Volume Four

Regulatory Review Group

Risk Technology Application

U.S. Nuclear Regulatory Commission
Office of the Executive Director For Operations

Frank Gillespie
Joe Murphy
Cecil Thomas
Johns Jaudon
Claudia Craig
Tony Cerne
Mary Drouin
Byron Siegel
Mack Cutchin
Administrative Support: Nancy Olson
Technical Editor: Louise Gallagher

6/1
DFO3

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The current state of the art in probabilistic risk analysis (PRA) technology was examined to determine under what circumstances information, either qualitative or quantitative, gleaned from PRA methods could be used in the regulatory process. It was determined that PRA methods provide an integral tool that can be used to help ensure coherence and consistency in the regulatory process and provide a means of converting diverse deterministic requirements to performance based requirements. This provision can occur with equivalent protection to public health and safety, while offering increased flexibility to licensees, provided the risk-based criteria are met. To this end, the current state of the art in PRA methods were assessed considering how the many strengths of these methods could be exploited, while minimizing the significance of those weaknesses that still remain in the application of risk-based methods in regulation.

Work in progress under the U.S. Nuclear Regulatory Commission (NRC) sponsorship devoted to the research, development, and application of risk-based methods to aid the regulatory process was surveyed. NRC has had an active program investigating the use of PRA methods in regulatory practices since 1983, and much (but not all) of the work done by others in this area in the U.S. draws heavily from this research. The more important elements relative to use of risk-based techniques in regulation are described in Section 4.9.1.

A number of papers sponsored by the regulated industry that address the potential use of risk-based techniques in regulation have been published in the literature. Informal discussions were held with several of the authors. Broad-based industry research on use of PRA methods for regulatory purposes, as reflected in the literature, is fairly recent, but several utilities have had long-term ongoing programs on use of risk methods to improve operations. These programs could be extended to the regulatory environment.

Further, international literature addressing the potential for risk-based regulations were reviewed, particularly the information contained in reports and workshops sponsored by the Organization for Economic Cooperation and Development/Committee on the Safety of Nuclear Installations Principal Working Group 5 *[Ref. 4-1]*. Because of their current substantial efforts in this regard, detailed discussions were also held with utility and regulatory authorities in Mexico and the United Kingdom to gain the benefit of their experience.

Based on the above, it is recommended that the utilization of PRA-based techniques in the regulatory process be characterized into three general classes, each having similar requirements in terms of the boundary conditions and assumptions used in the analysis, as

well as similar requirements in terms of the depth and breath of the review that would be required by the NRC staff.

- *Reliance on Quantitative Results from Multiple Plant-Specific PRAs* — This category of risk-related regulatory actions would use the risk analyses to separate the potentially important components and systems from the unimportant. This relative importance would be from a PRA perspective based on core damage prevention, relying on both plant-specific studies as well as on compilations of the results of risk-based studies of similar plants.

  This type of usage could be based on the type of PRA modeling effort that is common in responses to the Individual Plant Examination (IPE) Generic Letter 88-20, and the type of review currently being applied to IPE reviews by the NRC staff would likely suffice. Generic failure rate data could generally be employed and frequent updates of the PRA studies would not generally be required.

  Performance-based responses to the Maintenance Rule and risk-based approaches to graded quality assurance are possible examples of potential usage.

- *Reliance on Single Plant-Specific PRA Quantitative Results in Selected Areas* — Efforts of this type would require careful attention to the PRA methods and analyses in selected areas but would not involve close scrutiny of the entire plant risk analyses. It could be used to improve regulatory flexibility for a given component, or applied broadly to selected portions of the plant at the train level, without examining the detailed modeling at lower levels in the analytical trees.

  This type of application would also generally require average PRA modeling. Generic failure data would be sufficient in most instances, but it would need to be augmented with plant-specific data in those selected areas where heavy reliance was placed on the plant-specific results. For greater than one-time use, the PRA would have to be modified as necessary to reflect any changes in the current plant design and operational practices. This usage would likely require updating at least each refueling outage.

  Examples of this category would include optimization of selected Technical Specifications, evaluations of "unreviewed safety question" under 10 CFR 50.59, and use of pre-calculated configuration management analyses to support extension of allowed outage times under certain circumstances.

- *Reliance on Numerical Results from Single Plant-Specific PRAs* — In this category, regulatory decisions would be based almost exclusively on the numerical PRA results. It would require a very comprehensive analytical effort, since, in

this type of application, minor changes in assumptions or boundary conditions may significantly affect regulatory decisions.

This type of application would require a level of detail that either stretches or exceeds the current state of the art. It would require a comprehensive plant-specific data analysis, and would require that the PRA be reviewed by NRC staff at a depth equivalent to that afforded to a final safety analysis report in the course of a Part 50 operating license review.

An example of this type of usage would be the development of risk-based technical specifications requiring on-line updating of PRA models.

In the following sections, for each example in each class discussed above, candidate requirements have been developed for the boundary conditions and assumptions used in the analyses. These requirements should be regarded as candidate regulatory positions and can serve as a jumping off point for detailed discussions with the public and the regulated industry.

Beyond the technical recommendations, more specific recommendations regarding the nature of the regulatory environment needed to introduce the use of risk-based analyses in a broad fashion are offered.

- The current state of development and utilization of PRA techniques in the industry can support use of risk-based regulatory approaches at the present time. Several utilities have ongoing programs using risk methods and "living" PRA to improve operations and maintain plant safety and efficiency that could be extended to the regulatory environment and provide increased licensee flexibility while maintaining or improving the safety envelope. It is recommended that the Commission elicit licensee proposals in this regard to support such an effort.

- The development by NRC of methods for optimizing Technical Specifications using risk-based techniques is nearing completion and, with publication of a handbook early in calendar year 1994, will provide a technical basis for judging the acceptability of risk-based approaches proposed by licensees. In addition, this handbook could serve as the point of departure for discussions between the NRC staff and the industry leading to industry-proposed guidance, suitably endorsed by NRC. It is recommended that this handbook be published as a regulatory document or perhaps as a regulatory guide. This handbook can provide guidelines for methods or similar techniques that would be used in a pilot program in the near future if there is industry interest in such an application.

- NRC programs and interests on the development and implementation of risk-based methods in regulation currently span multiple offices and organizations. An integral agency plan covering the research, development, implementation, and use of risk-based techniques in regulation is needed in maintaining a consistency of approach throughout the agency and in allocating scarce resources. This plan would also assist in the efficient use of the limited number of NRC staff with expertise in PRA.

- Possible risk-based regulatory approaches span a continuum from modest applications of conventional PRA methods to techniques for risk-based configuration control on a real-time basis. They represent an increasingly valuable complement to the present regulatory structure. The required resource commitments for both the licensee and NRC are likely to increase as more complex approaches are investigated; however, these more comprehensive approaches will also offer the most flexibility to the licensee while maintaining the safety envelope.

  A reasoned approach is recommended for the transition to the more risk-based approaches, testing benefits gained versus costs of implementing in pilot programs before proceeding to complete implementation industrywide. As indicated above, certain risk-based approaches can be implemented now, while others will be suitable for trial investigation in the near future. An investigation of the usages that are compatible with the current strengths and limitations of risk methods needs to be pursued in supporting a transition to PRA-based regulation.

- In effect, the NRC currently uses PRA insights to primarily add requirements to the industry. This use of PRA needs to be changed to allow PRA-based insights to reduce regulatory burden when it is shown that such a reduction does not reduce the safety envelope of the plant. Thresholds (e.g., NRC guidelines on content of submittals, acceptable PRA methods, and decision criteria) must, therefore, be established by the NRC for each PRA usage class (as described above) in concert with any industry-proposed pilot applications of these potential uses.

4.1 INTRODUCTION

In 1975, the U.S. Nuclear Regulatory Commission (NRC) completed the first quantitative study of the probabilities and consequences of severe reactor accidents in commercial nuclear power plants — the Reactor Safety Study, published as WASH-1400 *[Ref. 4-2]*. This work for the first time used the techniques of probabilistic risk analysis (PRA) for the study of severe core damage accidents in two commercial nuclear power reactors. The product of probability and consequence, a measure of the risk associated with severe accidents, was estimated to be low relative to other man-made and naturally occurring risks for the two plants analyzed.

Following the completion of WASH-1400, and similar efforts conducted in parallel in other countries (most notably, Phase A of the German Risk Study *[Ref. 4-3]*), research efforts were initiated to develop advanced methods for assessing accident frequencies, improved means for collecting and analyzing operational plant data were put in place, methods were initiated to improve the ability to quantify the effects of human errors, and studies to better predict the nature and effect of common cause failures were begun. Further, limited research was begun on those key severe accident physical processes identified in the Reactor Safety Study.

The 1979 accident at Three Mile Island (TMI) substantially changed the character of the analysis of severe accidents worldwide. Based, at least in part, on the comments and recommendations of the major investigations of that accident, a substantial research program on severe accident phenomenology was planned and initiated with international sponsorship *[Ref. 4-4]*. This program has been the subject of many reviews and comments and included both experimental and analytical studies. It was also recommended in the various TMI investigation reports *[Ref. 4-5]* that PRA techniques be used to complement the traditional non-probabilistic methods of analyzing nuclear plant safety.

A large number of nuclear power plants have been or are being analyzed using probabilistic techniques throughout the world. Individual plant examinations (IPEs) are being or have been performed on all U.S. plants. At the present time, most nuclear power plants have been or are being analyzed to identify potential vulnerabilities and to determine the frequency of severe accidents. Important insights are being gained relative to the actions that might be taken to maintain or improve the plant safety envelope while providing increased flexibility to the plant operator.

In 1984, a study was performed by the NRC to evaluate the state of the art in risk analysis techniques, and a summary of PRA perspectives was published (NUREG-1050 *[Ref. 4-6]*). Before commenting on the proper usage of PRA analyses at present, the general conclusions of that document relative to the current state of the art,

recognizing both the strengths and weaknesses in the technology at present, needs to be revisited.

In the area of systems modeling, much of the basic methodology remains unchanged from that of the Reactor Safety Study. However, there is now a wealth of experience in applying these methods, and improved computer codes now permit the efficient handling of the more complex models required to analyze the effects of fires and external events such as earthquakes. Much, if not all, of the analysis of internal events can now be performed on personal computers, substantially reducing the cost and improving the efficiency of studies performed today. Techniques are available to calculate importance measures of plant systems and components from a variety of viewpoints, in a form amenable for use in determining the relative importance of systems and components to plant safety. The decision of the detail to which systems are modeled, however, is generally left to the judgment of the analyst, usually based on a perception of what may be important relative to other components or subsystems. Little guidance is available in the literature in this regard. Thus, before the results can be used in a regulatory application, the boundary conditions and assumptions used in the analysis must be examined to ensure they are appropriate to the specific usage envisioned.

Considerable data have been acquired on initiating event frequencies and component reliability, although this data may vary somewhat from plant to plant. Thus, while a comprehensive plant-specific data analysis is within the current capabilities, it sometimes is not performed because of the costs and resource allocations required. Thus, before a current probabilistic analysis is relied upon to support plant-specific regulatory initiatives, the degree to which the PRA analysis is also plant-specific may need to be ascertained. As discussed in the sections that follow, generic data may well suffice when using the PRA as a coarse screening device to separate the important from the unimportant, but plant-specific data may be needed for more complex usages.

Detailed methods have been developed for evaluating the significance of dependent failures, which address not only the quantitative aspects of the analysis but, more importantly, the qualitative knowledge gained that can help prevent their occurrence. At the present time, the lack of readily accessible root cause data on dependent failures from operating and maintenance logs is the more limiting factor, rather than the methods for analyzing the data. (The raw data is generally available to the plant owner/operator, but in many cases it may not be in readily usable form to the PRA analyst or to the regulator.) Guidance on acceptable ways of analyzing the raw data for dependent failures has been developed jointly by Electric Power Research Institute (EPRI) and NRC.

In contrast, methods for evaluating the reliability of solid-state control and protection devices are not yet available for routine application, particularly with respect to the adequacy of the software associated with the solid-state device. Information is available

from the aerospace and defense industries in this regard and this information, when coupled with research efforts currently under way, should do much to improve the situation. Therefore, at the present time, when software-driven solid state devices are analyzed, quantitative results should be viewed with considerable caution and care should be given to examining the adequacy of the methods employed.

In the area of human interactions, improved methods are available and additional data have been acquired that permit a more detailed analysis of the likelihood of failing to follow procedures for a number of situations. The state of the art is still relatively weak in the ability to address cognitive and comprehension errors, or to consider the pervasive effect of a poor safety attitude at a plant. Substantial work is under way in these areas in many countries, and some improvements are expected in the future. However, at the present time, the use of PRA information in a regulatory framework will be enhanced if such applications are structured such that they minimize the influence of the uncertainties inherent in the human error probabilities. Even when human errors are treated in a relative manner, however, care must be taken to ensure that dependencies and boundary condition changes are properly considered.

In the area of consequence analysis, models have been substantially improved, and many sensitivity analyses are now available. However, comprehensive uncertainty analyses of the models are only now being performed. As identified above, a detailed and comprehensive research program is directed to those elements necessary to reach regulatory closure on severe accident issues. The most recent assessment of the uncertainties in these portions of the analyses was contained in the NRC-sponsored NUREG-1150, "Severe Accident Risks, An Assessment for Five U.S. Nuclear Power Plants" *[Ref. 4-7]*, which considered uncertainties associated with both input parameters and modeling. While, in general, the central estimates (means, medians) of the distributions associated with the releases of the various radionuclides to the environment in NUREG-1150 are lower in magnitude than those predicted in earlier studies such as WASH-1400, the uncertainty range remains large.

The ability to perform comprehensive uncertainty analyses, including consideration of both modeling uncertainties as well as those associated with input parameters, has improved greatly. The most detailed study of this type is included in NUREG-1150. However, that method relies heavily on expert elicitation and is extremely resource intensive and time consuming. Improved, more efficient methods are needed if such analyses are to be routinely used in regulatory decisionmaking. Alternately, means should be devised to use risk insights in a manner consistent with a somewhat limited overall assessment of uncertainties.

Thus, to the extent possible, the use of probabilistic information in developing performance-based criteria may be more appropriate and robust when applied to the

potential for severe core damage or to system availability under given conditions rather than to public risk. The inherent uncertainties in assessments of individual or societal risk make analyses of such parameters more amenable to comparisons with goals rather than determination of compliance with criteria.

The ability to analyze the effect of fires, floods, and other external events has improved substantially. Major limitations still exist relative to the ability to estimate recurrence frequency for very rare catastrophic events (such as great earthquakes) and it does not appear that the uncertainties associated with such estimations will be narrowed substantially in the near future. Similarly, some of the subtle effects associated with certain other external events will require more study before they can be quantified without considerable uncertainty (e.g., effects of smoke and soot during fires). These factors may limit the use of probabilistic-type approaches in these areas of regulation unless consideration is given to the impact of the uncertainties involved on the regulatory decisionmaking process.

Given these strengths and weaknesses, how can probabilistic results be used? A comprehensive discussion appears in "Probabilistic Safety Assessment in Nuclear Power Plant Management," edited by N. J. Holloway and sponsored and published by Principal Working Group 5 (Risk Assessment), Organization for Economic Cooperation and Development/Nuclear Energy Agency *[Ref. 4-8]*. It evaluates the value of PRA as an increasingly valuable complement to general engineering analysis for assessing and managing the safety-related operations of a nuclear power plant. The report draws the following conclusions:

- The application of PRA provides plant management with a general systems engineering tool that generates insights not readily available from the traditional deterministic safety and licensing analyses. While some of these insights derive from probabilistic evaluation, the majority do not, but simply arise from the systematic yet unprejudiced nature of the PRA procedures. Some of the most important new insights have been derived from the integrated model of plant system behavior and operator actions that PRA can create.

- The existence of a PRA capability within a plant operator's organization provides for a logical framework of regulatory discussion and negotiation to be created. Furthermore, this framework is plant-specific and can thus be used for plant-specific evaluation and more logical resolution of generic safety issues.

- The benefits derived by plant operators are generally greatest when there is a full commitment to development and maintenance of an internal PRA capability, with minimal dependence on outside experts except for an initial technology transfer phase. Although such commitments are quite expensive, those who have

undertaken them are generally of the opinion that the benefits more than compensate.

- The application of PRA to an existing plant has always resulted in the identification of effective ways of achieving plant safety, and has thus contributed to the overall effectiveness of plant operation.

Therefore, the report comes to the conclusion that the implementation of PRA as an aid to nuclear power plant safety management is directly beneficial to those implementing it in support of their plant designs or operations and to all those concerned with ensuring nuclear plant safety. It is in this vein that the NRC has initiated the IPE process, in which each licensee is requested to conduct plant-specific risk-based searches for vulnerabilities.

Probabilistic analysis techniques also are of interest to the regulator in a variety of ways, and most of the comments addressing utility use in the OECD/NEA report referenced above are applicable in this venue as well. These techniques provide a unique perspective that permits an independent consideration of the body of regulatory requirements to ensure that potentially risk-significant factors are properly considered and that regulatory resources are not needlessly expended on unimportant matters by either the regulated or the regulator. They can be used to identify those systems, trains, and components that are important in maintaining a low likelihood of severe core damage, and, conversely, can also identify those items that have little influence on the likelihood of an accident. However, such analyses must be done with a clear appreciation for the strengths and weaknesses discussed above.

The results of PRA studies, including detailed uncertainty analyses, provide information useful in prioritizing the expenditure of resources for plant evaluations and future safety research. The models generated in a probabilistic study are useful in evaluating the significance of both plant-specific and generic issues. They are also useful when developing strategies to react to or manage a severe accident as it occurs. As before, this must be done with an appreciation of the boundary conditions and assumptions used in the original analyses. While items found risk-significant might warrant further analysis or regulatory attention, this will depend on the specifics of the situation, the degree to which existing regulatory instruments are met, and the potential for approaching or exceeding any safety goals that might be established. Similarly, items cannot be dismissed on the basis of low risk until it is clear the analysis is sufficiently robust in the area of interest and that it adequately supports the decision.

In summary, the strongest insights gained from a probabilistic analysis are derived from (1) the integrated and comprehensive examination that analyses of these types entail, (2) the attention devoted to interactions between systems, the operating staff, and the plant

systems, and (3) the structured examination of operating experience. In general, the insights and importance rankings developed from the analysis of a system, or from analyses of groups of systems, to assess the frequency of severe core damage are more robust than those that require an evaluation of overall risk; this determination is because the analyses in the former case are simpler and the uncertainties involved are not as broad as in the latter situation. The weakest insights are those that are derived primarily from the quantitative rankings alone, without considering the meaning of the results in an engineering context. While the quantitative results are important, they should be considered as most useful for a screening of the results to identify important accident sequences and plant features at the present time and to give indication of areas with relatively little or relatively high importance in a probabilistic context.

Probabilistic analysis presents an additional tool, an additional source of information that can be used to focus regulatory decisionmaking in many areas, identifying features most important to plant safety. Used properly, with recognition of the limitations and proper attention to the scope, boundary conditions, and assumptions of the analysis, it can be used to exploit the flexibility presently existing within the regulatory environment to improve plant safety while reducing undue regulatory burden. It can also be used to suggest areas where performance-based regulatory practices can be employed in the future. Techniques are now being developed and employed to improve plant configuration control and to optimize the required plant response to equipment outages or mode changes.

Recognizing these strengths and weaknesses, a set of general guidelines have been developed regarding the constraints that are needed on the boundary conditions and assumptions of a probabilistic analysis used to support various types of regulatory initiatives. The qualifications are discussed in detail in Section 4.2. A proposed approach to PRA application in the regulatory process is provided in Section 4.3. Detailed discussions of these applications are presented in Sections 4.4 through 4.6. How PRA can be used to provide a relative ranking and importance of rules and regulations is provided in Section 4.7. Perspectives from non-NRC organizations regarding the use of PRA is provided in Section 4.8. A summary of NRC programs, particularly how they can support the recommended applications, is provided in Section 4.9. Conclusions are provided in Section 4-10. A list of acronyms, abbreviations, and references is provided in Section 4.11.

4.2 PRA SUMMARY

In using a PRA-type analysis to provide additional flexibility in the regulations and their implementation, it is necessary to understand the purpose, boundary conditions, and type of results associated with this type of analysis.

A PRA of a nuclear power plant is an analytical process that quantifies the potential danger of the design, operation, and maintenance of the plant to the health and safety of the public. The danger or hazard that has been identified as posing the greatest risk to the public is the consequences associated with possible core melt accidents. Therefore, in the calculation of the risk, those events that could potentially lead to a core melt and a release of fission products are identified and their probability quantified.

A PRA can be performed to different levels. The first phase of a PRA, called a Level 1 PRA, involves the calculation of the potential core damage frequency. The second phase, a Level 2 PRA, calculates the frequency of the core damage progressing to a core melt and the release of fission products to the environment. The last phase, a Level 3 PRA, calculates the consequences of the fission product releases to the environment.

Each PRA level consists of numerous elements of which several are critical when considering various applications of the PRA. That is, the attributes of each element in the PRA will dictate the ability of the PRA to be used beyond its original purpose (for example, the original purpose might be an IPE). Only those attributes associated with a Level 1 PRA are discussed since the applications under consideration generally involve the Level 1 portion of the PRA.

In this report, the various potential applications of PRA in providing additional flexibility in the implementation of the regulations will focus on those aspects that address core damage prevention and not mitigation of the effects of core damage. Ultimately, some expansion will be needed to consider engineered safety features with mitigative functions. This expansion will be done in conjunction with any pilot programs in this regard proposed by the industry.

One objective of the Regulatory Review Group (hereinafter referred to as the Review Group) is to determine how an integral analysis can be used to provide more flexibility in the regulations and the implementation of the regulations. Therefore, in providing a general set of principles or guidelines, the various methods that are generally used by licensees--level of detail, scope, and assumptions--needs to be understood. The following discussion is written from the perspective of the content of licensees' PRAs.

4.2.1 PRA Elements

A Level 1 PRA is comprised of three essential elements as follows:

- The delineation of those events that, if not prevented, could result in a core damage state and the potential release of fission products.
- The development of the models representing the core damage events.
- The quantification of the models in the estimation of the core damage frequency.

The first element of a Level 1 PRA delineates those events that, if not prevented, could result in a core damage state and the potential release of radionuclide fission products. This process, generally referred to as the Accident Sequence Analysis, is typically divided into two parts: identification of the initiating events and development of the potential core damage accident sequences associated with the initiating events.

The initiating events generally modeled in current PRAs include loss-of-coolant accidents (LOCAs), general balance-of-plant (BOP) transients, and plant support system non-BOP transients. Event trees are developed for each of these initiators that delineate the core damage accident sequences that could potentially occur. The accident sequences are comprised of those sequences of events (i.e., success and failure of the functions and systems) that, if they occur, will result in core damage. The initiating events and accident sequences, therefore, identify the various systems for which a mathematical (i.e., Boolean algebra) model is required.

The Boolean models are developed in the second element of a Level 1 PRA. These models depict the different failure paths associated with each system in determining the system's unavailability and unreliability.

Two different types of fault trees are generally used to model a system's potential performance. The *"large fault tree"* concept involves developing a single fault tree that models each of the different failure configurations of a system. House events are modeled in the fault trees that are used activate each configuration. The *"support state fault tree"* concept involves developing a separate fault tree for each different failure configuration (or support). Each support state fault tree is, therefore, comprised of independent events.

The third element of a Level 1 PRA estimates the plant's core damage frequency. This estimation is performed by first quantifying the failure probabilities and unavailabilities of the various structures, systems, and components (SSCs), quantifying the initiating event frequencies, and quantifying the human error probabilities (HEPs) associated with the

various operator actions. The frequency for each event tree core damage accident sequence is then quantified by integrating the failure probabilities (i.e., event data) of the SSCs and the HEPs with the initiating event frequencies into the boolean models. These frequencies are summed to yield the overall core damage frequency of the plant. This value represents the average annual core damage frequency associated with the design, operation, and maintenance of the analyzed plant.

4.2.2 PRA Scope and Level of Detail

PRAs examine the consequences of events that involve a reactor scram[1] or forced shutdown with the need for subsequent core heat removal. These events can occur at different reactor operating states from full to low power and various shutdown modes.

The core damage frequency is estimated based on either internal events or external events or both. Internal events only consider equipment failure internal to the component when examining the potential failure of SSCs. Internal flooding is, however, considered part of the internal events analysis for the purpose of this discussion. External event analysis involves the examination of the effects of fire, earthquakes, high winds, flooding, etc.

Initiating Event Analysis —

The initiating events are generally incorporated in the current PRA models by a single event that represents the average annual frequency of the event. A Boolean model explicitly depicting the various systems and components contributing to the initiator occurrence is generally not developed and incorporated into the PRA model.

The initiating events generally modeled in current PRAs include LOCAs, general plant transients associated with BOP systems such as loss of feedwater, and support system transients associated with non-BOP systems such as loss of a vital AC bus.

Event Tree (Accident Sequence) Analysis —

The accident sequences are generally depicted at the functional or systemic level of detail. The selected functions or systems are dependent on the scope of the success criteria analysis that determines those systems, or combination of systems, if functioning will maintain the core in a safe condition (i.e., prevent the occurrence of a core damage state). Generally, in most PRAs, the core is assumed to be in a safe condition when the consequences of the radionuclide releases from the damaged fuel would be negligible. Typically, this state is assumed to be prevented if reactor water level is not allowed to

---

[1]The resulting reactor scram is an "immediate" occurrence. That is, inoperability of a system that requires the plant to go to shutdown conditions after, for example, 8 hours, would not be considered an initiator.

decrease below 2 feet above the bottom of the active fuel for BWRs and below the top of the active fuel for PWRs.[2]

The requirements of this defined core damage state is determined from detailed engineering analysis of both core and plant behavior under different accident conditions (e.g., large LOCA versus normal plant transient). The results are subject to, therefore, the codes, modeling assumptions, etc., that are used.

As noted, the defined success criteria and extent of supporting engineering analysis determines those plant-specific functions and systems that are identified as capable of preventing a core damage state. There are, however, numerous plant systems that either have no relationship to the needed function or do not meet the necessary criteria. These systems are not evaluated (e.g., modeled) in the PRA. An example of the number of plant systems as compared to those modeled in a PRA is shown in Table 4.2-1. It is easily seen from this table that a PRA, while successfully integrating the impact of design, operational, and maintenance faults on the plant from a core damage prevention perspective, is limited to a narrow set of systems.

Systems Analysis —

The fault trees constructed for the various systems can be developed to different levels of resolution as follows:

- *Component Resolution* — The individual components comprising the function or system and the possible failure modes of the components are explicitly depicted in the fault tree model as unique basic events. It should be noted that not every system component and failure mode is modeled. Generally, only those components whose failure mode results in the loss of system function with a relatively significant probability (e.g., $\geq$ 1E-6) are modeled.

  A component in a PRA is generally the major piece of equipment that is essential to the function of the system such as pumps, valves, heat exchangers, diesel generators, etc. Parts that are essential to the component's function (e.g., valve disk) are not explicitly modeled as unique basic events but are included within the boundary of the component (e.g., valve). Only those failure modes that prevent system function are usually modeled.

---

[2]The level is much higher for PWRs since steam cooling is not inherently part of its design.

Table 4.2-1
Example of Plant Systems Versus PRA Modeled Systems

SYSTEMS	PRA	SYSTEMS	PRA
Nuclear Boiler System	▽	Auxiliary Steam System	▽
Recirculation System	▽	Condensate System	◇
CRD Hydraulic System	◇	Feedwater System	◇
Redundant Reactivity Control	▽	Condensate Cleanup System	▽
Feedwater Control	▽	Heater, Vents Drains System	▽
Standby Liquid Control System	★	Turbine Systems	□
Neutron Monitoring System	▽	Generator Systems	□
Remote Shutdown System	▽	Condenser Systems	□
Reactor Protection System	□	Off Gas Systems	▽
Plant Annunciator System	▽	Circulating Water System	□
Fire Protection System	◇	Chlorination System	▽
Meteorological Monitoring	▽	Water Storage and Transfer	▽
Seismic-Instrumentation System	▽	Emergency Service Water	★
Vibration Monitoring System	▽	Component Cooling Water	△
Loose Parts Monitoring System	▽	Turbine Bldg Cooling Water	△
Transient Test System	▽	Normal Service Water	△
Drywell Monitoring System	▽	Plant Air System	◇
Residual Heat Removal System	★	Instrument Air System	★
Low Pressure Core Spray	★	Plant Chilled Water System	△
High Pressure Coolant Injection	★	Drywell Chilled Water	△
Leak Detection System	▽	Diesel Generator Systems	★
MSIV Leakage Control System	▽	Transformer Systems	▽
Feedwater Leakage Control	▽	Switchgear Systems	▽
RCIC System	★	Auxiliary Bldg Vent System	△
Liquid Radwaste System	▽	Radwater Bldg Vent System	▽
Reactor Water Clean-up System	△	Turbine Bldg Vent System	△
125V & 24V Batteries	★	Drywell Vent System	★
125V DC Power Supplies	□	Wetwell Vent System	★
125V Battery Chargers	★	Emer Swgr and Batt Rm Vent	△
Static Inverters	★	Other Bldg Vent Systems	△
Cont./Drywell All Monitoring	▽	Control Bldg HVAC System	△
Drywell Cooling System	△	Control Room HVAC System	△
Main and Reheat Steam System	◇	Load Seq and Shedding	△

★ Component level of resolution model
◇ Failure mode level of resolution model
□ Event level of resolution model
△ Not explicitly modeled
▽ Not evaluated

- *Failure Mode (Train) Resolution* — The individual components are not explicitly depicted in the fault tree model as unique basic events, only the failure modes of each train are modeled as unique basic events (e.g., train hardware fault, train out for maintenance, loss of power).

- *Event (System) Resolution* — The function or system is represented by a single event; that is, a Boolean model explicitly depicting the components and the failure modes as unique basic events is not constructed in computing the system failure probability. This level of resolution can be referred to as a "black box" model.

Data Analysis —

The data analysis basically involves the quantification of the different failure mode probabilities associated with the SSCs modeled in the system fault trees. The failure modes considered in current PRAs generally include the following:

- Hardware faults — This failure mode examines the potential for demand and time-related type failures associated with random hardware faults caused by such items as crud buildup on valve disk.

- Test and maintenance faults — This failure mode examines the potential for a component, train, or system to be unavailable when demanded because it is out-of-service for a test or maintenance activity.

- Common cause faults — This failure mode examines the potential for several components to dependently fail from the same specific cause such as replacing the same part in several components where each replacement part is defective.

The data analysis also involves the quantification of initiating event frequencies.

The identified events and the defined failure modes dictate what plant information is required to quantify the failure rates and unavailabilities and initiating event frequencies. The estimation of the probabilities and frequencies is dependent on the supporting plant documentation that provides the necessary information on plant history. If adequate plant documentation exists, then plant-specific equipment failure rates, unavailabilities, and initiating event frequencies are computed; however, if inadequate plant documentation exists, "generic"[3] data must be used, which places a limitation on the PRA application.

---

[3]Generic data are based on compilation of data of the operating history of components taken from the nuclear industry.

The period of time of the plant's history that is used to compute equipment failure rates, unavailabilities, and initiating event frequencies must be considered. A plant's historical performance changes over time; design, operational, and maintenance changes are occurring, which affect the reliability and unavailability of systems and components. It is important that the data reflect, as much as possible, the current performance of the plant.

Human Reliability Analysis (HRA) —

The estimation of event probabilities also involves the quantification of human performance events. This task is very diversified, and standardization among PRAs does not exist. This task, however, has the ability to change the dominant accident sequences; that is, change the results of the PRA. The HRA, therefore, not only impacts the estimated core damage frequency but what are identified as the most likely contributors to realizing a core damage state.

The human events include those operator actions conducted during normal plant operation that result in inoperable equipment without causing an initiating event (generally referred to as pre-initiator human actions). Also evaluated are those operator activities that are required to achieve a safe plant shutdown (generally referred to as post-initiator human actions). Post-initiator human actions include response type actions and recovery type actions.

Response-type actions are those human actions performed in response to the first level directive of the EOPs. For example, suppose the EOP directive instructs the operator to determine reactor water level status, and another directive instructs the operator to maintain reactor water level with system x. These actions — reading instrumentation to determine level and actuating system x to maintain level — are response-type actions.

Recovery-type actions include those performed to recover a specific failure or fault. For example, suppose system x failed to function and the operator attempts to recover it. This action — diagnosing the failure and then deciding on a course of action to "recover" the failed system — is a recovery-type action.

Quantification —

Using the event data and HEPs, the quantification of the core damage frequency is performed by integrating the initiating event models[4] with the system models as depicted by the event trees. This computation is typically performed on a sequence basis, with the

---

[4]These models, as mentioned previously, are generally a single event.

core damage frequency equal to the Boolean summation of the core damage frequencies of the individual sequences.

The core damage frequency is generally based on the summation of only the ***dominant*** accident sequences, and not every defined accident sequence. Those accident sequences whose calculated core damage frequency is typically less than 1E-8 may be truncated; they are not integrated into the overall PRA model. If the PRA contains quantified conclusions, i.e., importance measures, these conclusions are generally based on the dominant accident sequences alone.

4.2.3 PRA Boundary Conditions

In reviewing the scope and level of detail of a Level 1 PRA, certain boundary conditions can be identified that have the potential to impact the application of a PRA. These boundary conditions need to be addressed when considering using a PRA in the regulatory process.

The boundary conditions include the following:

- *Scope* — The PRA must involve a Level 1 analysis and must address at least internal events (including internal flooding).

- *Structure, System, and Components* — The application of the PRA is limited to those SSCs that are part of the PRA. If the SSCs are not modeled in the PRA, it does not mean they are unimportant to core damage prevention, but that, from a probabilistic perspective, they do not contribute significantly to the core damage frequency. Therefore, for SSCs not modeled (e.g., evaluated) in a PRA, it is difficult to use the PRA for insights relative to the impact of potential changes associated these SSCs, if these SSCs are not considered.

- *Level of Resolution* — The usefulness of a PRA is dependent on the level of resolution of its SSCs. If a PRA is performed at a system level, the insights of the PRA are at a system level. Conversely, a component level of resolution provides insights at the component level.

- *Failure Modes* — Although a PRA may be performed to a component level, the application will be restricted to those failure modes modeled for the component. A component level of resolution does not mean that each failure mode is modeled in the PRA.

- *Data* — The degree of plant-specific data that is used in the quantification of component failure rates, unavailabilities, and initiating event frequencies provides

the degree of actual plant-specific representation. Therefore, whether generic data or plant-specific data are used will determine the extent of the use of the PRA in the regulatory process.

- *HRA* — The incorporation of human activities into the PRA model has the ability to determine the dominant accident sequences and the dominant contributors to core damage. Insights from a PRA can, therefore, be misleading dependent on the type of human activities that were modeled. There are considerable uncertainties in the current ability to model human actions, and different assumptions can lead to significant changes in results.

- *Truncation* — In quantifying the core damage frequency, truncation of low probability events and sequences is generally performed. Although this truncation is normally preformed such that ~95 percent of the core damage frequency remains after truncation, the insights (e.g., importance measures, sensitivities) do not generally include the impact on the truncated events and sequences.

These boundary conditions are discussed in more detail for the individual applications in Sections 4.3 through 4.6.

4.2.4 PRA Results

The form of the results will dictate, in a sense, the usefulness of the PRA. Besides the calculated core damage frequency, there are numerous other types of results that are quantified in a PRA. The most meaningful, perhaps, when considering the use of PRA in the regulatory process are the importance measures. These measures show different types of insights to the core damage frequency if changes regarding the availability and reliability were made to a SSC.

The importance measures generally seen in PRAs include one or all of the following:

- ***Reduction Importance Measure*** — provides a ranking of the events (e.g., components) by those most crucial for safety improvement. The importance value for each event is the potential reduction in the core damage frequency if the event's (e.g., component's) probability was quantified as 0.0, or, for example, the component was assumed to be perfectly reliable. This measure, therefore, indicates how much the core damage frequency can be improved (i.e., reduced) if it can be assured that a SSC will function as required when demanded.

- ***Increase Importance Measure*** — provides a ranking of the events (e.g., components) by those most crucial to maintaining safety at the current estimated level. The importance value for each event is the potential increase to the core

damage frequency if the event's probability was quantified as 1.0, or for example the component was assumed to be always unavailable. This measure, therefore, indicates how much the core damage frequency can be hurt (i.e., increased) if failure of the SSC was certain.

- ***Fussell-Vesely Importance Measure*** — provides a ranking of the events (e.g., components) by contribution to the core damage frequency by computing their potential to change the core damage frequency. The importance value for each event is the summation of core damage frequencies of the cut sets[5] containing the event under consideration divided by the total core damage frequency.

These importance measures are significant because they can indicate the relative safety importance of an issue without requiring further manipulation of the PRA model. That is, safety insights can be gained from these measures. For example, the Reduction Importance Measure shows both those events (e.g., components) that are most likely to cause core damage and those events that have little-to-no impact on core damage. The Increase Importance Measure, on the other hand, indicates those events (e.g., components) that are critical to maintaining the current level of safety. That is, if their reliability and availability were to decrease, they would have the most significant impact on the core damage frequency. These measures can then be used to define generic categories to provide safety insights in the regulatory process.

[5]The minimum, unique combination of events that will result in the defined end state, e.g., core damage.

4.3 PRA APPLICATION DEFINITION

4.3.1 PRA-Based Reactor Regulation

Risk (or probabilistic risk) can be defined as the frequency of the consequences associated with an identified hazard that poses a potential danger to the health and safety of the public. Risk-based regulation involves the use of PRA of these identified hazards in the development and implementation of the regulations. PRAs of current facilities, however, address the frequency of the consequences of radionuclide releases. In this context, risk-based regulation is then defined as risk-based *reactor* regulation.

The staff has defined risk-based regulation as the use of PRA insights to focus licensee and regulatory attention on design and operational issues commensurate with their impact on risk to the public *[Ref. 4-9]*.

As used in this report, risk-based regulation refers to the panoply of possible current and future uses of probabilistic analyses to support regulatory actions. These applications include present uses such as generic issue prioritization and resolution, backfit decisions under 10 CFR 50.109, regulatory analysis in support of rulemaking, prioritization of licensee activities in response to regulatory requests, and justifications for continued operation. Other possible uses (described below) are included such as development of graded approaches to the maintenance rule and to quality assurance requirements, optimization of Technical Specification requirements for allowed outage times and surveillance test intervals, Technical Specification schemes that are based on risk-based configuration control, and ultimately, a set of regulatory requirements almost totally dependent on the risk analysis of the facility.

4.3.2 PRA Utilization in Regulatory Process

The Review Group charter regarding the assessment of risk technology directs the group to *"examine how an integral analysis (PRA) can be used to provide more flexibility in the regulctions and the implementation of the regulations. Determine what types of general ground rules or restrictions would be necessary to confidently sustain broad PRA usage as an accepted, credible tool for optimizing operations while maintaining the current level of safety. This will include addressing uncertainties and limitations of analytical tools and restrictions that should be placed on their use, identifying ways of accommodating limitations and specify conditions under which NRC could support broad application of risk technology to optimize licensee flexibility." [Ref. 4-10]*

In response to the above charter, the use of PRA to provide additional flexibility in the implementation of the regulations requires that general sets of PRA principles be defined. These principles need to define a set of general rules or guidelines that will establish

major boundary conditions and assumptions; however, it needs to be recognized that this set will change as one changes application. It will be most useful, therefore, to construct these principles in terms of requirements as the application progresses from the generic to the plant specific.

A possible structure from the more generic application to the plant specific is illustrated below in Figure 4.3-1.

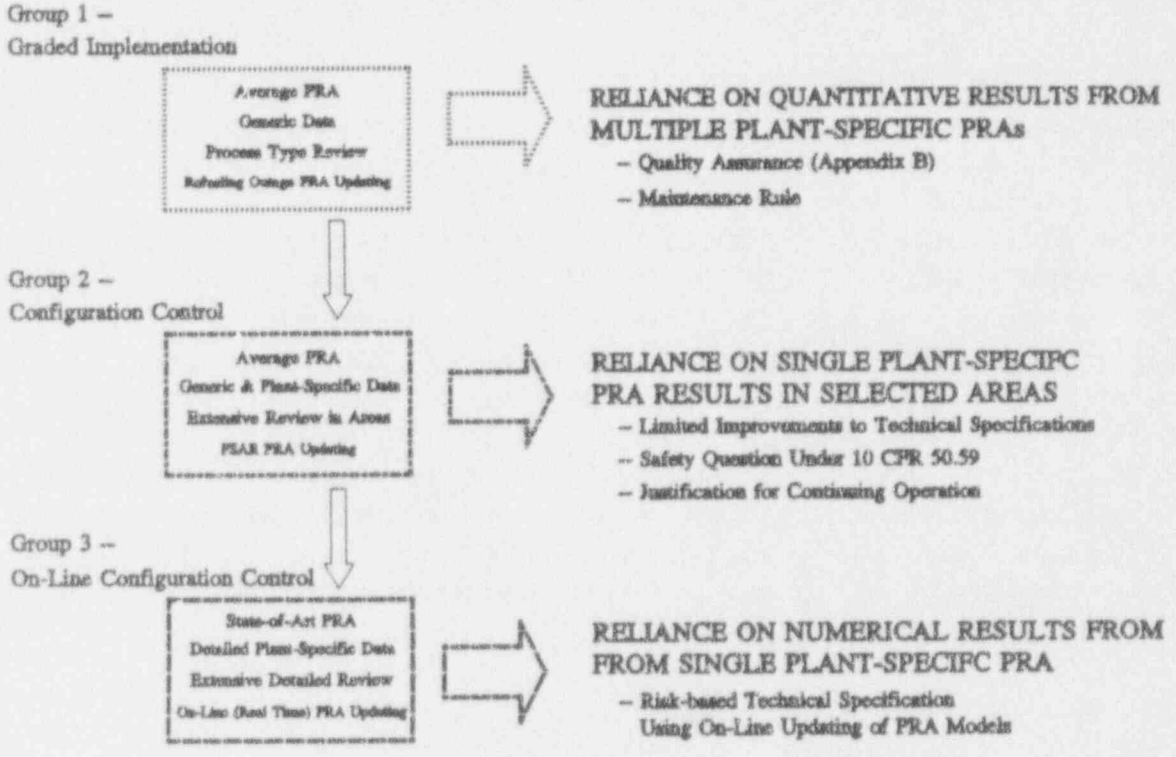

Figure 4.3-1. PRA Applications.

The first group would involve applications where great precision in the PRA is not required to identify general categories of plant SSCs in terms of their safety significance. Conversely, the regulator does not require a high degree of precision in the PRA, and therefore, it would not be necessary to conduct a thorough *de novo* review of the PRA.

For this type of utilization, generic failure rate data would probably suffice, supplemented with plant-specific data only where a qualitative examination of operating experience might indicate some anomalous behavior relative to the overall generic data base for such

components. Because the real purpose underlying Group 1 type uses is the separation of the important from the unimportant, and, only secondarily, the development of rank ordered groups of the "important," frequent updates of the PRA would not be required. Rather, they would need to be done only when there was a major redesign of one of the plant systems or a major modification in the basic operational principles.

For the second group, emphasis would be placed on those areas of the PRA that would be used directly in developing a probabilistic-based strategy to implement or modify a given regulatory practice. In general, these applications will fall into two general categories. The first would emphasize relative improvements in risk and would provide a measure of effectiveness in terms of the ratio of the calculated risk measure before the regulatory action is taken to that which would obtain after implementation. Simplistically, many areas of uncertainty would "cancel" and, thus, emphasis in both analysis and review could be sharply focused. This does ***not*** imply that it would not be necessary to ascertain that the elements in question did not affect other parts of the analyses.

In the second instance, the PRA would rely on coarse models of the plant, perhaps at the train level. In planning configuration control, for example, it probably is unnecessary to develop trees below the train level, as long as the interactions with supporting systems are understood and modeled appropriately. Again, the analysis and the associated review would have to be focused on the specific application envisioned, but the requirement for assured confidence in the results would be limited rather than global. These applications would require a comprehensive analysis of in-plant data in the selected areas under analysis, and updates of the PRA models would be desired each refueling outage.

The third group would involve applications that are within the state of the art in theory but the application would be difficult for both the industry and the regulator. A PRA of high calibre would be required. As an integral part of the regulatory structure, the PRA would require a comprehensive review by the staff. Perhaps of most significance, a comprehensive analysis of plant data would be required, since many of the methods currently available to optimize regulatory practices have imbedded assumptions regarding the characteristics of the failure data of the various components.. Updating of the system status would be needed on a frequent basis, perhaps even in real time.

The inherent difficulties in progressing beyond Group 1 type applications suggest that pilot programs be organized between the NRC and the regulated industry to test the viability of the more complex applications before they are offered to the industry as a whole.

A discussion of an application from each group is provided in the following sections. These discussions focus on the general sets of rules for the PRA relative to its application.

4.4 PRA APPLICATION FOR GRADED IMPLEMENTATION (Group 1)

The use of a PRA to support a graded implementation of the regulation requires that PRA criteria associated with the application be defined. These criteria need to ensure that the PRA application does not negatively affect the current level of safety associated with the design, operation, and maintenance of the plant. Therefore, criteria determining the definition of importance, criteria used to identify the important SSCs, and criteria establishing the basic conditions of the PRA in identifying importance are each necessary.

4.4.1 Importance Definition

The major element of the graded application is identifying those systems, trains, and components that are important and then determining their relative importance. It is, therefore, necessary to define what is meant by importance and define the criteria for relative importance. These definitions are both based on insights from PRA.

Importance is initially defined as those SSCs that are necessary to maintain the current level of safety that can be characterized by core damage prevention. Those SSCs necessary to core damage prevention are, therefore, defined as important; that is, those SSCs with the greatest potential to impact the core damage frequency are identified as important.

The relative importance of the SSCs necessary to core damage prevention can be determined from PRAs. The Increase Importance Measure is an excellent measure to use in defining different importance categories of SSCs. It provides a ranking of the events (i.e., SSCs) that are critical in maintaining the core damage frequency at its current estimation (i.e., maintaining safety at the current estimated level).[6] Therefore, those SSCs whose reliability and availability need to be closely maintained are identified by this measure. For example, in a graded quality assurance (QA) application, controls need to be assured for the relatively important SSCs so that their reliability and availability is not impacted.

Based on the Increase Importance Measure, the relative importance of SSCs to core damage prevention can be determined. The relatively important SSCs can be defined as those whose Increase Importance Measure impact on the core damage frequency is greater than or equal to a factor of 10-to-100, depending on the application, as shown by the following equation:

---

[6]This measure provides the impact on the core damage frequency if an event's failure probability is 1.0; that is, it identifies how badly the core damage frequency is impacted if the availability and reliability of an SSC is degraded to the point where failure is certain.

$$\frac{\text{Increase Importance Measure}_{ssc}}{\text{Core Damage Frequency}_{plant}} \geq 10\text{-}100$$

This definition is one suggestion for defining the relative importance. Whatever is used, the definition should be for all the applicable failure modes of the SSC that are addressed by the application and not just, necessarily, one of the basic events of the SSCs.

For example, if an SSC's estimated Increase Importance Measure is 4E-4, its unavailability impact on a core damage frequency of 1E-5 is a factor of 40. For this example, the SSC would be classified as "relatively important" to core damage prevention. If its estimated importance measure is, however, 5E-5, its unavailability impact to the core damage frequency of 1E-5 is only a factor of 4. In this case, the SSC would be classified as "relatively non-important" to core damage prevention.

4.4.2 Importance Classification

The objective of the graded application is to define different categories of rule implementation based on the relative importance of an SSC. Based on the results of PRA, the plant's SSCs of concern can be identified and classified into different importance groups. These groups are determined based on PRAs of plants of similar design. This generic grouping is applied based on the recommended criteria (see Section 4.4.4). Therefore, for each class of similar plants, relatively important and relatively non-important SSCs are identified.

Initially, similar designs could be considered one of the following:

- BWRs 1-4.
- BWRs 5&6.
- PWR Westinghouse.
- PWR CE.
- PWR B&W.

In using a graded approach for rule implementation, the plant's SSCs of concern would be ranked according to their importance to core damage based on PRA information. For example, in a graded QA implementation, only the SSCs identified as relatively important from a plant's Q list would be subject to the current implementation in meeting the QA regulatory requirements. The SSCs, however, identified as relatively non-important, would be subject to a graded implementation in meeting the QA regulatory requirements. This process is illustrated below in Figure 4.4-1.

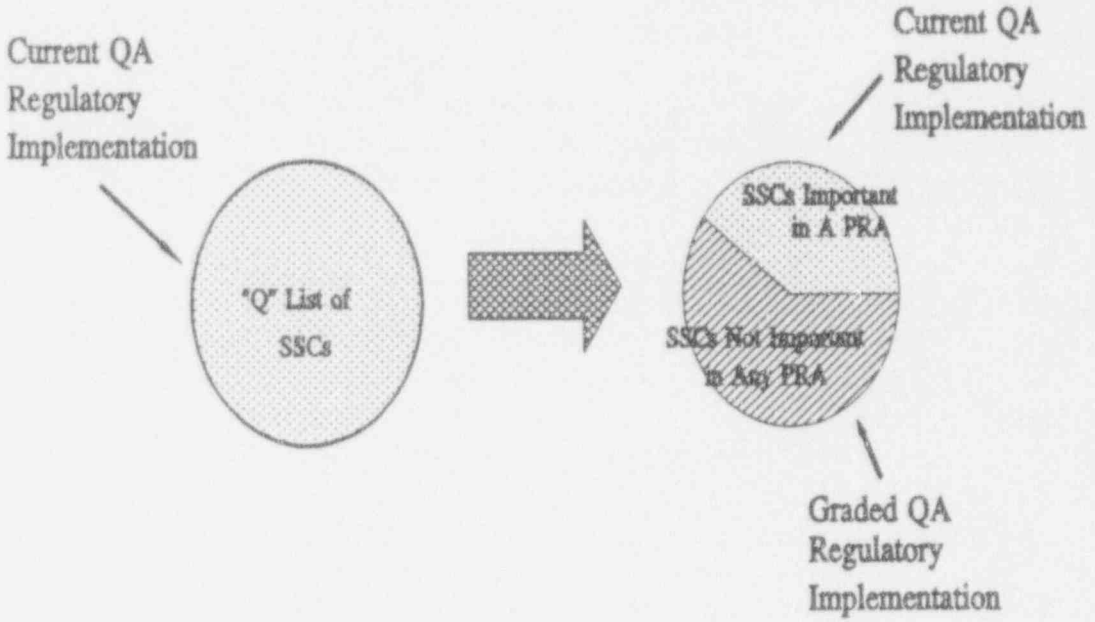

Figure 4.4-1. Generic Classification of SSCs for Graded QA.

For each class of plants, the relatively important SSCs are those SSCs that have been found to be relatively important in ***any*** of these PRAs. Therefore, for each of these SSCs, the ratio of their Increase Importance Measure to the core damage frequency is greater than or equal to a factor of 10-to-100 for at least one of the plants in that class. These SSCs, because of their relative importance to core damage prevention, would be subject to the current implementation in meeting the QA regulatory requirements.

The remaining Q list SSCs are then classified as relatively non-important since ***no*** PRA (of a similarly designed plant) identified any of these SSCs as relatively important. Although these SSCs have been determined to be probabilistically unimportant to core damage prevention, they have been identified as deterministically important to core damage prevention; therefore, removing these SSCs from the Q list is inappropriate. These SSCs would then be subject to a graded implementation of the QA regulatory requirements. This graded approach might focus on pre-operational functional testing, installation inspection, and compliance with recognized industrial procurement practices.

The initial identification of the relatively important and relatively non-important SSCs is performed based on probabilistic criteria. There are, however, SSCs that have been identified as deterministically important (i.e., identified as part of the "Q" list) but have not been modeled in the PRA. They are determined to be probabilistically unimportant; their failure probability is estimated to be negligible as compared to other SSCs. However, because of their deterministic importance and unless appropriate justification is provided, they would still be classified as relatively important to core damage prevention and would be subject to the current QA implementation requirements. An example of a component in this category would be the reactor pressure vessel, which is usually not directly included in the PRA model after truncation.

The SSCs of a plant that are not identified as part of the Q list have been determined to be deterministically unimportant. These SSCs are not subject to the current QA implementation requirements. If one of these SSCs were identified as probabilistically important, that is modeled in the PRA and determined to be relatively important, this SSC should be subject to QA requirements and subject to a graded implementation of the QA regulatory requirements in accordance with its risk importance.

A plant's SSCs of concern have now been divided into two groups of SSCs. One group of relatively important SSCs where the current regulatory implementation is maintained. The second group of relatively non-important SSCs, however, will now be subject to a graded regulatory implementation.

The initial classification of the relatively important SSCs is based on the results of PRA of plants of similar design and is a generic classification. There could, however, be a plant-specific SSC that is relatively non-important based on its plant-specific PRA. This difference could be due either to PRA reasons (e.g., boundary conditions or assumptions) or plant-specific design differences. Another classification of importance can then be defined — *plant-specific relatively non-important SSCs*. The SSCs in this class are plant-specific SSCs that are relatively non-important, but a PRA of a similarly designed plant found them to be relatively important. The difference is due to PRA considerations (e.g., different assumptions). This group of SSCs would not be subject to the current rule implementation but to a graded rule implementation. This implementation for these SSCs, however, would be more stringent than the implementation for those SSCs identified as relatively non-important. As a possible example, when considering graded QA, these components might be subjected to most elements of the present QA program, but the need to maintain the "pedigree" of the component could be eliminated. Further requirement reductions might be obtained if it could be shown that commercially available equipment of this type met the expected reliability characteristics of the PRA. If the difference is, however, due to design differences, this SSC could be classified in the generic relatively non-important group. This plant-specific process is illustrated below in Figure 4.4-2.

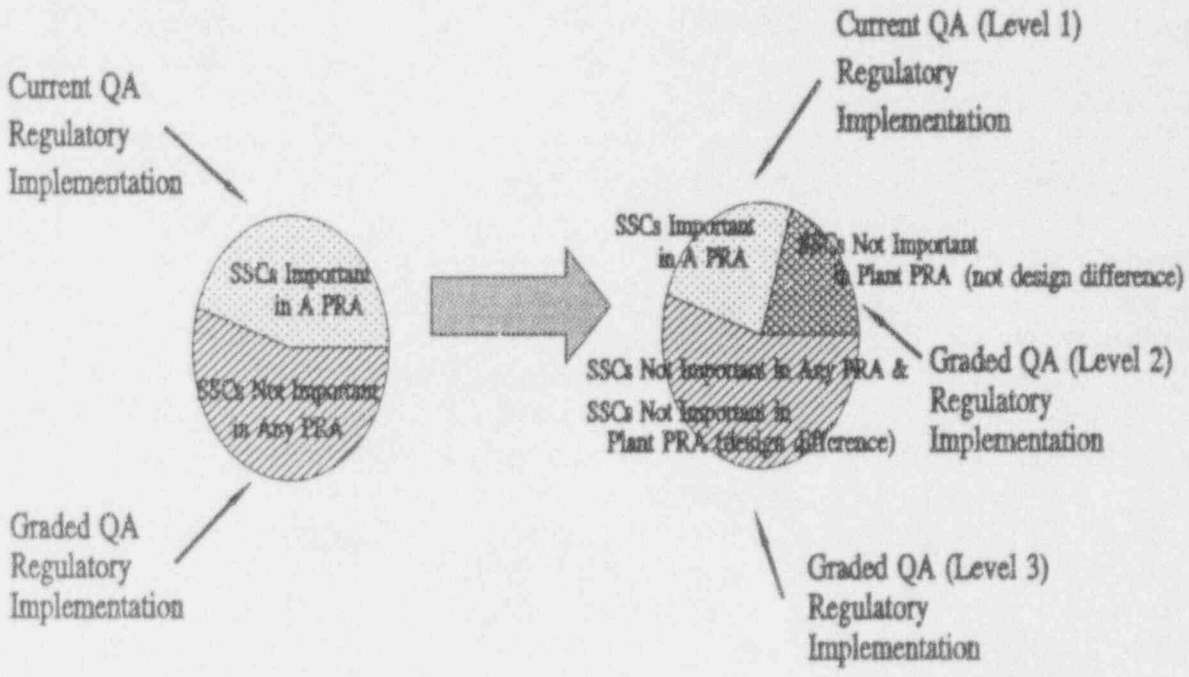

Figure 4.4-2. Plant-Specific Classification SSCs for Graded QA.

In considering a graded approach for rule implementation, it must be remembered that the PRA definition of a "component" is different from, for example, a Q list's definition. Many of the items on a Q list either are not modeled in a PRA, or if modeled are not explicitly depicted in the PRA model. These items are referred in the PRA as "parts."

In a PRA, if a component part is essential to the function (as defined by the PRA) of the component, then the part is included in the component boundary. There may be parts that are not essential for the component to perform its function even though the component has been identified as relatively important in the PRA. These parts would not be classified as relatively important and subject to the current implementation of the regulatory requirements. They would be classified as relatively non-important and subject to a graded implementation in meeting the regulatory requirements. This determination would be based on an engineering evaluation of the need for the piece part, considering the failure modes involved. For example, when considering graded QA, if an O-ring failure led to minimum leakage, but did not prevent functional performance, it

could receive reduced QA coverage. This classification is illustrated below in Figure 4.4-3.

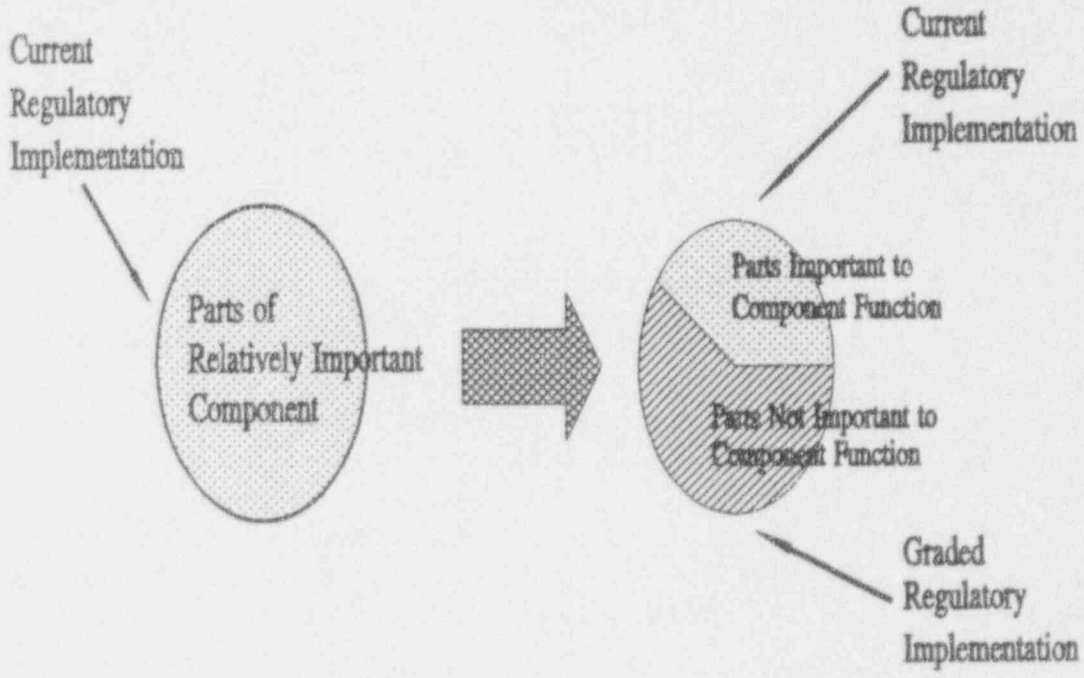

Figure 4.4-3. Classification of Component Parts.

4.4.3 Graded Implementation Requirements

Utilization of PRA for graded rule application potentially results in three levels or groups of importance of the SSCs:

- *Group A* — Those SSCs that have been found to be relatively important to core damage prevention in a PRA of plants of similar design. Also included in this group are those SSCs that have been found to be deterministically important, but not probabilistically important; and those SSCs that have been found to be probabilistically important but not deterministically important.

- *Group B* — Those SSCs that have not been found to be relatively important in the plant-specific PRA, but have been found to be relatively important to core damage

prevention in a PRA of plants of similar design. This difference is not due to design differences.

- *Group C* — Those SSCs that have not been found to be relatively important to core damage prevention in *any* PRA of plants of similar design and those SSCs not found to be relatively important in the plant-specific PRA because of to design differences.

For each of these groups, the actual implementation of the rule needs to be defined. Detailed development may require a pilot study to explore the most efficient implementation strategy.

4.4.4 PRA Criteria

In using a PRA to identify relatively important SSCs and subsequently define different categories of relatively important SSCs, the PRA must be performed to certain criteria. These criteria address those boundary conditions associated with a PRA (discussed in Section 4.2).

In addition to the criteria in Section 4.2, there are several others that must also be addressed when considering the use of PRA in the regulatory process. These criteria include the updating of the PRA and the level of review of the PRA.

In performing a PRA, the time period involved is generally 2 to 3 years. The models developed as part of the PRA reflect the design, operation and maintenance of the plant typically at the start of the PRA. As the PRA is used, the potential, therefore, exists for the PRA to be outdated and not reflect the current core damage frequency estimation (i.e., current level of safety) of the plant since the design, operation, and maintenance of the plant does change. How often the PRA needs to be updated must be addressed when considering the PRA application. These criteria can be divided into three categories as follows:

- *Outage Driven* — The PRA is updated at each plant refueling outage considering the plant design, operational, and maintenance changes.

- *PRA Driven* — The PRA is updated at the time of the plant design, operational, or maintenance change if the change has the potential to affect the PRA.

- *Real-time Driven* — The PRA is made "living" such that it continually reflects the status of the plant in real-time.

From a regulatory perspective, in considering the use of the PRA, the adequacy of the PRA for the identified use must be addressed. This determination will be based on the type and level of review that is performed by the NRC. The different levels and types of review that can be performed include the following:

- *Process* — The review primarily focuses on the methods, boundary conditions and assumptions of the PRA such that it can be determined that the SSCs important to core damage prevention are adequately addressed and identified in the PRA. Guidelines on the specific review criteria should be developed as part of any pilot study.

- *Detailed* — The review focuses on the accuracy of the core damage frequency estimation. The methods, boundary conditions, assumptions, scope, level of detail, models, and data of the PRA are reviewed. Guidelines on the specific review criteria should be developed as part of any pilot study where a detailed review is required.

PRA Criteria for Generic Importance Classification —

This categorization is basically determining relative importance of a plant's SSCs based on generic insights. Since only those SSCs that have never been shown to be relatively important in *any* PRA receive graded implementation, generic types of criteria are adequate.

An NRC review needs to have been performed of the plant-specific PRA of the licensee using the application. A review of the PRAs of the similar plants also needs to be performed. However, only a process-type review of these PRAs similar to that afforded to IPE submittals is needed for this generic application.

The PRAs need only to have addressed internal events, including internal flooding.

The classification of relatively non-important SSCs is bounded by the level of detail of the PRAs. For an SSC of a plant's Q list to potentially be considered as relatively non-important, the PRAs need to have addressed these SSCs. Therefore, the SSCs not addressed by any PRA (or parts of any component modeled), but on the plant's Q list, are classified as relatively important until appropriate justification is provided to remove it.

The PRAs only need to have addressed the probabilistically significant failure modes for each classified SSC (as either relatively important or non-important). Probabilistically significant is defined as an unavailability greater than or equal to 1E-5 at the component level.

The level of model resolution determines the degree of application of a plant's SSCs. To determine that an SSC may potentially be classified relatively non-important, then that SSC needs to be explicitly represented in the model. For example, if an SSC is modeled in the PRA, but not explicitly represented, it should be classified as a relatively important SSC.

The PRA quantification process may take advantage of truncation of low probability events, cut sets, or sequences. The truncation value must ensure, however, that at least 95 percent of the core damage frequency is captured. This truncation value may need to be reconsidered if the core damage frequency is dominated by a single SSC.

The use of generic data for the quantification of events failure rates and unavailabilities is adequate for this generic application.

HRA has the ability to impact the identification of the dominant sequences. Inadequate HRA could, therefore, erroneously result in identifying relatively important SSCs as relatively non-important. To preclude this possibility, the classification of the SSCs is performed with the HEPs for the various operator activities as follows:

- A screening value of at least 3E-2 must be used for pre-initiator human events.
- A screening value of at least 0.1 must be used for all response type post-initiator human events and a screening value of 0.5 for all recovery type post-initiator human events, with a bottom threshold value of 1E-3 for all post-initiator human events per accident sequence.[7]

The PRA needs to be current at the time of its application. Generally, updating the PRA at every refueling outage will provide this currency.

PRA Criteria for Plant-Specific Importance Classification —

This categorization credits plant-specific differences for the relatively important SSCs. Those plant-specific SSCs that are determined from the plant-specific PRA to be relatively non-important are differentiated from the generic list of relatively important SSCs.

This category of SSCs found non-important in a plant-specific study would not be subject to the current level of regulatory implementation for that plant, but to a graded

---

[7]As used here, recovery actions refer to all post-initiator human actions outside the Emergency Operating Procedures for the plant (see Section 4.2.2). The lower threshold value should be applied in the Boolean combination of all human errors in a given accident sequence.

implementation. The implementation, however, would be more stringent than for those SSCs that have been found to be relatively non-important in any PRA. The higher level of implementation is imposed since some PRA of a similar plant has found this SSC to be relatively important.

To categorize SSCs on plant-specific information, the criteria imposed on the plant-specific PRA is also more stringent. This stringency is applied to the data and truncation criteria. The other criteria are the same as for the generic application.

The data for those SSCs under consideration need to be based on plant-specific information. For example, if a specific SSC is determined as relatively important from a PRA of a similar plant, but this SSC is determined relatively non-important from its plant-specific PRA, the data used to estimate the plant-specific SSC's reliability and availability need to be based on plant-specific information.

In quantifying a PRA, it is natural to truncate low probability events, cut sets, or sequences. When this truncation is performed, the importance measures are only computed for those SSCs that are not truncated and do not consider the effect on the truncated portion. For a plant-specific SSC determined to be relatively non-important from its plant-specific PRA (although some PRA of a similar plant found it to be relatively important), the quantification of this SSC's importance measure needs to consider the effect of the SSC's unavailability and unreliability on the entire PRA model. In addition, any truncation value may need to be reconsidered if the core damage frequency is dominated by a single SSC.

4.4.5 Graded Type Applications

Appendix B to 10 CFR 50, states that *"the Quality Assurance program shall provide control over activities affecting the quality of the identified structure, system and components, to an extent consistent with their importance to safety."* A PRA provides a tool that can categorize the SSCs according to their relative importance to safety and, therefore, define different categories of QA implementation.

The graded QA implementation approach outlined above is but one example of fulfilling a regulatory request, a generic letter, etc. This type of approach — defining different categories of implementation for the SSCs commensurate with their relative importance — is not unique. For those regulations, generic letters, etc. where a ranking approach is appropriate to provide either gradations in the degree of response, or to prioritize the timing of the response, a similar process would be followed as illustrated below in Figure 4.4-4.

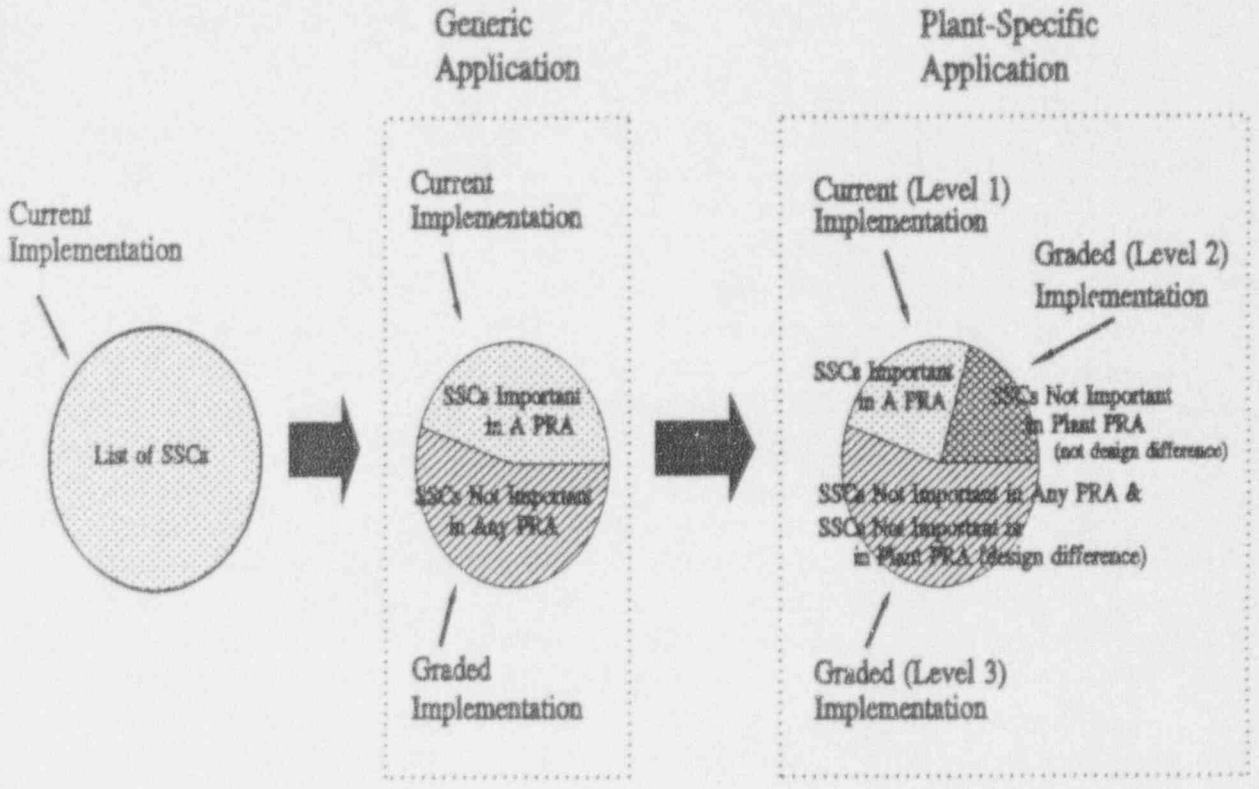

Figure 4.4-4. Graded Approach Process.

The criteria used in classifying relatively important and relatively non-important SSCs would be the same. In addition, the criteria established for the PRA would be the same.

The requirements for the various categories would need to be defined. These requirements should be commensurate with their relative importance. In addition, any application should not violate the defense-in-depth philosophy.

4.5 PRA APPLICATION FOR CONFIGURATION ANALYSIS (Group 2)

One aspect of the regulatory process involves technical specifications that, in a sense, control the configuration of a plant. The configurations are established by the allowed outage times (AOTs) associated with the limiting conditions of operation (LCO) in the Technical Specifications. The AOT defines that period of time that an SSC is allowed to be out-of-service before a plant shutdown is required.

The Technical Specifications also provide the surveillance test intervals (STIs) required for various plant SSCs. The surveillance test is performed to ensure that important standby systems will function as demanded when required.

The AOTs and STIs are modeled in a PRA as they affect the SSCs availability. The AOTs control SSC unavailability due to maintenance by the specified AOT time. The STIs control SSC unavailability due to failures by limiting the fault exposure time. A PRA can, therefore, be used to optimize these conditions.

A discussion of the types of applications and their associated criteria are provided below.

4.5.1 Configuration Application Regarding AOTs

Currently, Technical Specifications usually require a plant to shut down or take appropriate action when an AOT is exceeded. This requirement may, however, pose a challenge if the AOT applies to a system needed for shutting down or continued shutdown. Therefore, the required shutdown of the plant may present a greater risk than remaining at power for an additional amount of time. The risk should then be evaluated for remaining at power versus shutting down when an LCO occurs to determine whether it is best to repair the SSC with the plant at power or in shutdown. The risk of concern, in this context, is the occurrence of core damage.

The probability of a core damage state occurring from remaining at power when an AOT is exceeded is computed by analyzing the specific configuration using the PRA model. The PRA, however, provides the core damage ***frequency*** for an average configuration and any possible event. The PRA model must then be modified to account for the specific configuration and quantified for the core damage ***probability*** of the specific configuration.

The various SSCs in the plant are in a specific state. They are either "up" (i.e., available), or they are "down" (i.e., unavailable). These specific availabilities are modeled instead of the average annual availability.

The likelihood of a core damage state occurring from continued operation is compared to the probability of a core damage state occurring from shutting down. This latter state is comprised of three phases. A core damage state could potentially occur during the period of shutting down, during the shutdown period, or during the period of starting up. Each of these phases should be evaluated and compared to the likelihood of a core damage state from remaining at power.

It can be assumed that the probability for a core damage state occurring during the period of shutting down is comparable to one of a manual shutdown with the specified equipment out-of-service. The potential accident sequences associated with a manual shutdown, or normal transient, are delineated in a PRA. Therefore, the core damage probability associated with a normal transient is computed considering an initiating event probability of 1.0.

For a single line item AOT change or a group of several line item changes, comparison of the probability of a core damage state from continued operation to the probability of a core damage state from shutting down is adequate. PRAs can, however, be used in the optimization of AOTs. For this application, consideration of the average annual core damage frequency should be included.

The average annual core damage frequency provides the risk level for a normal power operation considering the likelihood of potential failures and the expected maintenance schedule. This value sets the limit, or upper bound, for the plant; that is, the net effect of the proposed chagne must either reduce overall risk or be risk neutral.

In this type of application, predetermined extensions of the AOTs for each SSC are evaluated. There could be a configuration where the core damage frequency exceeds the average core damage frequency. This increase would imply that the current estimated level of safety is not met, but this can be controlled by strictly limiting the time the adverse configuration is permitted to exist. It is, therefore, important to ensure that any individual AOT extension or set of extensions does not cause the current estimated average level of safety to be increased. The probability of a core damage state from any extended AOT must then be equal to or less than the average core damage frequency.

Using this ground rule, the maximum pre-determined AOT extension for any single SSC can be computed as follows:

$$AOT_{total} = \frac{CDP_{MS}}{CDF_{CO} - CDF_{avg}} \qquad \textit{[Ref. 4-11]}$$

where CDP_{MS} = core damage probability of manual shutdown
CDF_{CO} = core damage frequency of continued operation
CDF_{avg} = average core damage frequency

Note that if a train were successfully tested, showing evidence of continued operability, the core damage frequency for continued operation would decrease, thus extending the AOT. In this manner, a family of AOTs could be calculated for a variety of train operability configurations.

Figure 4.5-1 illustrates this concept of continued operation versus shutdown.

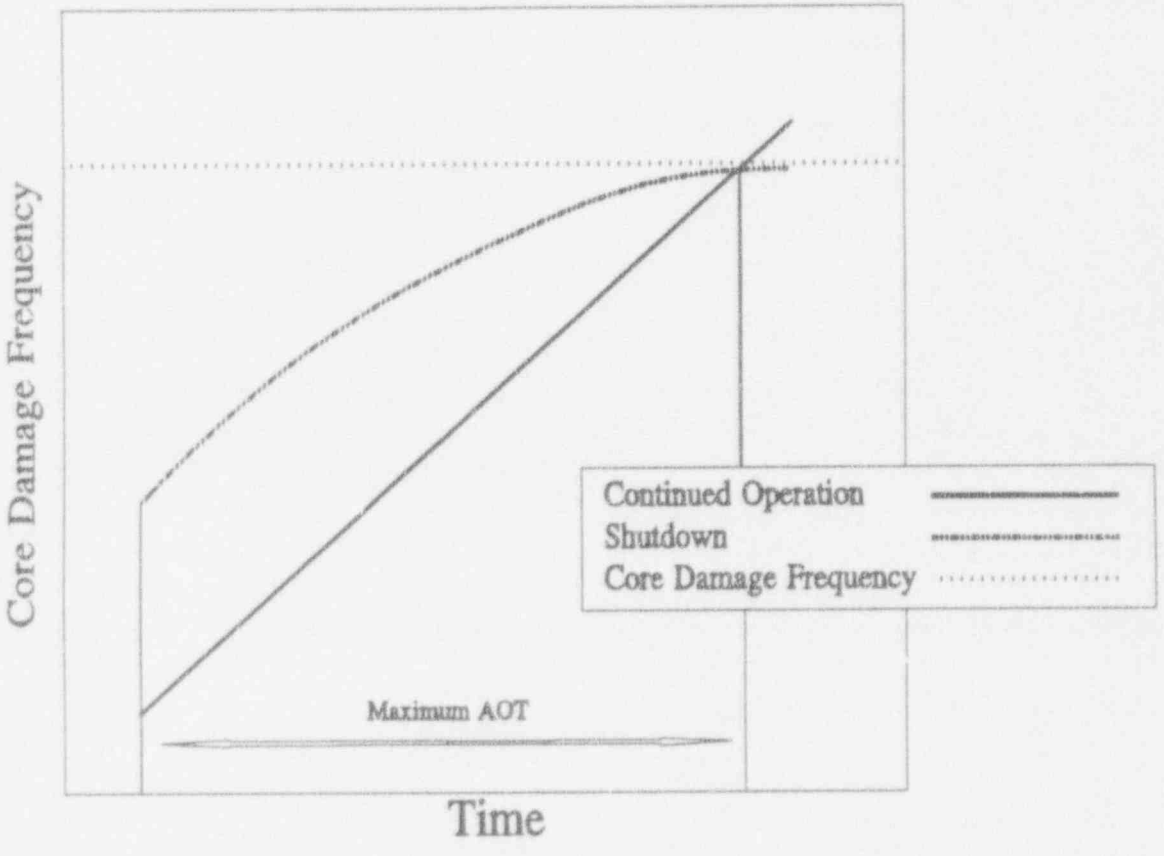

Figure 4.5-1. Comparison of Core Damage Probability of Continued Operation versus Shutdown.

In this application, the PRA could be used to "optimize" the AOTs in the Technical Specifications. That is, for either a single line item or a group of several line items, the AOTs are evaluated and additional AOTs are added to the Technical Specifications. These added AOTs are specified for certain predetermined plant configurations that must be maintained. (See Section 4.8 for a discussion of the Torness Technical Specifications.)

4.5.2 Configuration Application Regarding STIs

The Technical Specifications state the frequency at which standby components need to be tested. These requirements, however, have been argued to pose adverse effects on safety by causing plant transients or causing undue wearing of SSCs. A PRA can be used to optimize the STIs without affecting the current level of safety.

In considering an STI change, the core damage frequency based on the new STI needs to be compared to the core damage frequency based on the current STI.

As noted above, the STIs control SSC unavailability by limiting the fault exposure time. In as PRA, this unavailability is computed as follows:

$$Q \propto \lambda T$$

where Q = component unavailability, λ = component failure rate, T = component STI

Based on the above equation, if the STI for a component were increased, it can easily be seen that the unavailability of the component, not the failure rate, is increased. Conversely, the opposite is true. If the STI were decreased, the unavailability is decreased. Note that if one train is failed, the availability of the second train can be improved be increased surveillance testing.

Using the average core damage frequency as the upper limit, one approach to optimizing STIs is to investigate functional availabilities rather than the availability of a single component. In this approach, the functional availability is held constant while manipulating the availabilities of the systems comprising the function. That is, the STIs for some of the SSCs could be increased but decreased for others with the availability of the function remaining constant. The same would apply for either a system or train. The system or train availability would, therefore, be held constant while manipulating the availabilities of the trains and components comprising the system or train. These applications would require specifications at the functional, systemic, or train level to remain constant.

In this type of application, the availability for either the function, system, or train would be established from the average core damage frequency based on the current STIs.

Criteria similar to that defined for graded implementation (see Section 4.4.1) can also be used here to identify relatively important and non-important components; and therefore, identify the candidate components for increasing STIs, and identify the components where the STIs should not be changed. For example, the STIs for the relatively non-important SSCs could be increased, since the limits on the relatively important SSCs would control, and the current estimated safety level would not be impacted.

In the above application, the safety level is not impacted because either the overall function, system, or train availability is not changed. The STIs can also be manipulated with the safety envelope unchanged without maintaining the function, system, or train availability constant. Other compensatory measures could be proposed to offset any increased STI that would maintain the current level of safety.

It is noted that the situation is more complex than addressed here. The unavailability is a function of not only the time-dependent failure rate but also of the demand stresses placed on the system. In evaluating STIs, attention should be given to the root cause analyses of plant-specific failure to properly evaluate the effect of STIs. In addition, any application should not violate the defense-in-depth philosophy.

4.5.3 PRA Criteria

In using a PRA to optimize AOTs and STIs, the PRA must be performed to certain criteria. These criteria address those boundary conditions associated with a PRA (discussed in Section 4.2).

The PRA needs only to have addressed internal events, including internal flooding.

Proposed AOT and STI changes for SSCs are bounded by the level of detail of the PRAs. For a change to be considered, the PRA needs to have addressed these SSCs.

The failure modes that characterize the AOT and STI for the SSCs under consideration need to be included in the PRA model.

The level of model resolution determines the degree of application of a plant's SSCs. To determine the impact of changing an AOT or STI of an SSC, that SSC needs to be explicitly represented in the model.

The PRA quantification process may take advantage of truncation of low probability events, cut sets, or sequences. The truncation value must ensure, however, that at least 95 percent of the core damage frequency is captured. If truncation is performed, the quantification of importance measures, for the single line SSCs needs to consider the effect of the SSC's unavailability and unreliability on the entire PRA model. In addition,

the truncation value value may need to be reconsidered if the core damage frequency is dominated by a single SSC.

The use of generic data for the quantification of events failure rates and unavailabilities is adequate for most of the SSCs. For the SSCs involving single line item type reliefs, plant-specific data are required.

HRA has the ability to impact the identification of the dominant sequences. Inadequate HRA could, therefore, erroneously result in identifying relatively important SSCs as relatively non-important. To preclude this possibility, the classification of the SSCs is performed with the HEPs for the various operator activities as follows:

- A screening value of at least 3E-2 must be used for pre-initiator human events.

- A screening value of at least 0.1 must be used for all response type post-initiator human events and a screening value of 0.5 for all recovery type post-initiator human event, with a bottom threshold value of 1E-3 for all post-initiator human events per accident sequence.[8]

The PRA needs to be current at the time of its application. Generally, updating the PRA at every refueling outage will provide this currency.

An NRC review needs to have been performed of the plant-specific PRA of the licensee using the application. A process type review for the majority of the PRA is adequate for this type of application; however, focus needs to be particularly emphasized in the data area regarding the computation of the core damage frequency value. Guidelines on the specific review criteria should be developed as part of any pilot study.

---

[8] As used here, recovery actions refer to all post-initiator human actions outside the Emergency Operating Procedures for the plant. The lower threshold value should be applied in the Boolean combination of all human errors in a given accident sequence.

4.6 PRA APPLICATION FOR ON-LINE CONFIGURATION CONTROL (Group 3)

PRA, at its most optimum, can be used in a living manner. In this type of application, the probability of a core damage state is computed in real-time and plant decisions — operational, maintenance, etc. — are made based on the core damage probability. This applications would essentially replace the current concept of LCOs in 10CFR 50.36.

A real-time computation of the core damage probability would mean that the PRA model and the entire PRA process is computerized such that the PRA inputs can be manually or automatically fed into the PRA model for the plant. Therefore, at any given time, a core damage probability for the plant is known. A system would then need to be designed and implemented that could perform this task.

In this application, some plant safety decisions would be made based on a calculated core damage probability. A baseline core damage probability (or upper limit) would be established, and the plant would be designed, operated, and maintained within this baseline. Therefore, the absolute value of the core damage probability becomes critical. A standardization for PRA regarding such items as boundary conditions, assumptions, scope, level of detail, etc., would need to be established and uncertainties resolved.

Since the PRA would be used to regulate the plant, assurance would need to be provided of both the adequacy and accuracy of the PRA and the PRA supporting software and hardware. Also, the real-time input of plant conditions to the PRA computer model would have to meet standards of acceptance. This provision would need to occur at all levels: therefore, requirements, audits, and inspections would more than likely be required at each level.

Development of systems such as this are within the state of the art. Efforts are well under way to implement the capability to evaluate the instantaneous risk level on close to a real-time base in the U.S. and in other countries, and operational systems have been functioning for several years in the United Kingdom. These systems can be an excellent aid to the plant operators and provide the analytic capabiity to make those plant analyses suggested by the Group 1 and Group 2 type applications relatively easy. However, although PRA can provide valuable insights, and a living-PRA can be a tremendous asset to the internal operations of a licensee, it is felt that the state of the art of PRA will ***not*** currently support this type of ***regulatory*** application outlined for on-line configuration control, noted as Group 3 in this report.

4.7 RELATIVE IMPORTANCE OF REGULATIONS

The objective of this effort is to assess the consistency of regulations with the safety goals by examining the feasibility of determining the relative "safety importance" of regulations considering their importance to public safety and health.[9]

4.7.1 Work Requirements

For the Surry or Peach Bottom NUREG-1150 model, considering the plant systems impacted by the regulatory requirements and license commitments and considering the systems modeled in the PRA and their relative safety importance, the feasibility of estimating the relative importance of these requirements and commitments to the plant's core damage frequency and its potential impact to public health and safety is determined. This process was performed per the following:

- Identify the regulations to be examined and differentiate between programmatic type regulations that impact the inherent PRA model assumptions (e.g., quality assurance, training, equipment qualification) and ones that explicitly impact systems and components modeled in a PRA (e.g., Anticipated Transient Without Scram (ATWS) rule, Station Blackout Rule).

- Identify the risk significant plant systems and components impacted by the identified regulations.

4.7.2 Technical Approach

As a feasibility study, a limited number of hypothetical regulatory changes were investigated, and an analysis of the risk impact was performed for each change.

A regulatory change could lead to changes in the input parameters of the PRA or changes to the PRA model itself (to account for new failure paths or the elimination of safety barriers). For this feasibility study, it was necessary to focus on the most risk-significant components/systems/initiating events in the PRA; structural changes were not investigated. The impact of changes in the characteristic parameters for these components/systems/initiating events were then quantified using the IRRAS 4.0 code.

To implement the approach, the following basic tasks were performed:

- A sample set of regulations was identified and specific changes were hypothesized.

---

[9]This effort was performed with the assistance of Idaho National Engineering Laboratory.

- A framework was developed to systematically relate regulations to PRA model changes.

- The impact of the hypothetical regulation changes were quantified using expert elicitation and propagated through the NUREG-1150 PRA models.

Identification of the Regulation Sample Set and Changes —

A classification scheme was used to group and evaluate the 10 CFR 50 regulations to generate a sample of regulations for use in this feasibility study. This classification scheme employed a number of variables that characterized the impact a given regulation can have on a PRA model. In particular, they indicate the mechanism by which the regulation can impact the PRA model and the scope (extent) of this impact. The variables are binary and are defined as follows (the possible values are indicated in the brackets):

Mechanism of Impact

X_1:	Directness of impact mechanism	[Indirect/Direct]
X_2:	Potentially affects numerical values of PRA model parameters	[Yes/No]
X_3:	Potentially adds new parameters to PRA model	[Yes/No]
X_4:	Potentially removes parameters from PRA model	[Yes/No]

Scope of Impact

X_5:	Impact extent	[Localized/Pervasive]
X_6:	Potentially affects PRA dominant sequences	[Yes/No]
X_7:	Potentially affects non-dominant sequences in PRA	[Yes/No]
X_8:	Potentially affects systems/components/failure modes not in PRA	[Yes/No]

By rating the 10 CFR 50 regulation with these variables, 14 natural groupings of rules were identified. A representative sample set of four regulations were chosen for this study:

- 10 CFR 50.62 (The ATWS Rule).
- 10 CFR 50 Appendix B (The Quality Assurance Rule).
- 10 CFR 50.120 (The Training Rule).
- 10 CFR 50.65 (The Maintenance Rule).

The impact of the ATWS Rule, 10 CFR 50.62, is in a grouping that has a direct impact (on the PRA model), potentially affects model inputs, and may remove parameters in the PRA. The scope of the rule is considered local and changes would impact both dominant

and non-dominant sequences. As an additional point the rule was chosen because its risk significance is expected to differ for BWRs and PWRs. It also provides a case where a number of detailed PRA studies have been done to analyze alternative strategies for compliance.

The Quality Assurance Rule, 10 CFR 50 Appendix B, and the Maintenance Rule, 10 CFR 50.65, are in a grouping that has a direct impact and potentially affects model inputs. They have a pervasive effect on numerous components, systems, and structures in the plant. Appendix B has been in effect since 1970 while the Maintenance Rule has only recently been adopted. It has not yet been completely implemented.

The Training Rule, 10 CFR 50.120, is still in draft form. It will be in a grouping that has a direct impact, potentially affects model inputs, and may add parameters to the PRA. It will have a pervasive impact on numerous components, systems, and structures in the plant. Changes in this regulation will impact the numerical input values of both the dominant and non-dominant sequences in the PRA.

The regulation changes were developed in a manner to illustrate typical ("average") variations in safety significance variations between the regulations. The changes considered were as follows:

- 10 CFR 50.62 (The ATWS Rule) — Determine the impact of implementing the ATWS Rule as if the regulation had never existed. The average plant response was considered different for BWRs and PWRs.

- 10 CFR 50 Appendix B (The Quality Assurance Rule) — Determine the impact of the rule on general component reliability, first by examining the effect if it were eliminated and second examining the effect if it had not existed.

- 10 CFR 50.120 (The Training Rule) — First, determine the impact of total implementation of the Training Rule. Secondly, determine the impact of the industry implementing training that met the intent of the training regulation but without having a formal regulation.

- 10 CFR 50.65 (The Maintenance Rule) — Determine the impact of total implementation of the Maintenance Rule.

Modeling Framework —

The largest technical difficulty in the study was associated with developing credible linkages between a given regulation and the PRA model itself. The framework adopted for identifying these linkages is shown in Figure 4.7-1. Basically there are only four

classes of model parameters that impact the results of a risk assessment model: initiating event frequency changes, component unavailability changes, recovery probability changes, and changes to PRA model structure. The changes in these parameters associated with a given rule change were determined using an expert elicitation process. This process was designed to make the experts consider multiple mechanisms by which a particular parameter might be affected.

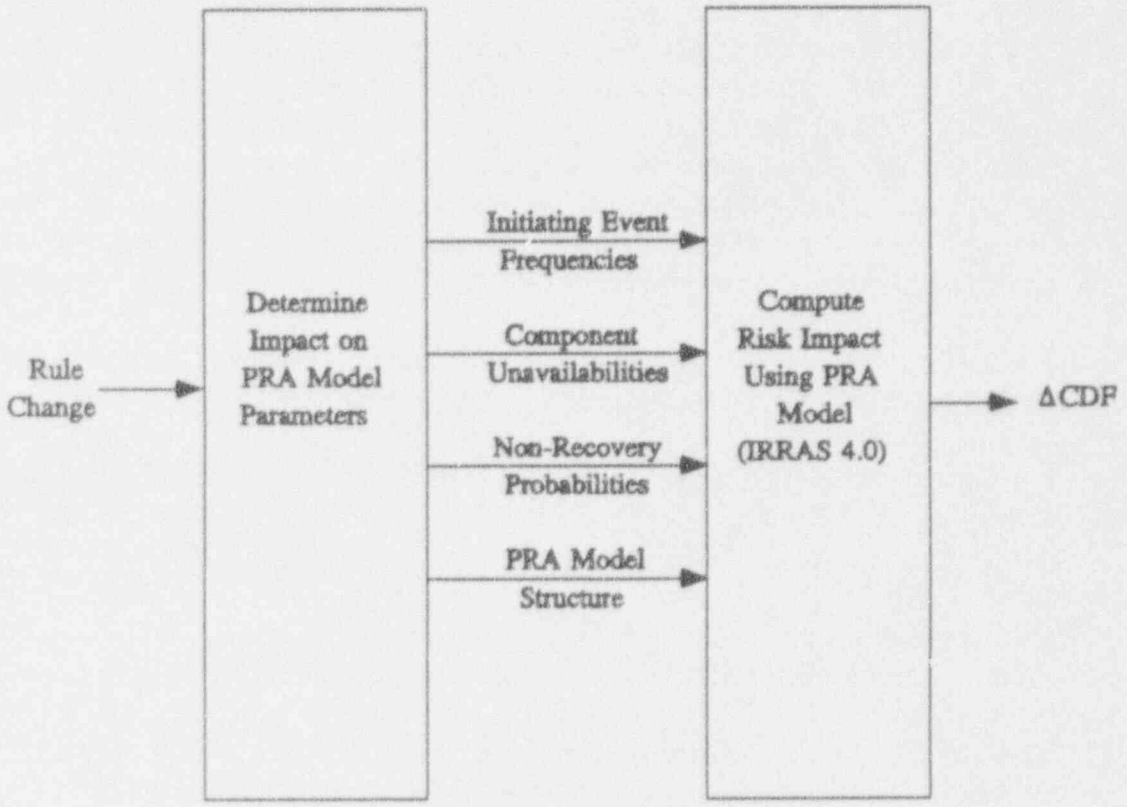

Figure 4.7-1. Modeling Framework.

To reduce the number of parameters elicited, importance analysis was used to focus on those parameters which had the greatest impact on core damage frequency risk. Importance measures were systematically developed for all PRA model parameters using the IRRAS 4.0 code. These measures are useful for predicting the effect of a change in a single PRA model parameter (e.g., a failure rate) or of small changes in a number of parameters. However, in this project, the simultaneous impact of a single regulation change on multiple basic events must be evaluated. Moreover, if the risk impact is significant, it can be expected that the magnitude of change in a given parameter may be one or more orders of magnitude greater than the original parameter value. Although

importance measures for multiple basic event variations can be developed, it is more direct and convenient to simply recompute the PRA model (i.e., to requantify the core damage frequency) using available computer software.

Quantification of the Impact of the Regulation Changes —

For each regulation change discussed above, the following steps were performed.

1. The specific scope of impact (i.e., which systems, components, basic events are affected by the regulation change) was determined and the qualitative impact documented in a summary discussion for the expert elicitation. Once the impacts were identified, a walk-through example was presented by a normative expert for each elicitation that illustrated how the regulatory change affects safety. (For example, in the case of quality assurance, the discussion could cover the different ways that QA impacts the procurement, installation, and testing of equipment.)

2. The mechanism of the impact (i.e., what PRA parameters might be modified) was determined for the rule change, and elicitation questions were developed.

   For each regulatory change, selected PRA parameters in the dominant sequences were grouped. The elicitation questions for each regulation were designed to directly address these PRA dominant sequence groups.

3. Qualitative measures of the expected change in groups of PRA parameters as a result of the benefit or elimination of selected regulations were elicited.

   Both the direction and magnitude of change were elicited. The magnitude elicitation was limited to a descriptive scale (obvious, noticeable, subtle).

   Direction of change was indicated by an increase, decrease, or no change.

   No change. This implies there is absolutely no relationship or correlation between the regulation and the PRA parameters. If no change is anticipated then the magnitude is not questioned.

   Magnitude of change in effect was elicited if there was either an increase or a decrease in the parameter (e.g., component unavailability).

   Subtle. A subtle change is anticipated. A subtle change implies a trend that requires a long period of time to discern (e.g., the trend if it exists is within the range of random fluctuations in data).

Noticeable. A noticeable change is anticipated. A noticeable trend is one that can be detected over time.

Obvious. An obvious change is anticipated. An obvious trend is immediately observable (i.e., marked and dramatic).

4. Quantification was accomplished by transforming the descriptive scale (obvious, noticeable, subtle) into numerical values. In this case, the descriptions were transformed into values based on the judgment of PRA experts.

5. The transformed numerical values were combined into a single factor (estimator) for each question; this factor was used to modify the dominant sequence groups, and then the PRA was requantified.

One of the weaknesses in this work concerns the connection between the qualitative data and the development of quantitative values. This is because each expert may have a differing opinion of the numerical values associated with their qualitative responses. Despite this weakness, it is expected the output of the estimation process is useful (in this feasibility study) to indicate the safety significance of these regulations.

4.7.3 Expert Elicitation Technique

To evaluate the magnitude of PRA model parameter changes used as inputs to the re-computation effort an expert elicitation was used. An expert panel was assembled consisting of two senior level nuclear utility managers (with expertise in operational safety assessment), an NRC Senior Resident Inspector, an NRC Senior Licensing Project Manager, and a Senior Manager from the NRC Office of Research. A formal training and normative session were held, and the experts were formally polled on the direction and magnitude of regulatory driven changes in key parameters impacting the PRA models.

The Nominal Group Technique was used for the expert elicitation in this feasibility study. The selection of this technique was based on considerations of available resources to demonstrate feasibility, expert estimation theory, and past experience with other methods. Scheduling constraints and cost considerations made it desirable to complete the face-to-face portions of the technique in one session. The Nominal Group approach allowed this.

The knowledge and expertise of experts was captured in pre-meeting preparation and information gathering and in the problem definition portion of the elicitation session itself. Problem decomposition into components was used to assist the development of each expert's final estimate.

The Nominal Group method employed no effort to obtain consensus judgments between experts. This structure, along with the facilitator's direction of the discussion, was designed to minimize bias due to domination of the group's thinking by any individual.

The expert elicitation session began with a brief introductory period in which participants were introduced, roles explained, and agenda reviewed. This was followed by an elicitation training session whose major focus was to introduce participants to the elicitation processes and to show them the importance of remaining open to new information as it becomes available. It also was used to introduce the scales to be employed.

The elicitation training was followed by a normative session in which general issue statements for each rule were introduced, and an overview of the linkages between plant functions and reliability was explained. Each issue statement summarized the objectives of elicitation, note background information provided, and defined the suggested baseline plant to be used. Issue statements also defined direction and magnitude of the changes to be elicited, explained the attached elicitation tables, and defined the suggested primary impacts of each rule.

For each rule change elicited, experts were asked to judge both the direction and the magnitude of the impact (i.e., Would the rule change increase, decrease, or not change reliability? Would the impact be subtle, noticeable, or obvious?). Specific components, systems, and functions to be considered were specifically named on the elicitation tables provided.

The experts were asked to first write their own estimates of the impacts of rule changes, and the basis for those impacts, on the forms provided. After all experts had completed making their estimates, they were asked in random sequence to disclose and explain their initial estimates to the rest of the group. The experts were then given the opportunity to privately change their estimates and to provide any additional reasoning on the provided forms. For each rule, a brief closing discussion was held.

For the expert elicitation, the qualitative results were summarized for each regulation as shown in the sample expert elicitation table shown in Table 4.7-1. There was excellent agreement among the experts concerning the direction of the regulation change impacts, and reasonably good agreement concerning the magnitude of impacts.

Table 4.7-1
Summary of Example of Expert Elicitation

	ELICITATION QUESTION/EXPERT RESPONSE	EXPERT A	EXPERT B	EXPERT C	EXPERT D	EXPERT E
	10 CFR 50.62 BWR ELICITATION					
1	Has the availability of the automatic scram system (RPS, ARI) increased or decreased?	Subtle Increase	Noticeable Increase	Subtle Increase	Subtle Increase	Expert not elicited
2	Has ability to achieve reactor subcriticality (via boron injection and RPT) increased or decreased?	Noticeable Increase	Subtle Increase	Noticeable Increase	Subtle Increase	Expert not elicited
3	Has the likelihood of the operator to initiate SLC (given an ATWS event) increased or decreased?	Noticeable Increase	Noticeable Increase	Obvious Increase	Noticeable Increase	Expert not elicited

4.7.4 Results

As described in Section 4.7.2, this feasibility study investigated four hypothetical regulatory changes and analyzed the risk impact from each change. The method used to quantify the impact of regulation changes was based on identifying appropriate changes to the PRA model, eliciting qualitative measures, and then quantifying the impact of these changes as described above.

After the expert elicitation, the qualitative results were summarized as shown in the sample expert elicitation table shown in Table 4.7-1. The qualitative results were then transformed into quantitative values and these numerical values were combined into a single factor (estimator) for each question. Each factor was then used to modify the dominant sequence groups of events from the dominant sequences, and the PRA was requantified to yield a new core damage frequency (core damge frequency after). The results as given in Table 4.7-2 and shown in Figures 4.7-2 and 4.7-3 demonstrate that the methodology can distinguish between risk impacts of different regulations. The experts elicited determined that the implementation of each regulations had some positive effect in reducing core damage frequency. It is important to note that the experts were careful to indicate that it is difficult (if not impossible) to determine all the combined influences on risk from other policies, regulations, and general knowledge and to estimate the contribution from each.

Table 4.7-2
Summary of Core Damage Frequency Impacts

	BWR BASE CASE CDF = 3.6E-6			PWR BASE CASE CDF = 3.2E-5		
REGULATION CHANGE	CDF AFTER	DELTA CDF	FACTOR	CDF AFTER	DELTA CDF	FACTOR
ATWS (IMPACT OF THE RULE)	1.6E-5	-1.3E-5	4	4.0E-5	-8.2E-6	>1
APPENDIX B (IMPACT IF THE RULE HAD NEVER EXISTED)	6.9E-6	-3.3E-6	2	1.2E-4	-9.0E-5	4
APPENDIX B (IMPACT IF THE RULE WERE ELIMINATED)	4.8E-6	-1.2E-6	>1	6.6E-5	-3.4E-5	2
TRAINING (IMPACT IF THE RULE WERE IMPLEMENTED)	3.4E-6	2.4E-7	0.9	2.7E-5	4.5E-6	0.8
TRAINING (IMPACT OF THE INTENT OF THE RULE)	1.9E-5	-1.6E-5	5	3.8E-4	-3.5E-4	12
MAINTENANCE (IMPACT IF THE RULE WERE IMPLEMENTED)	2.8E-6	8.2E-7	0.8	2.0E-5	1.2E-5	0.6

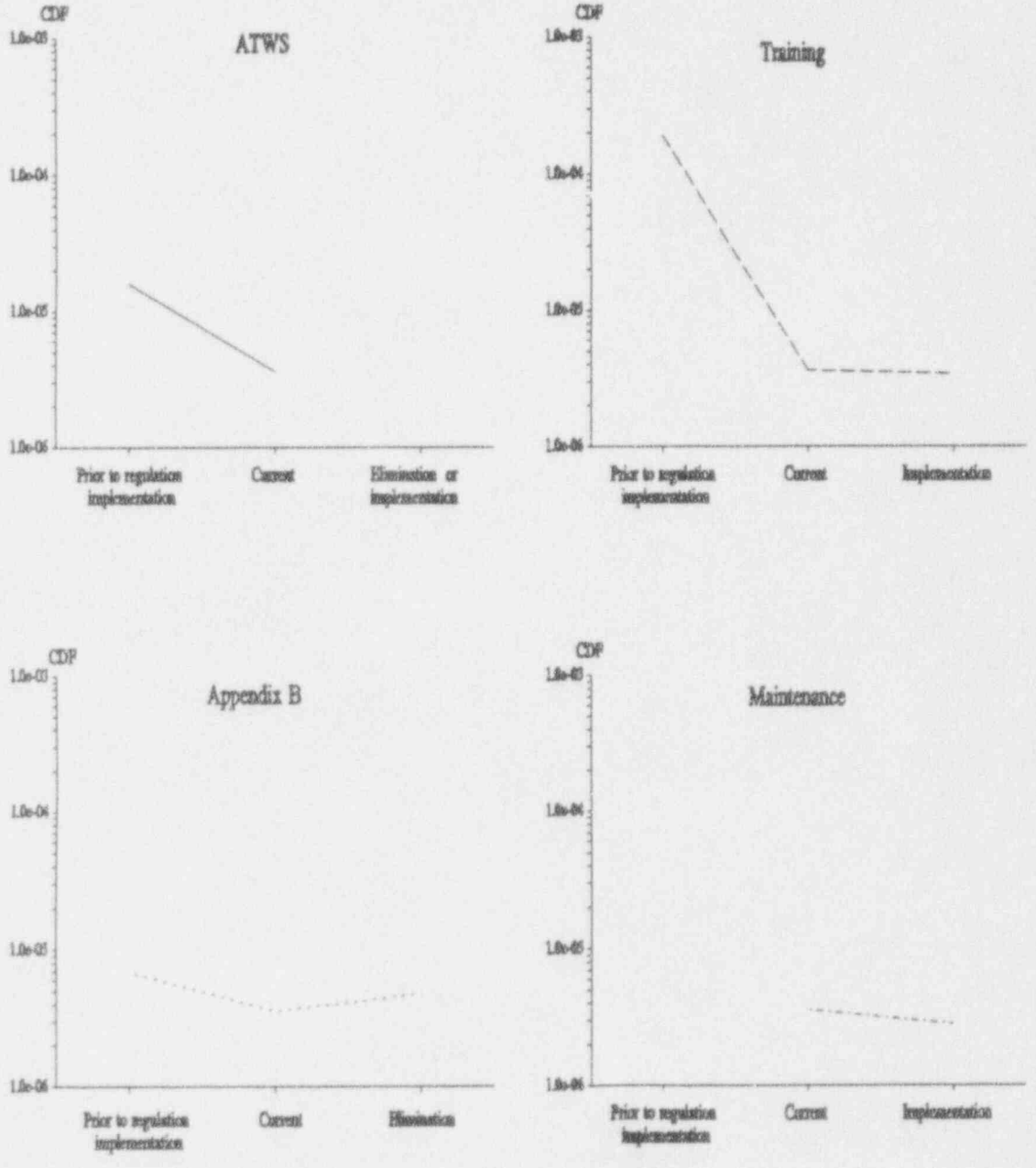

Figure 4.7-2. Resultant BWR Core Damage Frequencies Due to Changes in the Regulation.

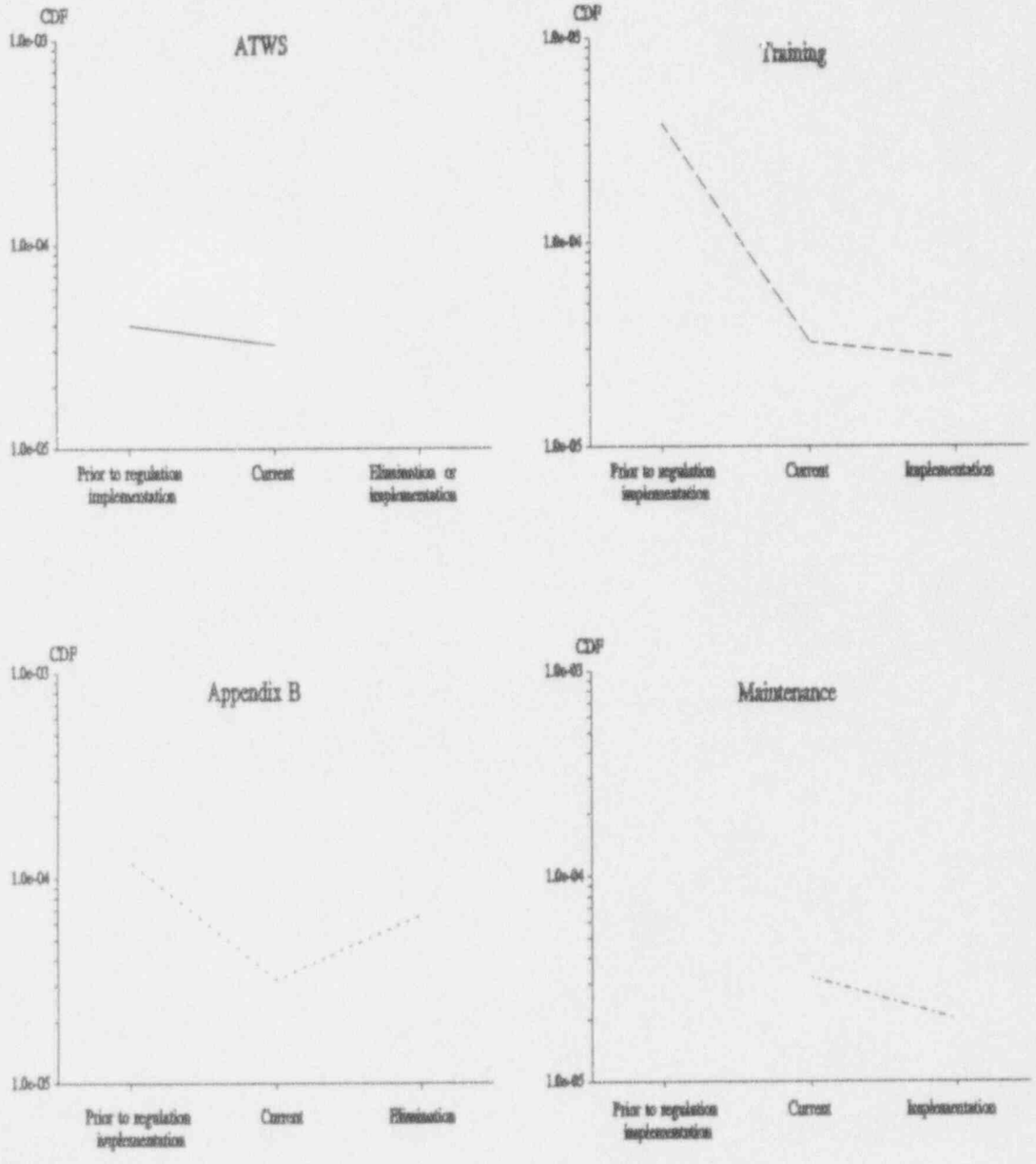

Figure 4.7-3. Resultant PWR Core Damage Frequency Due to Changes in the Regulation.

The Training Rule had the greatest impact of any of the regulation changes on the dominant sequences in both the BWRs and PWRs. The Training Rule was elicited for two impacts: (1) the impact of total implementation of the rule from the current 1993 situation and (2) the impact of the intent of the regulation prior to the 1982 timeframe. As is shown in Figures 4.7-2 and 4.7-3, the plant core damage frequencies, prior to implementation of the regulation, currently, and after total implementation are presented from left to right. The experts commented that the implementation of a systematic approach to training (this was initiated in 1983) greatly reduced risk. They felt it was difficult to tell how much of this change was actually due to the regulation and how much is related to other influences.

The ATWS Rule was elicited only on its impact prior to implementation. For the BWR it provided a greater factor of reduction in risk (4.4) than in the PWR (1.3). The experts felt that its greatest contribution was in increasing the knowledge base concerning reactor behavior and as a result the operators have an increased likelihood to initiate borate injection given an ATWS.

The Quality Assurance Rule, 10 CFR 50 Appendix B, was also elicited for two impacts: (1) the impact of total elimination of the rule from the current 1993 situation and (2) the impact of the intent of the regulation prior to the current timeframe. The results of the elicitation on Appendix B demonstrate that some benefit (a factor of 2 in BWRs and 4 in PWRs) was obtained from the original institution of this event. The benefit appears to produce a slightly better reduction in risk for the PWRs. The experts discussed that, with the elimination of this regulation, some benefit would be lost (a factor slightly greater than 1 in BWRs and 2 in PWRs) but that the average plant would maintain a level of QA that would maintain risk at much the current level. They also stated that information added to the knowledge base would not be lost with subsequent elimination of the regulation and this would also contribute to the maintenance of the current level of risk.

Information on the Maintenance Rule was elicited only on its impact after full implementation in the future. All the experts determined that the Maintenance Rule contributed the least to reduction of core damage frequency. For the BWR, it provided a factor of reduction in risk (4) than in the PWR (slightly greater than 1). The elicitation brought out that the Maintenance Rule's greatest significance was an increased focus on the safety significance of support systems. The reduction in risk will be subtle and largely due to the increase in the knowledge base.

4.7.5 Conclusions and Recommendations

Based on the results of this limited scope feasibility study, the following conclusions can be made:

- While some biases may exist in the interpretation of the impacts of regulations on PRA model parameters (event frequencies, component reliabilities, etc.) the relative directions and relative magnitudes of changes are not generally disputed by either utility or NRC experts. This was an unexpected result.

- Using the adjusted PRA model parameters obtained by the expert elicitation, it is possible to quantify and differentiate the risk impacts of specific NRC regulations. This can be done by identifying in a systematic fashion how regulations impact the frequency of potential initiating events, component reliability, probability of recovering failed systems, and PRA model structure (number of barriers available).

In the course of performing the study, several issues were identified that warrant further consideration in interpreting the absolute values obtained. The results obtained are a reflection of the specific modeling approaches taken in the Surry and Peach Bottom NUREG-1150 PRA studies. As an example, differences in the approaches taken for modeling the reactor protection system unavailability has an effect on the magnitude of the ATWS Rule risk impacts between PWRs and BWRs. Consideration of how to deal with these subtle differences could be the subject of future work. As an additional issue, the use of expert elicitation to estimate the likely changes to PRA model inputs is potentially biased by the inability to separate out the effects of numerous rule changes and industry initiatives that have been under way for the last decade. Each of the experts commented on this problem, and this should be given further thought.

To improve the ability to differentiate the risk impacts of a wider body of regulations, it will be necessary to eventually consider the impacts on PRA "back-end" parameters (e.g. those parameters that impact source terms and public exposure). This is a recommendation for future work that would lead to the ability to evaluate rules like the Combustible Gas Control Rule (10 CFR 50.44). The evaluation of these inputs can be done as an extension of the basic methodology put together for this feasibility study.

4.8 OTHER NON-NRC PERSPECTIVES

As part of the evaluation of the use of risk-based techniques in regulation, discussions were held with the regulatory authorities in Mexico, Sweden, Germany, and the United Kingdom, and with members of a working group of the OECD Committee on the Safety of Nuclear Installations Principal Working Group 5 that is exploring the state of the art of risk-based configuration control. Visits were also made to the Laguna Verde plant in Mexico and the Torness Power Station in Scotland to gain first-hand knowledge of their experiences.

The implementation of risk-based regulation in Mexico is comparable to that seen in the United States. PRA is used for issue prioritization and resolution, support in rulemaking, justification for continued operation, etc. A major PRA effort of the Laguna Verde plant is currently under way with the plant using the model in its operation and maintenance decisions. The plant is starting to explore the use of PRA in regulation in more detail with the encouragement of the Comisión Nacional de Seguridad Nuclear y Salvaguardias.

The joint Nordic study *[Ref. 4-11]* and *[Ref. 4-12]* is still in progress, but they are exploring the use of PRA in regulation in considerable detail, particularly in the regimes of AOT and STI determination. Results of this study should be available to assist the development of pilot studies in this area.

The Torness Power Station in Scotland has developed a technique for management of plant configuration control in a manner that appears to be consistent in many ways with the regulatory system employed in the United States and that may offer significant insights to those developing pilot applications relative to Technical Specifications or configuration control in this country.

The Torness Power Station employs a Mark II Advanced Gas Reactor. It uses a highly redundant and diverse combination of systems to provide essential post-trip cooling services. A quadrant approach is utilized in the design of the safety systems that provides substantial physical separation. A PRA was performed for the essential post-trip cooling function.

In setting the requirements for allowed time for component maintenance and repair, the plant examined a variety of possible configurations that might obtain from outages of selected equipment. Their approach to what are essentially AOTs for the various configurations was to permit the instantaneous core damage frequency to increase by a factor of up to 10 over that of the baseline PRA for a period of time not to exceed 30 days (approximately 1/10 year), and to allow the instantaneous core damage frequency to increase by a factor of 10-to-100 for a period not to exceed 3 days (approximately 1/100 year). In addition, they have overlaid requirements to preserve the "single failure

criterion" and to limit the overall amount the integrated instantaneous risk may exceed the baseline PRA.

Because the systems involved are complex and highly redundant, there are a large number of possible configurations. They have calculated the risk increase for a large number of possible configurations and incorporated the results into a series of approximately 200 rather complex tables that define the permissible outage times associated with the various configurations. These tables are incorporated into the plant's Identified Operating Instructions, which are roughly akin to the Technical Specifications of U.S. plants. A computer is available in the control room to search the outage tables and determine which may be satisfied given the actual status of the plant. Hard-copy versions of the table are also available to verify the computer search or to determine appropriate limits if the computer becomes unavailable. This type of operation, with pre-calculated and verified tables presenting AOTs for a wide variety of system configurations, is an excellent example of what might be accomplished under the Group 2 type of application of PRA methods, discussed above.

The Torness system also has other features that increase its utility operationally. The computer maintains an accurate log on the number and outage times associated with equipment outages, permitting an easy evaluation in trends in component reliability. The system can be used in a prospective mode and is routinely used to plan outages of equipment to minimize the risk impact. It can also provide a prioritized list of what repairs would have the greatest risk reduction potential if an undesirable configuration were to occur.

A more detailed description of the Torness approach can be found in the "Operational Experience of a Reliability Based Maintenance Strategy for the Control of Essential Post-Trip Cooling Plant in a Nuclear Power Station" by W. B. Waddell *[Ref. 4-13]*.

4.9 EXISTING NRC EFFORTS

PRA applications having the potential to provide more flexibility in the regulations and in the implementation of the regulations while maintaining safety are those that primarily address configuration control and QA issues. Configuration control applications generally involve the utilization of PRA methods to optimize STIs and AOTs. QA applications generally involve the utilization of PRA to support "graded" QA; that is, optimizing QA for those structures, systems, or components that are safety significant based on PRA insights. Current NRC-sponsored programs were examined to identify those efforts that are using PRA that could provide potential insights in these areas.

The use of PRA by the NRC has been both broad and narrow. The broad application is seen in the many various and diverse activities that have increased over time, particularly since the TMI accident. The utilization of PRA, however, has been narrow in that it has been limited to a small set of applications. These activities have been defined and summarized into several categories (as reported in the draft NRC PRA Working Group Report) *[Ref. 4-14]* as follows:

- *Licensing of reactors* that involves using PRA in the review of analyses submitted as part of advanced reactor design certification applications, and plant-specific licensing actions such as Technical Specification modifications, justifications for continued operations, etc.

- *Regulation of reactors* that involves using PRA in monitoring of operations (with risk-based inspections); screening of events for significance (including operational event screenings, generic safety issue screenings, and facility screening risk analyses); analyses of events and issues (including operational events analyses, component and system failure data analyses and trends, reliability monitoring now developing as a result of the maintenance rule, generic safety issue analyses, and severe accident research studies); facility analyses (both those performed by the staff such as NUREG-1150 and those performed by licensees in the individual plant examination process); and regulatory analyses supporting regulatory actions such as backfits.

- *Licensing of fuel cycle and materials* that involves using methods similar to risk analyses (called performance assessment methods) that are being used as part of the licensing of proposed high-level-waste repository.

These activities are summarized below in Table 4.9-1.

Table 4.9-1
Summary of Staff PRA Uses

CATEGORY	APPLICATION
Licensing of Reactors	• Reviews of advanced reactors. • Reviews of plant-specific licensing actions.
Regulations of Reactors	• Monitoring operations by inspection. • Issue screening of operational events, generic safety issues, and facility screening risk analyses. • Issue analyses of operational events analyses, operational data and trending analyses, maintenance rule regulatory guide, generic safety issues, and severe accident issues. • Facility analyses involving staff studies and individual plant examinations. • Regulatory actions including regulatory analyses.
Licensing of Fuel Cycle and Materials	• Reviews involving high level waste facilities.

As can be seen, these PRA efforts are relatively diverse; and although each NRC office is involved in programs using PRA, current utilization of this type of integral analysis by the NRC is rather limited when focused on attempts to reduce regulatory burden or provide additional flexibility with the regulations and licenses. Current NRC-sponsored programs that can provide insights in support of this area primarily involve configuration control regarding Technical Specification optimization. No NRC-sponsored programs supporting graded QA based on PRA were identified.

These specific types of activities are summarized below for each NRC office.

4.9.1 AEOD-Sponsored Programs

The Office for Analysis and Evaluation of Operational Data (AEOD) utilizes PRA techniques and insights in the accomplishment of its mission. Although their ongoing PRA-related programs are not focused on determining ways to reduce regulatory burden

and provide flexibility in licensing and regulatory actions, the Trends and Patterns Analysis and the Reactor Operations Analysis Branches within the Division of Safety Programs are involved in efforts that can ultimately assist in providing the data requirements and insights for PRA-based programs supporting configuration control and graded QA (from a regulatory perspective).

The Trends and Patterns Analysis Branch has ongoing programs that analyze operational data to identify and provide a quantitative content for new safety issues; evaluates the effectiveness of current regulations, regulatory actions, and initiatives taken by licensees to resolve safety issues concerns; and helps guide and focus engineering evaluations. These programs support four major activities as follows:

- Hardware performance studies of risk-important components, systems, initiating events, and accident sequences.

- Safety and regulatory studies of trend performance for selected regulatory issues through an appropriate parameter related to the specific issue to determine effectiveness of implementation.

- Data base studies involving common cause failure event data and a human performance data base that trends human actions important to plant safety and risk.

- Risk assessment studies evaluating the risk implications of trending results from the hardware, safety issues, and special data analyses.

The Reactor Operations Analysis Branch's ongoing Accident Sequence Precursor (ASP) Program also provides needed support for the PRA utilization in configuration control and graded QA optimization. The ASP program provides a safety significance perspective of nuclear plant operational experience. The program uses PRA techniques to provide estimates of operating event significance in terms of the potential for core damage; that is, accident sequence precursors are events that are important elements in core damage accident sequences. Such precursors could be infrequent initiating events or equipment failures that, when coupled with one of more postulated events, could result in a plant condition leading to severe core damage. The precursors are selected and evaluated using an evaluation process and significance quantification methodology. The types of events evaluated include initiators, degradations of plant conditions, and safety equipment failures that could increase the probability of postulated accident sequences.

4.9.2 NRR-Sponsored Programs

The Office of Nuclear Reactor Regulation (NRR) has current PRA efforts directly supporting licensing and regulatory activities that can provide regulatory burden reduction

and flexibility in the implementation of the regulations. These efforts are being performed in the Operational Reactor Support and Systems Safety Analysis Divisions by the Technical Specifications and Probabilistic Safety Assessment Branches, respectively.

In 1987, the Commission issued its interim "Policy Statement on Technical Specification Improvements for Nuclear Power Reactors" encouraging licensees to voluntarily implement a Technical Specification Improvement Program. As a result of this policy statement, five sets of improved STS were developed; one for each Nuclear Steam Supply System (NSSS) vendor (i.e., Westinghouse, Babcock and Wilcox, Combustion Engineering, General Electric BWR 4, and General Electric BWR 6). PRA was utilized in the development of these STS as follows:

- A number of completion times (i.e., AOTs) and STIs were relaxed based on NRC staff-approved topical reports and on draft NUREG-1366 *[Ref. 4-15]*. In their topical reports justifying the relaxations, the NSSS vendors based their conclusions on PRA insights. NUREG-1366 used qualitative rather than PRA insights to support such relaxations.

- Using the Grand Gulf and Surry PRAs from NUREG-1150, the core damage frequencies were recalculated with the new STS changes to identify any potential concerns. No significant increase in core damage frequency was observed as a result of these changes.

A "lead" plant for each NSSS STS has been identified by industry.

As the implementation of the improved STS and development of line-item improvements proceeds, the staff's intends to utilize PRA along with deterministic bases to support its decisions. This utilization will primarily be based on evaluations of industry's proposals. The information from the programs currently in progress in the Office of Nuclear Regulatory Research (RES) will be used to support or validate, as appropriate, industry's risk-based proposals.

Currently the staff is evaluating risk-based changes to Technical Specifications proposed by the South Texas Nuclear Project. This effort is currently in progress in RES.

The Probabilistic Safety Assessment Branch activities that directly involve PRA efforts to improve plant operations and maintenance primarily include providing risk assessment of potentially safety significant issues and reviewing applications submitted by the licensees. The issues reviewed for their risk impact are a result of identified safety concerns. Recent examples include:

- Intersystem LOCA.

- Shutdown Risk.
- Alternative Tube Plugging Criteria.

The applications submitted by the licensees are generally requests for exemptions (or waivers) from regulatory requirements. The justification for requesting and granting the exemption includes PRA insights. Recent examples include:

- Waiver to allow refurbishment of service water system.

- Minor actions involving man-made hazards, tornado protection, containment penetrations, and toxic gas detectors.

4.9.3 RES-Sponsored Programs

RES has several ongoing PRA efforts directly supporting licensing and regulatory activities. These programs are being performed in the System Research, Safety Issue Resolution and Engineering Divisions by the Human Factors Branch, the Severe Accident Issues and Probabilistic Risk Assessment Branches, and the Electrical and Mechanical Engineering Branch, respectively.

The PRA programs in the Human Factors Branch are currently those that have the greatest potential in assisting in the assessment of risk technology for providing regulatory burden reduction and flexibility while maintaining safety. These efforts are primarily focused on developing methods in direct support of Technical Specification improvements as follows:

- Risk impact in varying AOTs and STIs at power and during shutdown and considering the effects of test errors on optimum test intervals.

- Risk impact from action statements requiring shutdown if equipment needed during shutdown (e.g., residual heat removal) fails.

- Risk implications of taking equipment out-of-service for maintenance looking at rolling maintenance schedules, optimizing the frequency of schedule maintenance, and integrating surveillance with preventive maintenance.

- Dependent failures examining improved methods for recognizing and preventing dependent failures.

- Configuration management considering a conceptual framework for risk-based configuration management.

The methods that are being developed are reliability-engineering tools that analyze Technical Specification requirements within the framework of a PRA and that can estimate the risk impact of changing the level of a particular requirement in Technical Specifications; and therefore, they can provide a risk perspective on the bases for these Technical Specification requirements and for related maintenance guidelines.

These applications share the strengths and weaknesses of PRA. They are useful to integrate and prioritize only those considerations that can be quantified in terms of reliability and availability; therefore, they are applicable to only a fraction of the requirements in Technical Specifications. In general, these methods are directly applicable to evaluating AOTs and STIs for active, front-line systems, and support systems. The methods are only marginally applicable to instrumentation, and are not applicable to concerns not modeled in PRA, such as security and occupational health. In general, these methods are not yet sufficiently refined to treat uncertainties in detail. It is expected that consideration of uncertainties will be incorporated with the use of these methods.

There are currently six ongoing programs that are developing these methods as described below.

1 — Procedures for Evaluating Technical Specifications

In 1983, a task force established by the Executive Director for Operations (EDO) provided recommendations to improve surveillance testing requirements in Technical Specifications. The resulting actions formed the Technical Specification Improvement Program. In 1987, a Commission Interim Policy Statement on Technical Specifications Improvement encouraged licensees to voluntarily implement a Technical Specification Improvement Program that included applying risk analysis methods and human factors principles to improve Technical Specifications. In support of this program, research began to develop methods for evaluating the risk impact of requirements in Technical Specifications, to explore alternative approaches, and to provide a technical basis for improvements.

This research, which is largely completed, has published methods to evaluate the risk impact of AOTs and STIs (including the impact of test errors). The work also outlined a conceptual approach for operational configuration control. The remaining work on this project, which is being completed in 1993, will provide a method to evaluate the risk impact of scheduled maintenance intervals. The approach analyzes the balance between beneficial and adverse effects of maintenance, and models three states: operable, degraded (i.e., ready for preventive maintenance), and failed. The method can use NPRDS data for incipient, degraded, and complete failures. The results of this research will allow analysis of the risk impact of issues such as not permitting certain preventive

maintenances during power operation and instead requiring that AOTs during power operation be used only for corrective maintenance.

One of the new STS's will be used as a testbed for a limited pilot application of the methods described in this report for evaluating requirements in Technical Specifications. This pilot application involves developing a strategy and criteria that will result in clear, simple statements of requirements that integrate risk and practical considerations to control risk efficiently. These criteria are intended to address:

- The scope and frequency of updating of the PRA and data base that form the basis for the licensee's risk analysis.
- What risks must be assessed to support Technical Specification changes and acceptable ways to model them (e.g., test intervals, test effectiveness, test errors, and aging effects).
- Prioritizing risk contributors in Technical Specifications.
- Acceptable changes in risk.
- Experience feedback, if appropriate, in updating Technical Specification requirements.

2 — Technical Specification Requirements During Shutdown

NRC is reevaluating regulatory requirements for nuclear power plants during shutdown. One aspect of this reevaluation is to consider how effectively Technical Specifications control risk during shutdown.

In support of this endeavor, this project was established to develop methods for evaluating the risk impact of plant configurations permitted and surveillance required by Technical Specifications during shutdown; to explore alternative approaches; and to provide a technical basis for improvements. These analysis methods use as a framework the low-power-and-shutdown PRAs (described elsewhere in this report).

These models and trial applications to a pressurized water reactor (PWR) and a boiling water reactor (BWR) will be completed in late 1993.

3 — Action Statements That Require Shutdown

As part of the program to improve Technical Specifications, action statements that require plant shutdown if an AOT time is exceeded are being developed.

The issue concerns a few systems, such as residual heat removal (RHR), standby service water (SSW), and auxiliary feedwater, that may be required to cool the plant during shutdown. Currently, action statements in Technical Specifications typically require that plants shut down when an AOT is exceeded, even though shutdown may require use of the system that is out-of-service for maintenance. The work has developed a decision-analysis method for comparing the risk impact of transferring the plant to shutdown versus the risk impact of continued power operation.

The method and trial application to RHR and SSW at a BWR-6 are being published this Spring. An equivalent method and trial application to a PWR will be completed in early 1994.

4 — Technical Specification Defenses Against Dependent Failures

Technical Specifications set surveillance requirements and AOTs in order to ensure the availability of a plant's safety systems. These safety systems are designed to achieve high availability through redundancy. Redundancy, however, can be defeated by dependent (e.g., common cause) failures. For example, the Davis-Besse loss of all feedwater in 1985 involved several valves stuck shut (dependent failures). Despite the importance of dependent failures, most Technical Specification requirements do not explicitly address and protect against dependent failures.

In support of this concern, a method and criteria are being developed for explicitly addressing dependent failures in setting STIs and AOTs. This method uses a NUREG-1150 PRA as the framework within which to model and evaluate the risk impact of postulated Technical Specification improvements. A recent AEOD analysis of industry-wide experience with dependent-failure events is used as a reality check to supplement the PRA. Possible improvements in Technical Specifications that might better defend against such dependent failures are being postulated.

The purpose is to determine whether simple changes in surveillance requirements and AOTs would substantially reduce the risk of operating reactors. The result will be an assessment of the effectiveness of this approach.

5 — Method for Monitoring Dependent Failures

This effort is a related project that supports AEOD trends and analysis of operational data, This project has developed a method for analyzing failure data to estimate the fraction of failures that are dependent failures. The method compares the distribution of observed times-between-failures with the distribution expected if the failures were independent. The difference reflects dependent failures. The method estimates the

fraction of dependent failures (e.g., a beta factor) and the actual safety system unavailability with this degree of dependency.

The methods development has been completed, and the report will be published in mid-1993. AEOD and RES are discussing whether additional work is warranted to make the software directly applicable to AEOD screening of data to help recognize dependent-failure events.

6 — Handbook

This task is developing a handbook of methods for evaluating the risk impact of Technical Specification requirements. The handbook will facilitate staff evaluation of licensee proposals for changes to Technical Specifications and for scheduling of AOTs for preventive maintenance. This handbook will also transfer research results to support NRR's Technical Specifications Branch.

The scope of the handbook includes reliability and risk based methods for evaluating: AOTs, use of AOTs for preventive maintenance, action statements requiring shutdown, STIs, defenses against common cause failures, and managing plant configurations. For each of these topics, the handbook will summarize useful analysis methods and data needs, will outline in common-sense terms the insights to be gained from a risk perspective, and will list a few references for more detailed information and alternative methods. Writing of the handbook is starting in March 1993. A draft will be circulated for staff review and comment in October 1993. The completed handbook will be available early in 1994.

These six programs are focused on developing methods for Technical Specification optimization. The methods developed, given that the limitations, boundary conditions, assumptions, uncertainties, data, and human performance issues associated with PRA are properly addressed, can provide assistance in determining the ground rules or restrictions that would be necessary to maintain the current level of safety while providing additional flexibility in the implementation of the regulations. In addition, there are other ongoing programs within RES that also utilize PRA, will provide necessary insights, and will provide assistance in addressing the above-mentioned concerns.

Technical Analysis of Proposed Changes to the South Texas Technical Specifications

Houston Lighting and Power, the licensee for the South Texas Nuclear Project (STNP), submitted a proposed amendment to its operating license. The Probabilistic Risk Analysis Branch is developing a framework for analysis and a technical basis for evaluating the proposed changes to AOTs and STIs for the STNP. The evaluation involves reviewing the system failure models and sequence level cut sets of the STNP PSA, establishing a

systematic risk profile for the base case three-train configuration of the STNP, obtaining the overall risk impact of the proposed changes in AOTs and STIs, and developing a framework that will support the bases for approval of the proposed changes in AOTs and STIs based on risk arguments.

Although this effort is not a formal program to develop "generic" methods for evaluating proposed Technical Specification changes, insights can be used for generic applications.

Individual Plant Examination Data Base

On November 23, 1988, Generic Letter 88-20 was issued requesting licensees to perform an Individual Plant Examination (IPE) with the general purpose of each licensee "to develop an appreciation of severe accident behavior, to understand the most likely severe accident sequences that could occur at its plant, to gain a more quantitative understanding of the overall probabilities of core damage and fission product releases, and (if necessary) to reduce the overall probabilities of core damage and fission product releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents" *[Ref. 4-16]*.

In support of this effort, an IPE data base has been developed, which catalogs the information provided in each licensee's IPE submittal. The type of information being input to the data base for each IPE includes the following:

- Plant information (e.g., reactor and containment type).
- Initiating event information (e.g., initiating event and its associated frequency).
- Accident sequence information (e.g., accident sequence description and associated frequency).
- System and component dependency information.
- Core damage frequency information.
- Plant damage state information.

The data base will allow users to gather information both by plant and across plants. For example, the data base will identify those plants where a certain issue such as loss of offsite power is a concern; will identify concerns for a group of plants such as identifying the dominant contributors for 3-loop westinghouse plants; will identify those plants where a system concern may exist such as identifying plants where diesel generators are dependent on instrument air. These are a few examples of the IPE data base.

The information currently being entered into the data base only includes IPE data. As part of the IPE effort, licensees were only required to examine internal initiators and internal flooding. NUREG-1407 *[Ref. 4-17]* provides the guidelines for the

IPE of external events. The data base will be expanded to include this information for each licensee.

Low Power and Shutdown PRA

PRAs have traditionally examined severe accidents only occurring at full-power operation. Analyses have indicated that severe accident occurring at low power and shutdown could be significant. A major program has been in progress to assess the frequencies and risks of accidents initiated during low-power and shutdown modes of operation for two nuclear power plants by performing detailed PRAs for the various operational modes. This effort also involves the development of new methods and will compare the assessed risk with those of an accident initiated during full-power operation.

The work involves examining the accidents initiated by internal events (including flooding and fire) as well as external events (e.g., earthquakes). Ultimately a full PRA (core damage frequency, fission product releases and consequences) will be completed.

PRA Working Group

In 1991, the EDO formed a working group of staff management (i.e., PRA Working Group) to "consider what improvements in methods and data analysis are possible and needed, the role of uncertainty analysis in different staff uses of PRA, if improvements are needed in the allocation of existing PRA staff, and the need for recruitment of more staff (or for identifying other means for supplementing staff resources)." *[Ref. 4-18]*

The objectives of the PRA Working Group are to develop guidance on consistent and appropriate uses of PRA within the NRC; to identify skills and experience necessary for each category of staff use; and to identify improvements in PRA methods and associated data necessary for each category of staff use. In support of these objectives, the Group has defined the scope of its work as follows:

- Ascertain present uses of PRA by the staff; future PRA uses that are not now well defined (e.g., possible transition to risk-based reactor regulation) are not included in the Group's scope of work.

- Review available or developing risk analysis documents and guides, and develop recommendations for improvement. Such improvements are the responsibility of the user organization, with oversight by the Working Group. It is not within the Group's scope to update or replace such guides although the group may make recommendations to update them.

- Assess staff skills and experience needed to appropriately apply PRA, including staff organizational considerations, if appropriate. While the skills and experience assessment is within the scope of the Group's work, the development and implementation of plans to change staffing levels, staff training, or organizational arrangements are the principal responsibility of the Office of Personnel and the affected offices, as part of the overall development and implementation of the agency's Human Resources Strategic Plan.

- Assess needed improvements in PRA techniques and data to support appropriate staff use of risk analysis. This assessment focuses on improvements needed for particular uses, rather than a broad assessment of needed improvements in risk analysis methods, and uses state-of-the-art risk studies such as NUREG-1150 as reference and resource material. The performance of any such improvements is the responsibility of the appropriate staff organization, not the Working Group.

It must be ensured that the current level of safety is maintained when using an integral analysis, such as PRA, to provide more flexibility in the regulations and in the implementation of the regulations. NRC-sponsored programs were inventoried in a first step to determine what types of general rules and restrictions would need to be imposed so that PRA can be used while maintaining the current level of safety. A summary of these PRA programs that could provide insights are provided in Table 4.9-2 below.

Table 4.9-2
Summary of NRC-Sponsored PRA Programs

RESPONSIBILITY	PROGRAMS	APPLICATION
AEOD/DSP/TPAB	Analysis of operational data to identify and provide quantitative content for safety issues	Data support to Technical Specification and graded QA optimization
AEOD/DSP/ROAB	Accident Sequence Precursor Program	Data support to Technical Specification and graded QA optimization
NRR/DORS/TSB	Technical Specification Improvement Program	Utilization of Technical Specification optimization
NRR/DSSA/PSAB	• Risk Evaluation of Safety Issues • Review of Licensee Requests for Exemption	Information support to Technical Specification and graded QA optimization
RES/DSR/HFB	• Procedures for Evaluating Technical Specifications • Technical Specification Requirements During Shutdown • Actions Statements That Require Shutdown • Technical Specifications Defenses Against Dependent Failures • Method for Monitoring Dependent Failures • Handbook of Methods for Evaluating the Risk Impact	Development of Technical Specification optimization methods
RES/DSIR/PRAB	Technical Analysis of Proposed Changes to the South Texas Technical Specification	Information support to Technical Specification and graded QA optimization
RES/DSIR/SAIB	Individual Plant Examination Data Base	Information support to Technical Specification and graded QA optimization
RES/DSIR/PRAB	Low Power and Shutdown PRA	Information support to Technical Specification and graded QA optimization
RES/DSIR/PRAB	PRA Working Group	Information support to Technical Specification and graded QA optimization

4.10 CONCLUSIONS

It is recommended that the utilization of PRA-based techniques in the regulatory process be characterized into three general classes, each having similar requirements in terms of the boundary conditions and assumptions used in the analysis, as well as similar requirements in terms of the depth and breath of the review that would be required by the NRC staff.

- ***Reliance on Quantitative Results From Multiple Plant-Specific PRAs*** — This category of risk-related regulatory actions would utilize the risk analyses to separate the potentially important components and systems from the unimportant. This relative importance would be from a PRA perspective based on core damage prevention, relying on both plant-specific studies as well as on compilations of the results of risk-based studies on similar plants.

  This type of usage could be based on the type of PRA modeling effort that is common in responses to the IPE Generic Letter 88-20 and the type of review currently being applied to IPE reviews by the NRC staff would likely suffice. Generic failure rate data could generally be employed and frequent updates of the PRA studies would not generally be required.

  Performance-based responses to the Maintenance Rule and risk-based approaches to graded quality assurance are possible examples of potential usage.

- ***Reliance on Single Plant-Specific PRA Quantitative Results in Selected Areas*** — Efforts of this type would require careful attention to the PRA methods and analyses in selected areas but would not involve close scrutiny of the entire plant risk analyses. It could be used to improve regulatory flexibility for a given component, or applied broadly to selected portions of the plant at the train level, without examining the detailed modeling at lower levels in the analytical trees.

  This type of application would also generally require average PRA modeling. Generic failure data would be sufficient in most instances, but it would need to be augmented with plant-specific data in those selected areas where heavy reliance was placed on the plant-specific results. For greater than one-time use, the PRA would have to be modified as necessary to reflect any changes in the current plant design and operational practices. This would likely require updating at least each refueling outage.

  Examples of this category would include optimization of selected Technical Specifications, evaluations of "unreviewed safety question" under 10 CFR 50.59,

and use of pre-calculated configuration management analyses to support extension of AOTs under certain circumstances.

- *Reliance on Numerical Results from Single Plant-Specific PRAs* — In this category, regulatory decisions would be based almost exclusively on the numerical PRA results. It would require a very comprehensive analytical effort since, in this type of application, apparently minor changes in assumptions or boundary conditions may significantly affect regulatory decisions.

  This type of application would require a level of detail that either stretches or exceeds the current state of the art. It would require a comprehensive plant-specific data analysis, and would require that the PRA be reviewed at a depth equivalent of that afforded to a final safety analysis report in the course of a Part 50 operating license review.

  An example of this type of usage would be the development of risk-based Technical Specifications requiring on-line updating of PRA models.

Candidate requirements have been developed for the boundary conditions and assumptions used in the analyses for each of the above classes in the preceding sections. These requirements should be regarded as candidate regulatory positions and can serve as a jumping off point for detailed discussions with the public and the regulated industry.

Beyond the technical recommendations, more specific recommendations regarding the nature of the regulatory environment needed to introduce the use of risk-based analyses in a broad fashion are offered.

- The current state of development and utilization of probabilistic techniques in the industry can support use of risk-based regulatory approaches at the present time. Several utilities have ongoing programs using risk methods and "living" probabilistic analyses to improve operations and maintain plant safety and efficiency that could be extended to the regulatory environment and provide increased licensee flexibility while maintaining or improving the safety envelope. It is recommended that the Commission elicit licensee proposals in this regard to support such an effort.

- The development by NRC of methods for optimizing Technical Specifications using risk-based techniques is nearing completion and, with publication of a handbook early in calendar year 1994, will provide a technical basis for judging the acceptability of risk-based approaches proposed by licensees. In addition, this handbook could serve as the point of departure for discussions between the NRC staff and the industry leading to industry-proposed guidance, suitably endorsed by

NRC. It is recommended that this handbook be published as a regulatory document, perhaps as a regulatory guide. This handbook can provide guidelines for methods or similar techniques that would be used in a pilot program in the near future, if there is industry interest in such an application.

- NRC programs and interests on the development and implementation of risk-based methods in regulation currently span multiple offices and organizations. An integral agency plan covering the research, development, implementation, and use of risk-based techniques in regulation is needed in maintaining a consistency of approach throughout the agency and in allocating scarce resources. This plan would also assist in the efficient use of the limited number of NRC staff with expertise in quantitative risk assessment.

- Possible risk-based regulatory approaches span a continuum from modest applications of conventional probabilistic methods to techniques for risk-based configuration control on a real-time basis. They represent an increasingly valuable complement to the present regulatory structure. The required resource commitments for both the licensee and NRC are likely to increase as more complex approaches are investigated; however, these more comprehensive approaches will also offer the most flexibility to the licensee while maintaining the safety envelope.

  A reasoned approach is recommended for the transition to the more risk-based approaches, testing benefits gained versus costs of implementing in pilot programs before proceeding to complete implementation industrywide. As indicated above, certain risk-based approaches can be implemented now, while others will be suitable for trial investigation in the near future. An investigation of the usages that are compatible with the current strengths and limitations of risk methods needs to be pursued in supporting a transition to PRA-based regulation.

- In effect, the NRC currently uses PRA insights to primarily add requirements to the industry. This utilization of PRA needs to be changed to allow PRA-based insights to reduce regulatory burden when it is shown that such a reduction does not reduce the safety envelope of the plant. Thresholds (e.g., NRC guidelines on content of submittals, acceptable PRA methods, and decision criteria) must, therefore, be established by the NRC for each PRA usage class (as described above) in concert with any industry-proposed pilot applications of these potential uses.

4.11 ACRONYMS, ABBREVIATIONS AND REFERENCES

4.11.1 Acronyms and Abbreviations

AEOD	Office of Analysis and Evaluation of Operational Data
AOT	Allowed Outage Time
ARI	Alternate Rod Insertion
ASP	Accident Sequence Precursor
ATWS	Anticipated Transient Without Scram
BOP	Balance of Plant
BWR	Boiling Water Reactor
CDP	Core Damage Probability
CDF	Core Damage Frequency
CRD	Control Rod Drive
EDO	Executive Director of Operations
EPRI	Electric Power Research Institute
HEP	Human Error Probability
HRA	Human Reliability Analysis
HVAC	Heating, Ventilating and Air Conditioning
IPE	Individual Plant Examination
LCO	Limiting Condition of Operation
LOCA	Loss of Coolant Accident
MSIV	Main Steam Isolation Valve
NEA	Nuclear Energy Agency
NRC	U.S. Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation
NSSS	Nuclear Steam Supply System
OECD	Organization for Economic Cooperation and Development
PRA	Probabilistic Risk Analysis
PWR	Pressurized Water Reactor
QA	Quality Assurance
RCIC	Reactor Core Isolation Cooling
RES	Office of Nuclear Regulatory Research
RHR	Residual Heat Removal
RPS	Reactor Protection System
SLC	Standby Liquid Control System
SSC	Structure, System, Component
SSW	Standby Service Water
STI	Surveillance Test Interval
STNP	South Texas Nuclear Plant
STS	Standard Technical Specification
TMI	Three Mile Island

4.11.2 References

[4-1] Organization for Economic Cooperation and Development, Third Workshop on Living-PSA Application, Hamburg, Germany, May 1992.

[4-2] U.S. Nuclear Regulatory Commission (USNRC), "Reactor Safety Study — An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

[4-3] Gesellschaft für Reaktorsicherheit (GRS) mbH, "Deutsche Risikostudie Kernkraftwerke: Eine Untersuchung zu dem durch Stöfälle in Kernkraftwerken verursachten Risiko," Hrsg.: Der Bundesminister für Forschung und Technologie Verlag TüV Rheinland, Köln, 1979.

[4-4] G.P. Marino (Ed.), "Nuclear Power Plant Severe Accident Research Plan," USNRC Report NUREG-0900, Revision 1, April 1986.

[4-5] J.G Kemeny et al., "Report of the President's Commission on the Accident at Three Mile Island," October 1979.

M. Rogovin et al., "Three Mile Island— Report to the Commissioners and to the Public," NUREG/CR-1250, Vol. 1, January 1980.

[4-6] USNRC, "Probabilistic Risk Assessment Reference Document," NUREG-1050, September 1984.

[4-7] USNRC, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," NUREG-1150, December 1990.

[4-8] N.J. Holloway (editor), "Probabilistic Safety Assessment in Nuclear Power Plant Management — A Report by a Group of Experts of the Committee on the Safety of Nuclear Installations," Nuclear Energy Agency, June 1989.

[4-9] USNRC, Memorandum to the Commission on Risk-Based Regulation, February 22, 1993.

[4-10] USNRC, Memorandum from James H. Sniezek, Deputy Executive Director for Nuclear Reactor Regulation and Regional Operations and Research, to Frank Gillespie, Group Leader, et. al., "Revised Charter for Regulatory Review Group," February 4, 1993.

[4-11] Sandstedt, Johan, "Living-PSA Application for a Swedish BWR with the Aid of Risk Spectrum," 3rd Workshop on Living-PSA Application, Hamburg, Germany, May 1992.

[4-12] Gunnar Johanson and Jan Holmberg, The Use of Living PSA in Safety Management, a Procedure Developed in the Nordic Project "Safety Evaluation, NKS/SIK-1", American Nuclear Society, Proceedings of Probabilistic Safety Assessment International Topical Meeting, PSA '93, Clearwater Beach, FL., January, 1993.

[4-13] W. B. Waddell, "Operational Experience of a Reliability Based Maintenance Strategy for the Control of Essential Post-Trip Cooling Plant in a Nuclear Power Station," The Institution of Mechanical Engineers - Power Industries Division, Seminar on Operating Reliability and Maintenance of Nuclear Power Plant, March 1990.

[4-14] USNRC, Memorandum from Eric S. Beckjord, Director Office of Nuclear Regulatory Research, to James M. Taylor, Executive Director for Operations, "Draft Report of the PRA Working Group," April 22, 1993.

[4-15] USNRC, "Improvements to Technical Specifications Surveillance Requirements," NUREG-1366, December 1992.

[4-16] USNRC, "Individual Plant Examination for Severe Accident Vulnerabilities — 10CFR§50.54(f)," Generic Letter No. 88-20, November 23, 1988.

[4-17] USNRC, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities," NUREG-1407, June 1991.

[4-18] USNRC, Letter from James M. Taylor, Executive Director for Operations, NRC, to David A. Ward, Chairman, ACRS, October 1, 1991.