracy and as long as the increase in core damage frequency as a result of technical specification changes is small the request is accepted. However, as the number of requests for a given plant or design increases, there is a need for assessment of cumulative effect of these changes to make sure they do not adversely effect plant risk.

Alternatively, it can be argued that within each plant's technical specifications, there are perhaps some requirements that if analyzed probabilistically using a plant-level criteria might result in stricter AOTs or STIs. Thus, eventhough line item improvements using probabilistic analyses should be encouraged, there is a strong need for a high level criteria and a comprehensive approach to this issue.

Several criteria at the plant level have been suggested and used on trial bases (6,11). None of these criteria have been officially accepted by a regulatory body. However, it might not be necessary to completely adapt a criteria to the same level of regulatory detail as technical specifications. These types of probabilistic criteria can be used as a guideline for PRA-based line item calculations, with the complete knowledge that these guidelines and calculations are used as supplements to our deterministic knowledge.

Once such a probabilistic criteria is set, then it can be used for several purposes. It would be the basis for determination of acceptability of a give technical specifications. It can also be used for assessment of utility requests to extend a Limiting Condition for Operation

(LCO) if the plant feel they might need a reasonable amount of extra time beyond the technical specification required AOT to complete a maintenance or test activity and avoid a shutdown.

More globally, such a criteria can be the basis for an initial examination of all AOT requirements for each individual plant. It can also be used for setting AOTs for combinations of component failures, an area which is lacking in the current technical specifications and potentially can lead to very high risk conditions.

Finally, the work by the Nordic countries in development of risk of plant shutdown as a measure to establish AOTs should be considered in the development of any risk-based criteria. This approach can be used for establishing AOT for components necessary during shutdown, or be part of the general criteria for establishing AOTs for all components.

3.2 Reliability Based Surveillance Test Intervals

Most of the programs discussed so far are designed to improve the AOT requirements by bringing greater risk-perspective to setting these limits. The STI requirements also can be improved by looking at the characteristics of each component using plant-specific data.

Recent studies have shown that there are two major contributors to the failure of a standby component. The first contributor is a time dependent standby stress caused by a series of component-specific events that are linked to lack of operation of the component. The second contribution is the time independent demand stress caused by testing of the component. The relative dominance of each of these contributions dictates the optimum test intervals. This implies that if a component is tested more frequently than its optimum test interval then its failure rate increases due to demand stress caused by excessive testing. Alternatively, if the interval between successive tests is much longer than the optimum point the component failure rate increases due to standby stress. Studies on several components so far have confirmed that these contributions are component specific and most likely they are also plant specific because of the impact of components environment including test and maintenance procedures (12).

One approach to resolve this issue is to analyze the past failure data for a series of important components such as diesel generators, MOVs, different types of valves and pumps. Because of lack of substantial plant specific data on each component, the initial analysis can be based on a large data base from all plants for each type of component. This analysis can next be refined by looking at the plant specific experience.

Such an analysis has two major benefits. First it would allow each plant to optimize their STIs and thereby lower standby components failure probability. The second benefit is incorporation of the correct standby components failure relationships in the plant-specific PRAs which could have a major impact on STI calculations as discussed below.

In most PRA's the average unavailability of a standby component is calculated using the following relationship:

$$q_d = \frac{1}{2} \lambda T \quad (3-1)$$

where:

q_d is the unavailability of a component on demand
 λ is the hourly component failure rate in standby mode, and
 T is the time interval between successive tests which is the same as the STI

The hourly component failure rate, λ , in most cases is derived from actual demand failure rates based on a known (such as monthly) test intervals for each component.

As mentioned earlier, the unavailability of a component in the standby mode is dependent on both a time dependent standby stress contribution, and a time independent demand stress contribution. Equation 3-1 used in most PRA's effectively implies that the time dependent portion of the standby component unavailability due to standby stress always dominates the total standby unavailability.

Thus, the major problem with using Equation 3-1 is that it gives a very pessimistic view of the impact of an increase in the STI, i.e., it implies that if a component's STI is tripled from monthly to quarterly, the component unavailability is also tripled. In reality, depending on the component, if the time independent demand stress dominates the total component unavailability, the impact of such a change would be substantially less than that tripling the component unavailability.

The correct relationship that must be used in the PRAs is:

$$q_d = (\lambda_{SS} * STI) + f_{DS} \quad (3-2)$$

where:

λ_{SS} is the hourly component failure rate due to standby stress
 STI is the Surveillance Test Interval, and
 f_{DS} is the standby component unavailability due to demand stress which is calculated from the relationship:

$$f_{DS} = \frac{\text{Number of demand stress related failures}}{\text{Total number of demands}} \quad (3-3)$$

The λ_{SS} and f_{DS} are component-specific elements that needs to be developed for both STI optimization and technical specifications calculations.

Thus, any component specific data collection and analysis activity that helps in determining the major contributors to the standby demand failure rate would help both the optimization of STIs and a more correct model in plant-specific PRAs.

3.3 Development of a Real Time Risk Monitor

As discussed earlier, current technical specifications requirements in some cases might not be effective in controlling plant risk, and in other cases might be too restrictive, preventing the necessary flexibility that the plant operations personnel might need. To assess these concerns and practical issues associated with a comprehensive risk-based approach to technical specifications, a pilot program can be initiated whereby one or more volunteer utilities would participate in an effort to gather actual data on plant operation, and develop the plant risk profile as a function of time using a plant-specific PRA.

The primary objective of such a pilot program would be to assess the characteristics and effectiveness of a risk-based approach to technical specifications compared to the current deterministic approach.

The starting point of this effort would be for each participating utility to model the plant status (in terms of components that are out of service) in their plant-specific PRA. Once the initial plant status is recorded, the plant personnel are requested to keep a daily record of change to plant status. There are two types of data that are necessary to this purpose. First, there is need for a daily record of what components are taken out of service, and what components are put back into service. All changes to plant status should be recorded regardless of whether the component is taken out on a voluntary basis for preventive maintenance, a normal test, or as a result of an actual component failure. The second type of data is related to situations where the plant would have wanted to take a component out of service for preventive maintenance, special test, or any other reasons, but they were prevented because taking the component out of service would result in entering an LCO.

The case study must consider the difference between the actual equipment inoperability and the administrative definition of inoperability which could be much more conservative. This difference will significantly affect study results.

Using these data, the plant personnel can next calculate the changes in the plant operational risk profile due to plant configuration changes using their plant-specific PSA. These calculations can be performed on a daily or weekly basis depending on the plant's preference and availability of the required resources. For this pilot program it is proposed to use core melt frequency to represent plant operational risk to avoid the larger effort associated with containment and consequence analysis, and questions regarding uncertainty with Level 2 or 3 PRA analyses.

The starting point for these calculations would be to calculate the core melt frequency of the plant for the initial plant configuration that data gathering effort was initiated. From this point, the core melt frequency of the plant would be calculated for each change in plant configuration due to taking a component out of service or restoring a component back to operation. If at any time the plant enters a Limiting Condition for Operation (LCO), the risk-based AOT associated with this situation would be calculated using a risk-based criteria and recorded to compare with the current deterministic criteria. In addition to this, for each scenario that the plant would have wanted to take a component out of service for preventive maintenance or other purposes, but were prevented because of violation of LCO limits, a calculation should be done on the increase of the plant's core melt frequency if that component had been taken out of service and record the risk-based recommendation for these scenarios.

The potential benefits of such a pilot program are:

- 1) Insight into the changes in the plant core melt frequency profile as a function of time during normal operation of the plant. Specifically, assessment of the effectiveness of the current deterministic technical specifications in controlling plant operational risk. This includes identification of actual scenarios consisting of multiple component outages that do not result in technical specifications violations, but result in large increases in core melt frequency and are not intuitively obvious to the plant operators. This point would provide the initial input on whether a real-time risk-based advisory system would be useful in assisting the plant operators in controlling plant operational risk.
- 2) Effect of current deterministic technical specifications in preventing the plant to have the necessary flexibility in performing tests or preventive maintenance on various components without a substantial increase in plant's operation risk.
- 3) Application of risk-based criteria for setting AOTs and practical issues associated with use of a risk-based criteria within a regulatory framework.
- 4) Assessment and resolution of a whole series of PRA modeling issues such as changes to initiating event frequencies due to ongoing maintenance activities, recovery, and human error models.
- 5) Understanding of any practical issues associated with acceptability of such an approach by the plant personnel and the regulatory staff.

Finally, the proposed pilot program discussed so far, the plant risk profile, is developed on a daily or weekly basis. This is a practical starting point to approach this program. This approach can become real time if a fast response software similar to ESSM is developed. However, development of such a software would be initiated after a successful semi-real

time pilot study where the benefits of this approach are compared to current well established technical specifications.

3.4 Shutdown Configuration Application

With the increasing concern regarding the risk associated with the operation of a reactor in the shutdown and refueling modes, the application of probabilistic analyses to shutdown conditions and shutdown related technical specifications appears to be warranted. Many of the approaches described in the preceding sections can be used to address shutdown technical specifications. Shutdown PRAs can be used to a) identify risk significant configurations associated with shutdown operation (for example mid-loop operation in a PWR), b) identify line item improvements to allowed outage times, c) establish a coordinate surveillance test intervals, and d) create a shutdown real time risk monitor.

Shutdown PRAs are only now being performed in a detailed and coordinated manner. The French have completed a shutdown PRA and the USNRC is developing a prototypical PRA for both a PWR and BWR during shutdown. Plant specific application of these methodologies could provide the basis for implementing risk-related technical specifications during shutdown.

4.0 CONCLUSIONS

Substantial progress has been made in the application of risk and reliability techniques to plant safety in general, and to the technical specifications requirements specifically. Based on the results of a series of studies in several countries around the world, it is clear that the effectiveness of the current technical specifications to control plant operational risk can be improved substantially by applying risk and reliability techniques to these requirements. These types of applications can vary from line item improvements using simple risk-based calculations all the way to a complete risk-based approach to technical specifications. What is important is to start a systematic approach to apply these techniques to improve maintenance outage planning, to better control plant core damage or risk on real time basis, and to create a better basis for AOTs and STIs requirements.

The most interesting aspect of risk-based approaches to technical specifications is that it can improve plant safety while increasing plant availability. Worldwide experience with the application of risk and reliability techniques to technical specifications to date provides a strong indication about the importance and effectiveness of this approach for improving plant safety and availability.

5.0 REFERENCES

1. Puglia, W.J., et. al., "The Effect of Proposed Changes in the New Standard Technical Specifications on Nuclear Power Plant Risk," Final Report, SAIC-90/1394, June 28, 1991.
2. Atefi, B., et. al., "Alternative Approaches to Risk-Based Technical Specifications," Final Report, SAIC-88/3110, June 3, 1988.
3. Atefi, B., et. al., "Feasibility Assessment of a Risk-Based Technical Specifications," SAIC-91/1033, March 29, 1990.
4. Cottrell, W.B., et. al., "Precursors to Potential Severe Core Damage Accidents 1980-1981," NUREG/CR-3591, ORNL/NSIC-217, July 1984.
5. Minorick, J.W., et. al., "Precursors to Potential Severe Core Damage Accidents 1984, 1985, 1986" NUREG/CR-4674, ORNL/NOAC-232, Volume 1-6.
6. Atefi, B., et. al., "Feasibility Assessment of a Risk-Based Technical Specifications," Volume 1, 2, NUREG/CR-5742, SAIC-90/1400, May 1991.
7. Samanta, P.K., et. al., "Evaluation of Risks Associated with AOT and STI Requirements at the ANO-Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, August 1988.
8. Vessely, W.E., "Evaluation of Allowed Outage Times (AOTs) From a Risk and Reliability Standpoint," NUREG/CR-5264, BNL, August 1989.
9. Vessely, et. al., "Evaluation of Diesel Unavailability and Risk Effectiveness Surveillance Test Interval," NUREG/CR-4810, BNL Technical Report A-3859-10-18-89, October 1989.
10. Samanta, P.K., et. al., "Consideration of Test Strategy in Defining Surveillance Requirements," BNL Technical Report A-3859-10-18-89, October 1989.
11. Vessely, W. E., "Procedure to Define Numerical Criteria to Assess Risk Associated with Technical Specification," BNL Technical Report A-3230, June 1986.
12. Lofgren, E.V., et. al., "Analysis of Standby and Demand Stress Failure Modes: Methodology and Applications to EDGs and MOVs," Draft Report, SAIC, February 7, 1991.
13. Wagner, D.P., et. al., "Risk-Based Evaluation of Technical Specifications," NP-4317, EPRI, March 1987.

14. Goertner, J.P., et. al., "Demonstrations of Reliability Centered Maintenance," NP-8152, Volume 1, January 1989, Volumes 2-3, September 1989.
15. "Optimization of Technical Specifications by Use of Probabilistic Methods," A Nordic Perspective 1985-1989. Draft Report NKA/RAS 450, November 1989. Nordic Liaison Committee for Atomic Energy (Edited by K. Laakso, Technical Research Center of Finland).
16. Mankomo, Tumas, and Mikko Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," April 10, 1991.
17. Horne, B.E., "The Introduction of Probabilistic Evaluations Into the Operation of CEGB NPP Using the ESSM Facility," ANS/ENS International Topical Meeting on Probabilistic Safety Assessment and Risk Management, Zurich, Switzerland, September 1987.

