THE 4TH INTERNATIONAL TOPICAL MEETING ON
NUCLEAR THERMAL HYDRAULICS, OPERATIONS AND SAFETY
April 6-8, 1994, Taipei, Taiwan

RISK MANAGEMENT THROUGH DYNAMIC TECHNICAL SPECIFICATIONS

George T. Klopp
Commmonwealth Edison Company
1400 Opus Place, Suite 300
Downers Grove, IL 60515

Thomas A. Petersen
NUS
1411 Opus Place, Suite 103
Downers Grove, IL 60515

INTRODUCTION

The wide deployment of plant specific probabilistic risk assessments for nuclear power plants has provided the means to effect a fresh risk management perspective and a fresh, risk based, regulatory outlook on nuclear power. There has been a great deal of conversation on risk based regulation within the U. S. nuclear power industry but, curiously, very little on effective risk management. This paper proposes a means to link the two subjects through the plant Technical Specifications. A revised concept for Technical Specifications is suggested which is based on deterministic analyses and probabilistic risk assessments for each plant. The revised Technical Specifications would consider, on a real-time basis, the exact state of the plant in terms of the status of key components and systems. It would depict current plant risk levels and compare those levels to the desired and limiting (alert/action) levels. It would advise the plant operator on the risk impact of proposed actions through a simple query system and illustrate the impact of such actions on plant status relative to designated risk values.

The basis for the proposed approach lies in realistic deterministic plant analyses and probabilistic risk assessment (PRA) deployment tools being developed, in parallel, by a number of parties in the U.S. today. These PRAs are based primarily on the existing plant responses to Generic Letter 88-20, "Individual Plant Examinations" (IPEs). Each of these tools allows the plant operator to input, on a real-time basis, the status of key equipment and systems. The tools then provide explicit illustrations of dependency effects; updated, "real-time" risk status indications such as core damage frequency; and, in some cases, allow the operator to assess the risk impact of removing from service selected components for maintenance or testing. These systems generally operate on personal computers and provide nearly instantaneous responses to plant queries.

Moving from these tools to real-time "risk-based", or as defined in this paper, "dynamic" Technical Specifications is, technically, a small step. Risk limits would have to be established; the displays would have to be chosen to reflect the regulatory purpose of the Technical Specification; and the calculational "engines" would need to undergo a verification and validation process. The largest hurdle is not technical. It is, rather, in the area of human acceptance and the regulatory basis for a new way of doing business and a new way of judging safety.

BACKGROUND

The philosophy of linking risk management with risk-based regulation, via plant Technical Specifications (TS) is based on existing TS not always reflecting safest action. Risk-based regulation can be viewed as using PRA insights to focus utility and regulatory attention on design and operational issues relative to their impact on risk to the public. As uncertainties associated with the techniques and data bases have decreased and their credibility increased, the use of PRA information to address regulatory issues has increased. Safety concerns derived from qualitative risk insights have been primarily the bases for most rules since they were derived prior to the availability of PRA techniques.

In as early as February 1987, the Commission's Policy Statement on Technical Specification Improvements for Nuclear Power Reactors, recommended further development of risk and reliability techniques in defining the requirements of the Technical Specifications.

Risk is currently reflected in the regulations by either prescriptive or performance requirements based either on quantitative or qualitative risk estimates. For example, the ATWS rule is prescriptive and is based on quantitative risk insights (10 CFR 50.62). The ECCS rule is performance related and is based on qualitative risk insights. As a result, quantitative risk, such as core damage frequency (CDF) can be reflected in some regulatory requirements, and furthermore are appropriate to be addressed in dynamic TS. In addition, to ensure safety is not unduly compromised, TS that are based on prescriptive regulations must be understood prior to allowance to be more risk-based.

The NRC has discussed (Reference 1) that it will consider regulatory changes sought by the industry when they are technically justified and do not adversely affect existing plant safety. They will also grant exemptions when appropriate plant-specific requests are submitted. Hence, it is expected that dynamic TS do have a place in future risk-based regulation. In addition, ongoing programs, such as the new standard Technical Specification Improvement Program will be examined for future risk-based changes.

DYNAMIC TS VS. CURRENT TS

The purpose of dynamic TS is to take advantage of optimization possibilities of Allowed Outage Times (AOTs), Surveillance Test Intervals (STIs), and Limiting Conditions of Operation (LCO). Of the remaining Technical Specification sections (definitions, safety limits, limiting safety system settings, design features, administrative controls, and bases), only LCOs, AOTs and surveillance requirements are potential sections able to be influenced by PRA techniques.

The state-of-the-art for PRA needs to be commensurate with the desired safety goals. The availability of pertinent data, the adequacy of modelling, the accident progression understanding, and accident phenomena are key areas for uncertainties and limitations affecting the PRA accuracy. Accordingly, dynamic TS with absolute numerical values for acceptable CDF and resultant AOTs and STIs, for example, may not be practical from a licensing and enforcement perspective. Rather, ranges of acceptable values for change in CDF (relative risk choices) and resultant AOTs and STIs may be more appropriate. Based on equipment configurations and unavailabilities, these ranges would provide levels for acceptable plant operation, levels for increased risk awareness and compensatory measures, and ranges for actions requiring plant shutdown.

In dynamic TS, the AOTs and STIs for components and systems are based on the importance of the component or system to the actual plant's core damage frequency.

Existing TS do not always provide the safest fallback action. Multiple events or outages are not consistently addressed by most Technical Specifications, but dynamic TS can address these concerns. As may be allowed by some plant Technical Specifications, some multiple component outages could occur that, in turn, could significantly increase plant risk, yet not even violate an LCO. In some other cases, plant shutdowns may be required by Technical Specifications, yet the increase in plant risk due to the configuration may be negligible. Some LCOs and AOTs are too restrictive or do not consider that different plant operating conditions might alter the risk significance of each TS requirement.

Dynamic TS would not only enhance Technical Specification compliance and optimization, but minimize unnecessary plant shutdowns, improve plant safety, and enhance testing, maintenance planning and inspection programs. Furthermore, dynamic TS would provide a major step towards development of a comprehensive plant risk management program.

Dynamic TS can enhance or replace existing requirements, while improving plant safety. A dynamic TS system has the potential to improve both plant safety and availability, hence, the potential for increased capacity factor. As a result, a positive outlook will be placed on the continued use of PRAs.

One potential advantage of dynamic TS is to allow on-line maintenance to reduce replacement power costs when the maintenance is performed while the reactor is shut down.

The scope of dynamic TS may encompass differing levels of risk important to plant equipment such as found in custom TS, Standard TS, or Improved TS. Furthermore, for each type of TS and plant specifics, each TS may be based on qualitative risk or may not be modelled in the plant PRA.

In Great Britain, Nuclear Electric has developed a system called Essential Systems Status Monitor (ESSM) for its Heysham B Nuclear Power Station. This is a system that allows operators to determine plant risk based on current equipment operability status. This system is an integral part of the plants Technical Specifications and provides the principal basis for acceptable plant operations.

PROGRAM DESCRIPTION AND DEVELOPMENT

Research and development has been conducted on prototype real-time risk monitor programs for evolution into dynamic TS. These programs are based on actual PRAs and real-time risk management systems and associated data bases and inputs.

A real-time plant operating risk monitor, Global Risk Management System, (GloRiMan), has been developed by Commonwealth Edison Company. This system utilizes a library of cutset equations for each of the various plant operating states that are likely to be experienced. This approach reduces the likelihood of model truncation errors. Changes to the risk model are accomplished by the regeneration of the equation libraries.

Another real-time plant operating risk monitor (Safety Monitor) has been developed by the Southern California Edison Company. This software program is based on a Level 1 PRA. It provides Level 1 core damage results in less than 2 minutes by utilizing optimized PRA modelling and a 486DX2-66 personal computer. It has been verified and validated and the Safety Monitor yields the same numerical results as the original model. The program will be manually and periodically updated/accessed based on plant configuration changes. The program utilizes unique plant operating conditions, as well as various environmental and testing conditions in the assessment of plant risk (CDF). The program is designed to Quality Affecting standards and Verification and Validation has been performed.

The design requirements of both the GloRiMan and Safety Monitor systems include the use of key PRA information to be displayed in a format readily understandable to non-PRA trained personnel and the ability to calculate an estimate of current plant risk using a complete Level 1 PRA fault tree within a few minutes. Risk model development, software operation, and plans for plant usage of the Safety Monitor are discussed in Reference 2. Both systems have directly applicable attributes for use in a dynamic TS system.

Dynamic TS model would be based on a plant specific PRA. It would have to be capable of being quantified rapidly based on the real-time plant configurations. An operator would use the program interactively and the program will not be static. The program operator would not be required to have detailed PRA knowledge beyond a brief introduction to its overall use. The program model would be more detailed than the normal PRA. This detail would provide assurance that significant component outage combinations are captured even though they may not have been important to the average core damage frequency.

OVERALL REGULATORY REQUIREMENTS FOR ACCEPTANCE

Risk management, risk optimization, and balancing of risk of shutdown vs. staying at power by AOT optimization and its relationship to defense in depth is the overall theme for regulatory acceptance of dynamic TS. LCO and STI optimization are also important and may be possible via dynamic TS in certain conditions.

Quantitative risk is important, but change in risk is most important. Regulatory issues to be addressed will include the licensing of the dynamic TS process. This may include licensing of the model, the computer software, the change process, the computer hardware, and all associated documentation. A backup computer, a methodology to perform hand calculations, and/or a license document with prescriptive AOT and STI values may also be required for licensing of the process.

Approximately 30% of current Standard TS are addressed in an average plant IPE. A consistent risk perspective will be provided via the dynamic TS. Items modelled in PRAs, but not in the current TS also need to be addressed for potential inclusion it the dynamic TS.

The use of risk insights to improve TS, such as STIs, AOTs, LCOs (identification of risk significant systems, structures and components), and in assuring a consistent application of risk perspectives are TS areas that can benefit from the application of dynamic TS. Overly restrictive TS will also be identified.

In dynamic TS the AOTs are not fixed as in the case of current TS. The AOTs for different components and systems are based on the importance of the component or system to plant risk. This risk is a function of current plant configuration and will increase or decrease depending on what other components or systems are made available or unavailable at the same time.

A risk based criteria set for AOTs will have to be developed for dynamic TS.

Dynamic TS AOTs would be based on the plant's dominant accident sequence core damage frequency. A relationship of the change in risk due to component unavailability to the resulting AOT will be required to be developed.

Use of dynamic TS may help to allow such occurrences as redundant trains of the same system to be simultaneously unavailable for a period of time, provided backup systems serving the same safety function are available. LCO identified systems, structures and components (SSCs) may be reduced in number and importance via dynamic TS results.

Surveillance Test Intervals (STIs) for dynamic TS would be based on industry data for known average failure rates of components. In addition, dynamic TS would need to consider the affect of demand stress (vs. only standby stress), since some equipment such as diesel generators have their unavailabilities dominated by demand stress failures. Factoring this into dynamic TS would ensure plant-specific accuracy.

IPE COMPATIBILITY WITH DYNAMIC TS

Current Technical Specifications are component-based, therefore the PRA level of detail must be compatible. Some components may not be modelled in the plant PRA, therefore this level of detail must be compatible. In addition, plant configuration control must be provided and records or computer data bases maintained to ensure accurate and timely inputs to the dynamic TS.

Some TS may not be addressed by the PRA. Since TS are component based and PRAs are event based, the PRAs must be related to the TS. Assumptions in the PRAs and TS must be compared and uncertainties resolved before dynamic TS can be licensed.

Changes to procedures, design, data or assumptions modelled in the PRA may require a change to the dynamic TS, therefore, potentially requiring regulatory acceptance prior to the change of the dynamic TS system.

Some systems not Level 1 PRA modelled include: containment isolation valves, containment pressure control systems, and containment radioactivity cleanup systems. These systems can be addressed on a quantitative risk-basis if Level 2 PRA models are included in the dynamic TS.

Other Technical Specification requirements not able to be addressed by PRA techniques include: shutdown margins and control rod response times. Parameter indications such as pressure, temperature, flux and power distribution limits, and special test exceptions may also not be addressed in PRAs unless addressed as operator actions. These requirements must be assessed via other risk-based and qualitative approaches such as direct risk impact (component risk importance), indirect risk impact (test-induced risk), reliability (dominant failure cause), licensee burden (labor intense factor/risk importance), and engineering judgement.

Shutdown systems are also not included in Level 1 PRAs, hence, inclusion of shutdown risk assessments would also provide quantitative risk information for dynamic TS for these systems.

Low ranked components in PRA may require review for inclusion also in the dynamic TS. TS items not addressed by current PRAs, must be addressed in some risk-related manner to provide consistency for the overall dynamic TS model. Additional risk-based (quantitative/qualitative) approaches to non-PRA modelled TS can be developed.

All possible system alignment states during power operation must be modelled, such as "swing trains/components" even though not normally modelled in the Level 1 PRA (due to being logically equivalent). Dynamic TS PRA models need to be reviewed to determine which components pertain to each basic event.

Dynamic TS will allow the varying of AOTs based upon specific plant configurations, e.g., a component may have an extended AOT, provided certain other risk contributing components are not simultaneously unavailable, and a shorter AOT if these risk contributing components are unavailable.

Current IPE models do not have sufficient details especially in the areas of instrumentation and control, such as reactor protection system (RPS) and engineered safety features actuation system (ESFAS). In most PRAs the RPS and the ESFAS instrumentation and control logic are not modelled. Since a high percentage of current Technical Specifications address this instrumentation, this instrumentation should be modelled into the dynamic TS. Also support systems such as equipment cooling are reflected in TS, but overly conservatively analyzed in PRAs.

For dynamic TS to be accepted as regulatory basis for operation, many issues must be addressed, such as in the enhancement of deterministic based specifications. How defense in depth and single failure criterion are supplemented by risk-based approaches, is one of many issues. Other issues include the adequacy of analytical tools, the availability of decision criteria and methods, and policy issues such as how license amendments are approved and the use of 10 CFR 50.59 reviews.

PROGRAM IMPLEMENTATION

Should the plant PRA be in poor condition, dynamic TS results will be inaccurate and not licensable. Real-time systems may be best serving if an automated input is received from a plant configuration control system. This system would receive all real-time actual and planned equipment outage data resulting from all maintenance and testing activities, and equipment rotation data.

Plant modifications and dynamic TS model configuration control must be maintained for a properly operating dynamic TS. Living PRA (real-time or periodic) data collection and input techniques must be determined. Fast response time software, a detailed plant risk model that is component based or compatible with its related TS, and a plant configuration system are required to operate a dynamic TS system.

The plant configuration control system will track the availability or unavailability of all plant components based on all plant activities affecting the components such as testing or maintenance. Plant operators, maintenance schedulers, and outage planners would access the system for actual and hypothetical risk profiles based on component availability information. The operating staff would maintain inputting of the real-time actual component availability data based on plant operating status, or this task may be automated via outputs generated by the plant process computer.

It is expected that once an IPE is completed there would not be many changes at the plant to warrant model changes in IPE, however, a full PRA rebaseline each 10 years may be appropriate. IPE changes may be required for cases where plant modifications are involved. However, there may be some minor model changes resulting from procedure changes or from Emergency Operating Procedure changes. A basic PRA update may be necessary about every 18 months to each 4 years due to modifications performed during plant outages.

Against some common thoughts that equipment failure rates vary significantly from year to year, the equipment failure rates do not, and should not, vary significantly on an annual basis. This is true for the failure model that is used in current IPE studies. One of the basic assumptions which is made in evaluation of failure data calculation is that failure rate is constant with respect to time. If a significant variation in equipment failure data is detected, this essentially indicates that the current IPE based dynamic TS failure model is not adequate to properly represent the existing plant condition. This may warrant using a more complex failure model such as a time dependent failure model, if the variation in failure data is mainly driven by equipment aging problems.

FUTURE USES AND ENHANCEMENTS

Several data collection features and resultant availability information utilized in a dynamic TS system may also support compliance with other performance based requirements such the NRC Maintenance Rule (10 CFR 50.65), e.g., identification of SSCs, and the setting of equipment and system availability goals. Much of the same plant configuration data collected would be utilized in the plant living PRA program.

A system piping and instrumentation diagram (P&ID) drawing may be utilized in dynamic TS as the primary input screen for determination/input of unavailable equipment. This human-factored entry screen would enhance the speed and mental processing of displayed risk profile results.

Dynamic TS results can be utilized in justifying on-line (Mode 1) maintenance while minimizing overall operating risk. In addition, the prioritization of both on-line and off-line maintenance will be enhanced with dynamic TS.

Inclusion of Level 2 PRA models, for those IPEs which did not address Level 2 PRAs, for dynamic TS will capture those containment related TS systems for risk-based regulatory management.

Shutdown system models included in dynamic TS would allow the quantitative comparison of risk impacts of performing maintenance while at power versus while shutdown (or any other non-power plant mode). Generic plant outage schedules or preplanned outage schedules could also be evaluated for risk significance by the grouped (by out-of-service time) input of system/component outages into the dynamic TS.

CONCLUSION

Dynamic TS has several advantages over the currently used deterministic Technical Specifications: comprehensive plant risk models (PRAs) can be utilized which provide greater insights due to individual and multiple component outages, beyond design basis accidents and severe accidents can be addressed, and plant and regulatory safety goals can be achieved.

A demonstration program utilizing IPEs that address the implementation concerns identified in this paper, and facilitated possibly under the auspices of NUMARC, should be initiated at a few volunteering nuclear power stations to provide assurance to both the utility and the regulatory agencies that dynamic TS are feasible and can be used to minimize plant risk and maximize plant availability. The demonstration program should provide a real-time comparison between the dynamic TS and the current deterministic Technical Specifications utilized at the station. The comparison results will identify any implementation concerns and verify the usefulness of the dynamic TS. Upon completion of the demonstration programs, the nuclear industry will be able to assess its needs for adoption of all or selected aspects of dynamic TS.

REFERENCES

1. "Risk-Based Regulation", NRC Memorandum, James M. Taylor to NRC Commissioners, February 22, 1993.

2. "Development and Application of the San Onofre Safety Monitor", Thomas G. Hook, Roger J. Lee,

Thomas A. Morgan, 4th International Topical Meeting on Nuclear Thermal Hydraulics, Operations, and Safety, Taipei, Taiwan, April 1994.