NUREG-0460
Vol. 1

ANTICIPATED TRANSIENTS WITHOUT SCRAM FOR LIGHT WATER REACTORS

Staff Report

April 1978

Division of Systems Safety
U. S. Nuclear Regulatory Commission

A

NOTICE:

This report was issued by staff members of the Division of Systems Safety of the Nuclear Regulatory Commission. The statements contained in this report do not represent those of the Nuclear Regulatory Commission; the report has neither been approved nor disapproved by the Commission.

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy $6.50; Microfiche $3.00

The price of this document for requesters outside of the North American Continent can be obtained from the National Technical Information Service.

NUREG-0460
Vol. 1

ANTICIPATED TRANSIENTS WITHOUT SCRAM FOR LIGHT WATER REACTORS

Staff Report

Manuscript Completed: April 1978
Date Published: April 1978

Division of Systems Safety
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

Summary

The staff position on anticipated transients without scram (ATWS) has been a subject of continuing controversy since its publication in the "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors," WASH-1270, in 1973. The status of the implementation of this position, including the staff's review of each reactor manufacturer's analysis methods and results, was published in 1975 in a series of reports. These status reports were criticized by the nuclear industry as being excessively conservative.

This report is, in part, a response to the industry criticism and has the purpose of reviewing and evaluating the information now available on the subject of ATWS, in particular, the material developed subsequent to the publication of the status reports.

The significance of ATWS in the evaluation of reactor safety is that some ATWS events could result in melting of the reactor fuel and the release of a large amount of radioactive fission products. The questions in contention concern whether the probability of such events is great enough to justify their consideration and if so, what degree of protection is required.

Based on the occurrence of transients in currently operating nuclear power plants, the staff now concludes that transients that would result in serious consequences if accompanied by scram failure could be expected to occur in the future population of plants at a rate of five to eight per reactor-year. We also estimate that the probability of scram failure, based on nearly 700 reactor years of operating experience in foreign and domestic commercial power reactors with one observed potential scram failure, is in the range of 10^{-4} to 10^{-5} per demand. Thus, the expected frequency of ATWS events that could result in serious consequences is approximately 2×10^{-4} per reactor-year. We recommend that a safety objective of 10^{-6} unacceptable ATWS events per reactor-year is more appropriate, and therefore, that some corrective measures to reduce the probability or consequences of ATWS are required.

Although reducing the frequency of anticipated transients might be a means of reducing the probability of ATWS events, the difficulty in accomplishing the necessarily large reduction appears to make this approach impractical. Alternatively, improvement of the reliability of scram systems, particularly with regard to potential for common mode failures, by providing a second independent, separate and diverse scram system has been considered, but no completely acceptable design has been proposed. These considerations lead us to recommend that the provision of systems to mitigate the consequences of ATWS events, should they occur, is the most promising alternative for meeting the safety objective. This approach has been the principal subject of the development, analysis and staff review presented in this report.

We have developed a set of requirements for the design and performance of systems provided to reduce the consequences or probability of ATWS events. Acceptance criteria are stated that address radiological dose limits; reactor coolant system, fuel and containment integrity; core cooling capability; and mitigating system design and performance. Requirements are given for the analysis of postulated ATWS events. The requirements would provide reasonable assurance that, considering the frequency of ATWS events, the probability of additional system failures, and the uncertainty and variation in initial conditions and parameters, the acceptance criteria are not violated.

We have also considered the value and impact of these requirements. Estimates of the impact, primarily the costs associated with implementing the requirements, range from 1 to 43 million dollars per plant, depending on the type of plant and its stage of construction or operation. The direct value consists of the cost of the averted radiological and economic consequences. Estimates of the value range from approximately 1 to 47 million dollars per plant and are generally larger than the corresponding impact for any one type of design. The averted potential for shutdown of a number of operating reactors, should an ATWS with severe offsite consequences occur, has been estimated to translate into an additional indirect value ranging from 1.5 to 23 million dollars.

We have found that, considering the expected frequency of occurrence of transients, the reliability of current reactor scram systems necessary to meet the safety objectives has not been demonstrated and may well have not been attained. Therefore, we recommend that means of reducing the probability or consequences of ATWS events should be provided. Furthermore, we envision that the initiation of rulemaking to incorporate ATWS requirements in the Commission's regulations would fairly and clearly resolve the long standing uncertainty in the status of regulatory requirements in this area.

ANTICIPATED TRANSIENTS WITHOUT SCRAM

1. Introduction

This report presents the results of a recently completed review and evaluation by the NRC staff of the extensive information that has been developed over the past ten years on the subject of anticipated transient without scram (ATWS) events and the manner in which they should be considered in the design and safety evaluation of nuclear power plants. In September 1973, the then AEC regulatory staff published a "Technical Report on Anticipated Transients Without Scram" (WASH-1270) which enunciated the staff's position that certain design features should be required to reduce the probability and mitigate the consequences of such events. That report led to the development by the industry and the staff of substantial additional information regarding ATWS. The staff reviewed this information and the results of industry analyses of postulated ATWS events and in 1975 issued a series of status reports summarizing the staff's conclusion regarding acceptable methods of evaluating such postulated events and, based on these evaluations, identifying the equipment and design changes the staff believed to be required. These requirements were sharply criticized by the nuclear industry. Since the publication of the 1975 status reports, additional information relevant to ATWS has been developed by the industry, the staff and the Reactor Safety Study group.

In 1977 the Staff initiated an extensive re-evaluation of all the information available on the subject of ATWS, and in particular the material developed subsequent to publication of the staff status reports. This report is a statement of the current proposed position of the staff relative to ATWS and an exposition of the bases for this position.

The report consists of the main body of text and seventeen appendices. The main body discusses the significance of ATWS events to reactor safety and the probability that an ATWS event might occur. This probability is then compared with the desired safety objective. The possible and proposed means of attaining the desired safety objective are presented. The specific regulatory requirements proposed by the staff for use in determining the acceptability of ATWS evaluations are also discussed. Finally, the value and impact of these proposed requirements are discussed.

The appendices provide additional more detailed information on particular subjects relating to ATWS. Appendix I is a bibliography of sources of information on ATWS. Appendix II discusses the subject of scram system reliability in general terms and Appendix III provides information on the reliability of control rods and drives in particular. The staff's proposed licensing requirements, specific guidance applicable to consideration of steam generator tube failures, and methods for calculating radiological doses are provided in Appendices IV, V and VI, respectively. A probabilistic study of ATWS consequences is provided in Appendix VII. Two

particularly significant parameters for PWRs, the moderator temperature coefficient of reactivity and the safety valve discharge flow rate, are discussed in Appendices VIII and IX, respectively. Appendix X discusses the treatment of ATWS events in the Reactor Safety Study (WASH-1400). Appendix XI discusses the bases for the ATWS fuel damage criteria. The details of the value-impact evaluation are given in Appendix XII. The responses to various differing staff views on the staff position are given in Appendix XIII. Evaluations of each reactor manufacturer's designs are given in Appendices XIV, XV, XVI and XVII.

2. Background

The manner in which anticipated transients without scram (ATWS) events must be considered in the design and safety evaluation of nuclear power plants has been a subject of extensive and continuing controversy among members of the nuclear industry and the regulatory staff. The controversy stems principally from differing perceptions of the potential extent and probability of serious consequences resulting from such events. Initial discussions of ATWS began as early as 1969, when a consultant to the Advisory Committee on Reactor Safeguards (ACRS) pointed out the possibility of a safety problem if common mode failures could reduce the reliability of protection systems in such a way that the system might not function properly in the event of an anticipated transient. As a result of this expressed concern and ensuing discussions among the staff and ACRS, the

staff requested the reactor manufacturers to prepare studies of the probability and consequences of a failure of the control rods to insert following an anticipated transient. These studies concluded that the probability of such an event was negligibly low, but could result in failure of the reactor vessel or piping due to overpressure. Based on the review of these studies and other material, in September 1973 the staff published the "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors" (WASH-1270) containing its position on ATWS. The ACRS had agreed with the position in April 1973.

The thrust of the staff position in WASH-1270 was that, considering common mode failures, the needed reliability of reactor shutdown systems was difficult to verify and, since larger safety margins were appropriate as increasing numbers of reactors were built and operated, ATWS events should be considered in the safety analysis of nuclear reactors. For future plants, for which applications for construction permits would be docketed after October 1, 1976, the staff concluded that an additional separate and diverse reactivity shutdown system should be required. For plants with construction permit applications docketed after early 1968 but before October 1, 1976, the staff concluded that any necessary design changes should be made to assure that the consequences of anticipated transients would be acceptable in the event of a postulated failure to scram. Subsequently, as a result of further consideration, the staff and the ACRS concluded that the requirement for an additional shutdown system in future

plants was not necessary in order to achieve the desired safety objective and that the requirement to mitigate the consequences of ATWS events applied to current plants would also suffice for new plants.

After WASH-1270 was issued, reactor manufacturers, in conjunction with the staff, began to develop acceptable methods of performing analyses of ATWS events. A draft ANSI standard, N661, was written, which outlined general guidelines for the analysis of ATWS events in PWRs. In October 1974 the vendors submitted reports describing the analysis of ATWS events for their reactor designs. The staff reviewed these reports, and after requesting and receiving additional information, issued status reports that provided the results of this review. The staff found the vendor analysis methods to be generally acceptable except for the treatment of system failures and some system parameters. Subsequently, in mid-1976, applicants were requested to perform analyses for their plants using the methods developed by the vendors and modified as indicated in the staff status reports. These requests and the status reports led to substantial criticisms from applicants, reactor vendors and industry groups, principally to the effect that the staff requirements are unnecessary, or at best overly conservative. The basic industry position is that the high reliability of reactor protection systems makes the probability of an ATWS event negligibly small and not worthy of consideration as a design basis. It is also maintained that if consideration of ATWS events is necessary in reactor safety evaluations, the requirements expressed in the staff status reports are excessively

conservative. Such views were expressed in letters from individual applicants, and industry groups including AIF and EPRI. Three of the vendors submitted additional reports in support of such arguments and provided evaluations of the reliability of their reactor protection systems, particularly with respect to the potential for common mode failures in the control rod drive mechanisms. EPRI also submitted a set of reports containing a detailed statistical analysis of scram system failure and the frequency of anticipated transients.

One of the primary points made by these critics was that the results of the Reactor Safety Study, WASH-1400, which had been published in 1975 and therefore was not available for consideration in the previous evaluations of ATWS, apparently showed that ATWS events were not significant contributors to the overall risk from nuclear power plants. The industry further contended that the cost of the changes required by the staff position to mitigate ATWS events would be significant and not justified. In response to these criticisms the Director of NRR requested that the vendors submit their estimates of the cost of these changes.

This report summarizes the staff's review and evaluation of all of the information currently available on the subject of ATWS, and in particular the material submitted subsequent to the previous staff status reports and the industry criticisms. The report is a statement of the current position of the staff regarding the treatment of ATWS events in the safety evaluation

of nuclear power plants and an exposition of the bases for this position. Detailed discussions of the bases for the requirements are presented in the appendices.

3. Significance of ATWS Events

The significance of ATWS events in the evaluation of reactor safety and the basis for the continuing discussions relating to the need for their consideration in reactor designs involve the extent to which ATWS events could be a major contributor to the overall risk from the operation of nuclear power plants. The principal risk that reactors present arises from the potential for the large release of radioactive fission products if the fuel in the reactor core were to melt. Some anticipated transients if not controlled by scramming the rods or by the actions of other systems, could result in melting of the core.

Nuclear power plants, in common with other types of power plants, have control systems to maintain system parameters within normal limits. However, these control systems are effective over a limited range. Additional systems are provided to protect the plant in the event parameters exceed the normal limits. In a nuclear reactor this protection system automatically initiates other systems, primarily the control rods, to maintain acceptable system conditions following anticipated transients.

Transients that isolate the reactor from the normal cooling systems have the greatest likelihood of occurring and for most reactors the severest potential consequences if the scram system fails. Closure of the valves in the main steam or feedwater lines, or tripping of the feedwater or condensate pumps can isolate the reactor and interrupt the transfer of the heat generated in the core. Real or spurious signals indicating off-normal plant conditions, or external events such as a loss of offsite power may initiate the closing of valves and tripping of pumps. Normally the action of the protection system to scram the rods limits the consequences of these events to moderate transient increases in system pressure and core power. The power of the core is also quickly reduced to the level where the standby systems can then maintain core cooling. However, if the control rods fail to insert following transients that isolate the reactor from the normal cooling systems, the resulting pressure rise can be large enough to threaten the integrity of the reactor coolant pressure boundary, which includes the reactor pressure vessel and connected piping, and the operability of valves in the standby cooling systems, which would be eventually required to cool the core. Unless core power and system pressure are reduced to within the capacities of the standby cooling and makeup systems within a few minutes the core can be uncovered and melting can occur. Of course the severity of such ATWS events varies with the design of the reactor and can be modified by the action of other systems.

The argument for the need to consider ATWS events in reactor safety evaluations, first presented in WASH-1270, is not that reactor protection and reactivity shutdown systems are unreliable, but that considering the relatively high rate at which they are challenged by anticipated transients, the stringent safety goals that are specified, and the increasing number of nuclear power plants, an extraordinarily high reliability is required. The practicality of attaining and demonstrating the required high reliability in a single system subject to multiple failures due to a single cause was questioned. The possibility of such common mode failures, that have been observed in reactor protection and other systems, raised questions as to the validity of the assumption of independent failures that was the basis of previous statistical analyses used to demonstrate extremely small protection system unreliabilities and led to the staff conclusion that ATWS events must be considered.

4. Occurrence of ATWS Events

The frequency of ATWS events is the product of the frequency of anticipated transients and the conditional probability of scram failure given the occurrence of a transient. The probability of failure of the reactor protection system is the sum of two components. Based on experience to date, the dominant component is the probability that the reactor protection system fails before the transient as an independent event and then remains undetected and therefore uncorrected until tested or challenged. The

second component is the probability of a scram failure caused by the transient. Because reactor protection systems are carefully designed and tested to function under conditions more severe than those imposed by anticipated transients, the probability of scram failure directly resulting from an anticipated transient is negligibly small compared with the probability of independent failures. However, some events, which are not anticipated transients, result in conditions that approach or exceed the reactor protection system design bases. In these events, the probability of scram failure directly resulting from the event may be significant. Because the frequency of these events is so low, the combined frequency of the event and the probability of resultant failure of the protection system has been neglected in this evaluation.

4.1 Frequency of Transients

The frequency of occurrence of transients depends on many factors, such as the type of transient and the age, operating mode and location of the plant. In the statistical analysis of ATWS presented in WASH-1270, these differences were ignored and transients requiring scram were assumed to occur once per reactor-year. This was based on the information available at that time and now appears to be an underestimate. Nevertheless, even using this low estimate of the frequency of anticipated transients the staff concluded in WASH-1270 that reactor protection system reliability was insufficient to achieve the desired safety goal.

Better estimates of the frequency of anticipated transients have been made since the publication of WASH-1270. Estimates of this frequency were made and reported in the Reactor Safety Study (WASH-1400). These estimates were based on the operating experience of plants of the types studied. For the BWR, the Reactor Safety Study estimated that transients, primarily turbine trips, requiring reactor shutdown occurred approximately ten times per year. For the PWR, the estimated rate was also ten per year with the majority being turbine trips, but with some feedwater trips.

Recently the Electric Power Research Institute (EPRI) has made a more comprehensive survey of transients at operating reactors. The results of this survey show the variation of the frequency of transients with plant age. For older plants, the rate was nearly 20 per year early in plant life and decreased to approximately six per year later in plant life. EPRI also estimated that one-half to three-quarters of the transients would not have resulted in significant consequences even if control rod insertion had failed to occur. EPRI also assumed that improvements in the operation of the plants would continue to reduce the rate. Based on this, EPRI reported that an occurrence frequency of approximately three significant transients per reactor year would be expected in the future.

The data collected by EPRI are the most extensive data on plant transients available to the staff and provide the best basis for estimating the frequency of anticipated transients in nuclear power plants. Because this

experience is from a population of relatively young reactors which are early versions of evolving designs, the data cannot be used directly to estimate the rate of occurrence of transients in the future population of old and young reactors which reflect various stages in the design evolution. The data do indicate that the initially high rate of transients experienced by plants newly placed in service decreases as the plants mature. This is in general agreement with the operating experience at many other types of plants, including fossil-fuel power plants. However, since few of the currently operating nuclear power plants have been in service for more than six years, the data do not reveal whether the frequency of occurrence of transients will increase again as the plants near the end of their design life, as has also been generally experienced in other types of plants.

The data also indicate that as new designs are introduced, the frequency of occurrence of transients can be higher than in the plants of older designs. Although changes in design may be less frequent in the future as a result of standardization, reactors of the latest design are still under construction. Therefore reactors with new designs will continue to enter the population of operating reactors for at least five more years.

Based on the data provided in the EPRI study, the rate of occurrence of anticipated transients at both BWRs and PWRs has averaged approximately ten per reactor-year over the first five years of operation. The staff

believes this represents actual experience to date and is more appropriate than the extrapolations of the effect of opposing factors of uncertain magnitude. Of these ten transients per year, the data indicate that on the average only five per reactor-year at PWRs and eight per reactor-year at BWRs would have resulted in significant consequences had scram not occurred and need be considered in ATWS evaluations. Since the difference between these estimated rates is within the error of the estimates, the single value of six per reactor-year is used in subsequent discussions.

4.2 Scram Reliability

The estimation of the failure rate of reactor protection systems from experience data is difficult because the systems are highly reliable. Although many components and subsystem failures and a variety of design, manufacturing and operating errors have occurred, these types of systems are designed to be redundant and capable of performing their safety function even with the occurrence of single failures. Failures of the common mode type that could cause all or most of the control rods to fail to insert have been rare events.

Two methods have been used to estimate scram system reliability. The "system experience method" evaluates the reliability of the system as a whole based on the actual operating experience of the system without necessarily identifying the specific modes of failure. The "synthesis

method" uses fault and event trees to identify failure paths and individual component fai'ure rate data to quantify the estimate of reliability. The system experience method was used by the staff in WASH-1270, and the synthesis method was used by the Reactor Safety Study. EPRI has used both methods in their series of reports on scram reliability. An expanded discussion of scram reliability is contained in Appendix II.

The data available for the system experience method is limited, since the actual operating experience with commercial power reactor scram systems is limited. Only approximately 150 central station nuclear power plants are in operation worldwide. Fewer than half of these plants are in the U.S. The experience of foreign power reactors has varying applicabil:ty to the estimation of the reliability of U.S. reactor scram systems. Most of the German, Spanish, Japanese, and Italian power reactors and their scram systems resemble domestic design quite closely, whereas the French and British systems are different. Design details and operating experience for USSR scram systems are not known to the staff. It therefore seems most appropriate to use the U.S. experience and the portion of foreign experience from reactors similar to U.S. designs as the relevant data base.

Thus, our knowledge is limited to an approximately 700 reactor-year operating history of commercial light water power reactors. Although these plants do not have identical reactor protection systems and do not operate

under identical conditions, the similarities in design, construction and operation justify, in our opinion, treating all of these plants as part of the same population for the purpose of statistical analysis.

The current staff estimate excludes the experience with an equally large, if not larger, population of research, test, production, merchant and naval marine propulsion and other military reactors. Although we believe that exclusion of this experience is appropriate, as is explained shortly, its omission does not affect the conclusion that the necessary reliability of reactivity shutdown systems has not and cannot be demonstrated solely by operating experience. Even if all of these reactors are included, the operating experience necessary to demonstrate the necessarily high reliability cannot be obtained in a practical period of time. For example, 58,000 reactor-years of failure free operating experience are required to demonstrate an unreliability of 10^{-6} per demand with a confidence level of 50% if monthly testing is assumed. If a higher confidence level, say 95%, is desired, failure free operating experience over four times as long, some 250,000 reactor-years, is necessary.

Furthermore, actual experience is not failure free; failures to scram have occurred in some of these other types of reactors. One in particular, the failure at the N-reactor in Hanford, Washington, is discussed in WASH-1270 and included in the estimate of power reactor scram system reliability presented there. None of these failures is included in the current staff

estimate since we now believe that the scram systems in these types of reactors are not representative of current power reactor designs. At most only a few reactors of each design were built and in many cases the scram systems were one-of-a-kind designs. These scram systems did not have the same degree of design review, testing and actual operating experience that is reflected in the scram systems of current power reactors.

Operation of naval propulsion reactors has resulted in a very large body of experience, that we now exclude from the basis of our estimate of reactivity shutdown system reliability, although it was also included in the WASH-1270 analysis. Its inclusion in the WASH-1270 analysis was appropriate to the conclusion of that report, which was that even with the liberal inclusion of a large amount of operating experience assumed to be failure free, the required reliability still could not be demonstrated. The staff reviewed the design and operation of naval reactor scram systems with naval reactor personnel to assess the applicability to commercial reactors. The design objectives and operating conditions of naval reactors are different from those of commercial power reactors. Although some portions of the reactor protection systems in naval reactors are similar to those of commercial power reactors, other portions are significantly different. However, the differences are no greater than differences among the designs of the various reactor manufacturers and would not by this reason alone justify excluding the naval data. EPRI has attempted to infer the naval reactor experience, "based on discussion with people

familiar with their practice," but based on our review we believe that the EPRI interpretation of this experience is incorrect for several reasons. Since this classified information cannot be openly evaluated and can therefore be subject to misapplication, we do not believe that it should be used directly to estimate commercial reactor scram reliability. However, based on the staff review it is clear that in any event inclusion of the naval data would not change the staff conclusion regarding scram reliability.

The one scram system failure that we do include in our estimate of reactor protection system reliability is the failure of all of the scram relays in the Kahl boiling water reactor protection system and discovered during a periodic surveillance test. Although this reactor was constructed in Germany, the design and components of the scram system were provided by a U.S. vendor, General Electric. Furthermore, the same common failure mode was also observed during preoperational testing of the boiling water reactor at Monticello, Minnesota. Since the failure at Monticello was only partial and was detected prior to operation through the normal testing procedures, it is not included in the reliability estimate, but it does indicate that this type of failure could have occurred during operation of a U.S. reactor and was not unique to a foreign reactor.

The failure at Kahl is worth further discussion since it is illustrative of the general problem of common mode failures in reactor protection systems. The Kahl failure occurred after the original scram relays were

replaced by a complete new set. As required by quality assurance procedures, the system including the replacement relays was tested before the reactor returned to operation. The potential for failure was not detected until the relays had been in operation for approximately two weeks, because the test procedure was not designed to detect the potential for the type of failure that did occur. The long period of preoperational check-out and testing at Monticello produced the conditions necessary for failure and later testing revealed it before operation. Although testing is often cited as an effective means of increasing the system reliability, its effectiveness is often limited by the inability of designers to recognize all potential failure modes in developing test procedures.

The Kahl failure was the result of the inadequate heat curing of a protective coating during the manufacture of the relays. The relays were operated in a so-called "fail-safe" mode, where the contacts were held closed during normal operation by the continuously energized coils. Interruption of power to the coils as a result of either a scram signal or failure of the power supply would open the relays and activate the protection system. During operation, heat generated in the coils hardened the coating and caused the contact points to stick closed. Interruption of power to the coils in this condition would not initiate scram. Because all the relays were of the same manufacture and all operated in the same power-on mode, the failure was common to all. If some diversity in design, manufacture or operation had been provided this failure most probably would not have

occurred. Although absolute protection is not attainable, a considerable measure of protection against common mode failures can be provided by diversity in such things as design, manufacture and operation. Even though diversity may be difficult to define precisely or to quantify, the staff believes that it can be a means of decreasing the vulnerability to common mode failures.

The Kahl failure also illustrates the difficulty in identifying all potential common mode failures in a design. This type of relay had a long and successful operating history. However, the first link in the chain of events leading to eventual failure appeared to be the relocation of the plant that manufactured the relay. Possibly the process for coating and curing the relay was not specified in sufficient detail. Slight but significant differences in the process of curing the coated relays were introduced at the new plant. Since reactor protection system designs are carefully reviewed for common modes of failures, it is not unexpected that the one that did occur was subtle.

The process of manufacturing these types of relays has been revised so that this particular type of failure is less likely to occur again. This will be generally true of those potential common mode failures that are recognized. EPRI, in its statistical analyses of scram system reliability, excludes the scram relay failures at Kahl for this reason, which they call "rectifiability." Although correction of failure modes that have been

experienced obviously increases reliability, the degree to which it does this is not readily determined. For systems with relatively low reliability, failures will occur relatively quickly and be rectified, thus significantly improving the reliability of the system. However, for highly reliable systems such as reactor protection systems, only a small fraction of the potential failure modes will occur during any reasonable period of observation. Correction of these few modes may not increase the already high system reliability significantly. Thus, for example, if there are ten modes of failure each of which has a rate of occurrence of once per 10,000 reactor-years, at least one failure would be expected to occur before 1000 reactor-years of operation had been experienced. Correcting this mode of failure only improves the total failure rate by ten percent, which is not a significant improvement. Because the number of potential common modes of failure in reactor protection systems is unknown, the degree to which reliability is increased by correcting observed failures cannot be determined.

Three estimates of scram system reliability based on differing evaluations of this system experience are summarized in Table I. The derivations of these estimates are discussed in Appendix II.

Table I

Scram Failure Probability per Demand
(Assuming Monthly Testing)

Confidence Level	EPRI Part I	WASH-1270	Current Staff Estimate
50%	3.0×10^{-6}	6.9×10^{-5}	1.1×10^{-4}
95%	1.3×10^{-5}	1.6×10^{-4}	3.0×10^{-4}

The EPRI estimate is reported in Part I of their five volume report entitled, "ATWS: A Reappraisal." The ERPI estimate is based on the assumption that scram failure is related to demand and that a constant failure probability model best represents this relationship. The estimate assumes no failures in over approximately 110,000 scram system demands in foreign and domestic power reactors and naval reactors.

The EPRI estimate does not include the failure at the Kahl reactor discussed previously, because of "the concept of rectifiability." The staff believes that although some learning effect may be present, it is not significant enough to justify ignoring the Kahl failure. Experience shows that causes of failures are not always correctly identified and corrective measures are not always successful. Furthermore, as previously discussed, the elimination of one failure mode may not significantly reduce the failure rate if it is the result of multiple modes of failure each with a low failure rate.

The naval reactor experience, estimated by EPRI to be approximately 75,000 scrams, is a large fraction of experience used in the EPRI estimate. As discussed previously, the staff believes the EPRI interpretation of the Navy data is incorrect for several reasons. Since the data are classified and cannot be independently evaluated, the staff believes they should not be included.

The earlier staff estimate reported in WASH-1270 is based on the assumption that scram failures will occur at a uniform rate independent of the demands on the system and remain undetected until a test or other demand occurs. Based on the failures to date the staff continues to believe that this constant failure rate model represents actual experience more realistically than the EPRI model.

The WASH-1270 estimate assumes two failures in approximately 1600 reactor-years of U.S. and foreign power reactor, merchant and naval propulsion and other military reactor experience. The power reactor experience included a failure at the N-reactor, which is a dual purpose power and production reactor. As discussed previously, the current estimate does not include this event because the design of the N-reactor scram system is not typical of power reactor designs. The foreign reactor experience included the Kahl failure which, as discussed above, the staff still believes to be applicable to U.S. power reactors. The naval reactor experience, estimated

to be approximately 1000 reactor-years, is a large portion of the total experience data base for the WASH-1270 estimate.

Our current estimate is based on the U.S. and foreign light water power reactor experience to date, which is nearly 700 reactor-years and includes the operating period after 1973 when WASH-1270 was published. The estimate is based on the constant failure rate model. Only the one failure at Kahl is considered applicable to current U.S. power reactor designs.

The one observed common mode failure of a commercial power reactor protection system occurred in the electrical portion of the system. To date, none of the rod or drive failure events has come anywhere close to constituting a scram failure. The experience with rod failures is presented in Appendix III. The question naturally arises as to whether the electrical and mechanical portions of the scram systems have significantly different scram failure rates. The system experience estimates of the probability of the electrical portion of the scram system would result in the same values as presented in Table I for the scram system as a whole. Synthesis methods have been used, principally by the vendors, to estimate the probability of failure of portions of the system. These estimates either do not include common mode failures, or adopt arbitrary methods of including their effect. Consequently, many of these analyses result in very small estimates of failure probability. The staff believes that common mode failures are likely to dominate reactor protection system unreliability,

and the staff estimates do not weigh heavily the results of synthesis calculations.

It is possible that failures in the mechanical portion of reactor protection systems, that is, the drive mechanisms or the rods themselves, are much less likely than failures of the electrical portion. Whether a greater faith in the reliability of mechanical systems is justified has been a central issue in the debate over ATWS. The analyses of Appendix II show that a large number of rods must fail to insert to constitute a scram failure. The number of rods that must fail to constitute a scram failure depends upon several factors including the distribution of the rods within the core, the time in the fuel cycle, and power and xenon levels. Insufficient analyses have been performed to permit a precise and comprehensive statement to be made. However, based on available information, insertion of approximately 20% of the rods would be expected to limit system pressures to within acceptable limits, and insertion of approximately 50% of the rods would almost certainly do so. Since the probability of an individual rod to insert is low, multiple concurrent independent failures are highly improbable and constitute a negligible contribution to the overall probability of scram failures. Common mode failures are believed to be the most likely cause of multiple failures of rods.

The vendors have vigorously defended the reliability of the mechanical portions of their scram system, i.e., the control rod drive mechanisms.

They have taken the position, in various forms, that if the probability of an ATWS with existing scram systems is high enough to be of safety significance, it is due to the potential for an electrical common mode failure, and not to a potential for mechanical common mode failure in the mechanisms.

Three vendors have submitted reports documenting the engineering bases for their contention that control rod drive mechanisms are extremely resistant to rapidly initiated common mode failures that could result in an ATWS. The substance of these reports consists of failure mode analyses based on consideration of design, manufacturing and service-related factors which could conceivably have an effect on the capability of a particular mechanism to perform or fail to perform its design function.

In the course of these analyses, failures are postulated for each of the mechanism parts and the effect of each failure on the capability of the mechanism to scram is evaluated. Additionally, the effect of each such postulated failure on the scram function of other mechanisms is considered.

The conclusions reached by the vendors may be characterized as follows:

> The probability that all or a sufficiently large number of mechanisms would fail at exactly the same moment or within a very short time, while still performing to technical specification surveillance requirements and going undetected during periodic test and maintenance,

is extremely low. Taking into consideration the level to which the mechanisms are designed and manufactured; the testing which is performed prior to service and also after maintenance; and the variability in the parameters, such as mechanical properties and dimensional tolerances, that affect failure rates, the time to failure for the most credible modes will differ from one mechanism to the other.

Review of data in Appendix III gives no positive indication, given present manufacturing and reactor operational practices, that the required short time undetected mechanical degradation phenomena which would prevent a sufficiently large number of rods from entering the core would be of concern. The majority of the review of the reliability of the mechanical portions of the scram system has been concentrated on the control rod drive mechanisms, up until this time. This occurred because of guidelines initially established by the AEC in WASH-1270. Nevertheless, it is considered likely that control rods are as reliable as the mechanisms.

Whether some credit for the necessarily more subjective studies should be granted has been an issue in the ATWS debate. The amount of credit to be given has been an item of debate within the staff as well as between the staff and the industry. (For more details on this debate, see item 3.2.1 in Appendix XIII.) Acceptance of the mechanical portions of the scram systems as having sufficient reliability results in the conclusions that adequate protection against ATWS can and presumably should be accomplished

by improving the electrical portion of the scram systems, i.e., diverse reactor trip system.

The estimation of the failure rate of the control rod and drive system reduces to the estimation of the probability of a common mode failure in the system. However, all of the statistical analyses made in an attempt to estimate this rate suffer from the same difficulty; no failures of the rods or drives that have significantly affected the performance of the scram system have occurred. While the data do not exclude unreliabilities of the mechanical portion of the scram system in the order of 10^{-7}, the data are also consistent with much higher failure probabilities in the 10^{-4} to 10^{-5} range. At best, these statistical analyses can only show the bounds within which the reliability of the rods and drives probably fall. Although only the failure to insert many rods is of consequence, the staff has not found an acceptable quantitative prediction of the probability of common mode failure of different number of rods. The failure mode studies that have been made in an attempt to evaluate the reliability of the drive mechanisms are also necessarily imperfect. First, there is no method of estimating the rate at which those common mode failures that have been identified in the studies might occur. Second, there is no assurance that all of the potential modes have been identified. Paradoxically, these highly reliable systems are more troublesome to the statistical analyst

than less reliable systems for which failure data are available to make reliability estimates.

The staff believes that its current estimate of unreliability is appropriate for the electrical portion of the scram system, but recognizes that the lack of observed control rod or drive failures may make the estimate less applicable to the mechanical portion of the scram system. The vendor common mode failure studies provide some increased confidence in the reliability of drive mechanisms, but do little toward quantifying the reliability. The upper bound of the unreliabilities of the two portions of the scram system, assuming one failure in the electrical portion and no failures in the mechanical portion, differ by approximately a factor of two. This is not a significant difference considering the uncertainty of both estimates. Therefore, for the purposes of considering requirements for protection against ATWS events, the staff has adopted the position that the control rod drive system unreliabilty is approximately equivalent to that of the electrical portion of the protection system.

Based on the available data, the staff concludes that a probability of undetected scram system failure of 10^{-5} to 10^{-4} per demand should be used. In assessing the additional requirements that might be necessary in order to meet the staff safety objective for ATWS events, we have used a value of 3×10^{-5} per demand for this probability, which includes some allowance for the improvement in future reactor protection systems compared with the

systems used to derive the estimate. This value is not much different from that estimated in WASH-1270 and only a factor of five greater than the EPRI estimate, when that is corrected for a factor of two error in the EPRI application of the constant failure probability model. A more detailed discussion of these estimates is provided in Appendix II.

4.3 Probability of ATWS Events

As discussed in Section 4.1, the staff concludes that anticipated transients that would result in significant consequences if not controlled by a reactor scram would be expected to occur at a rate of approximately six per reactor-year. Since the difference between the estimated rates for PWRs and BWRs is within the accuracy of the estimates, it is neglected. As discussed in Section 4.2, the staff estimates that the probability of the rods failing to insert when called upon is approximately 3×10^{-5} per demand, again neglecting the difference between PWRs and BWRs. Based on these estimates the staff concludes that the frequency of an anticipated transient occurring with the subsequent failure of the rods to insert resulting in significant consequences is about 2×10^{-4} per reactor-year.

5. Probability Objective

The specification of safety objectives involves the exercise of subjective judgments that are properly societal decisions. To date, the specification

of safety goals for nuclear power plants in federal legislation has been limited to the general direction "to protect health and to minimize the danger to life or property...". Accordingly, specific safety requirements in the Commission's regulations have been based largely on qualitative evaluations of the possible hazards. Accidents, including the initiating event and the sequence of events that was assumed to follow, have been evaluated assuming a set of conditions that bounded or at least conservatively represented, the possible conditions. The reliability of the required safety systems was indirectly specified by requiring systems that were designed, manufactured, inspected, installed, operated and tested to specified and approved codes, standards, guides and procedures. In addition, these systems were required to incorporate appropriate independence, redundancy, protection against single failures and in some cases diversity.

This general procedure provides a workable method of applying safety requirements whose primary merit is its simplicity. Its most criticized shortcoming is the additional costs that may result if unnecessary conservatism is included in the design of safety systems. However, the perceived conservatism of the approach can be exaggerated if attention is directed only to the low probability of the individual bounding event being evaluated, without recognizing that the aggregate probability of all such accident sequences may be much larger.

The choice of the design basis accidents to be evaluated in the design of nuclear power plants involves some notion of the probability of their occurrence and is the basis for excluding more severe, but highly unlikely accidents from the design basis. As safety designs evolve and as the technology of safety evaluation is further developed, more sophisticated methods become feasible and desirable. Better methods may, by providing quantitative assessments of risk and thereby allowing efforts to be directed towards areas of higher risk, provide safer designs at less cost. Since it is clear that all conceivable events need not, and should not, be protected against, the question becomes one of where to draw the line. If probabilistic methods are to be used in deciding which events should be considered, some numerical objective is needed. Although its genesis is unclear, an accident rate of once in a million reactor-years has been widely used as a safety objective and some events have been evaluated against this objective.

In its 1973 report on ATWS (WASH-1270) the staff adopted an objective of 10^{-6} unacceptable events per reactor-year, but allocated only one tenth of that objective to ATWS events. In a 1974 study (WASH-1318), the staff concluded that the upper bound of the probability of the occurrence of a disruptive failure of a reactor pressure vessel is in the range of 10^{-6} to 10^{-7} per vessel year. The staff further concluded that this result supported the prior decision, that unless special circumstances were present, the failure of reactor pressure vessels need not be a design

basis event. In 1975 the staff published the Standard Review Plan. Section 2.2.3 of the plan states that events external to a nuclear power plant (such as explosions on nearby transportation routes), that could result in potential exposures of the 10 CFR Part 100 guidelines, need not be considered in the design of a plant if the probability of their occurring can be conservatively estimated to be approximately 10^{-6} per year or less or can be realistically estimated to be approximately 10^{-7} per year or less.

The Reactor Safety Study (RSS), published in 1975, provided the first comprehensive estimates of the overall risk resulting from the operation of nuclear reactors. The purpose of the study was to make a realistic estimate of the probability and consequences of accidents at nuclear power plants. The study did not attempt to define acceptable safety objectives or other regulatory requirements. Although the results of the study are not a basis for licensing, they have been compared with the safety objectives, either explicit or implicit, actually used in the safety evaluation of nuclear power plants. In general, the results indicate that the probability of the dominant contributor to risk (core melt) in the plants studied is about 5×10^{-5} per reactor-year. However, only about two percent of the core-melt events were reported to result in any early fatalities, although Part 100 exposure guidelines were calculated to be exceeded in most cases. Since the RSS results presented are in terms of integrated dose to the public and the licensing requirements are expressed

in terms of the maximum offsite dose at the site boundary, a direct comparison is not possible.

The RSS does provide a perspective on the risk to an individual member of the public from nuclear reactors relative to other accidents. Based on the RSS results, the probability of an individual being killed as an early result of an accident at a nuclear power plant is very small compared to the probability of being killed from other causes. The nuclear risk is also less than the probability of a person on the ground being killed by aircraft crashes, which is representative of recognized involuntarily imposed hazards.

However, this RSS estimate has not been uncritically accepted. Some have criticized this comparison as incorrectly excluding later deaths due to accident radiation-induced cancer. The number of later deaths due to the delayed effects of other accidents has not been estimated, thus making a direct comparison difficult. If all delayed deaths are conservatively included in the risk due to reactor accidents, but not in the non-nuclear risk, the risk due to reactor accidents is still only a small fraction of the overall risk due to all non-nuclear accidents and slightly lower than the risk to people on the ground from aircraft crashes.

Although the results of the RSS may not be sufficient justification to accept current levels of reactor safety as adequate, the regulatory staff

takes support from these comparisons that the application of current safety objectives, while still under scrutiny, is achieving acceptable levels of risks.

The Reactor Safety Study also provides a perspective on the relative contribution to overall risk of the various types of accidents postulated at nuclear power plants. Because of the methods used in the study, it is difficult to express these individual contributors in terms of relative risk to individual members of the public. However, since the calculated radiological doses resulting from the release of fission products in the event of an accident leading to the melting of the fuel rods in the reactor core are reported in the RSS to be the dominant contributors to the overall risk to which the public might be subjected by accidents in nuclear power reactors, the probability that an accident might result in a core melt is a measure of public risk. The staff therefore included consideration of the probability of core melt in establishing ATWS safety objectives and licensing criteria.

During the review of the draft of the RSS, the regulatory staff concluded that the RSS estimates of core melt frequency may have been assessed rather conservatively. One possible conservatism is that the conservative licensing methods and criteria were used to determine if accident sequences resulted in core melt. Another indication that the core melt frequency may be overestimated is that accident sequences, such as failure to maintain

cooling following a transient induced shutdown, that are major contributors to the probability of core melt in the reactors studied in the RSS may not have as high a probability of resulting in melting in another reactor. In general, the RSS estimate is applicable only to reactors similar in design to those studied and does not reflect the many changes that have been made in subsequent reactor designs. Continual improvements in reactor safety are expected in the future as a result of the concern with the increasing number of plants. Thus, an estimate of core melt probability in the future population of reactors would be expected to be lower than the RSS estimate.

Appendix X provides a review of the contribution that ATWS events make to the overall probability of core melt. Based on this review, the staff concludes that ATWS events would be significant contributors to the overall probability of core melt in future reactors. This conclusion differs somewhat from the results of the RSS for the following reasons.

Although ATWS events are small contributors to the overall probability of core melt in the PWR studied in the RSS, this is not true for all PWRs. Although still requiring a licensing review, the PWR studied would not require any modifications to meet the requirements proposed by the staff regarding ATWS, which are discussed in Section 7. Consequently, the probability of core melt resulting from an ATWS event is already low in this PWR. However other PWRs of different design that do not meet the

proposed staff requirements, would experience significantly higher system pressure following an ATWS event and would therefore have a higher probability of core melt resulting from an ATWS than the PWR studied in the RSS.

The BWR studied in the RSS is generally representative of most BWRs, except for one significant design feature. This feature, a trip of the reactor system recirculation pumps initiated by high pressure, has been shown through analyses by GE of ATWS events in a BWR, to be one of the means of meeting some of the proposed staff ATWS requirements. However, many BWRs currently in operation have not installed this feature. Thus, in the general population of BWRs, ATWS events would be larger contributors to the probability of core melt than indicated in the RSS.

Analyses not considered in the RSS show that ATWS events are a larger contributor to the probability of a core melt than estimated in the RSS. In the RSS it was assumed that tripping of the recirculation pumps followed by manual actuation of the Standby Liquid Control System (SLCS) to inject boron into the core would limit reactor pressure and power such that core melting would not occur. However, these analyses show that manual actuation is too slow and the capacity of the SLCS too small to adequately control the core power level following an ATWS event. Therefore, the core might not remain covered because the steam generation rate exceeded the ECC system's capacity or resulted in the failure of the suppression pool even if the recirculation pumps tripped.

If the frequency of ATWS events resulting in core melt were reduced to approximately 10^{-6} per reactor-year, ATWS would be a small fraction of the overall risk from nuclear power plants even if further improvements were to reduce the probability of other accident sequences. In the 1973 WASH-1270 report, the staff proposed 10^{-7} per reactor-year as an objective for the probability of ATWS events; we now believe that 10^{-6} per reactor-year is a more appropriate objective for the probability of ATWS events that would exceed conservative ATWS acceptance limits on system parameters. As discussed later in more detail, these acceptance limits or criteria have been chosen to prevent core melting or radiation doses greater than the 10 CFR Part 100 guideline values in the event of an ATWS.

This safety objective, given the present state of the art of probabilistic assessment of risk, should be used only as an aiming point in establishing whether a safety problem exists. Similarly, comparison of the ATWS frequency with this safety goal can only be a starting point to the development of safety criteria. These criteria and their bases are discussed in Section 7.

It is recognized that this objective appears to depart from the precedent in the selection of design basis events; that is, an overall safety objective of 10^{-6} per year and an objective for individual events of 10^{-7} per year. However, these previous objectives are generally applied for the purpose of determining which events might be totally excluded from the

safety design basis of reactors. The original intent of WASH-1270 was that for future reactors, ATWS events could be excluded from the design basis by requiring a second separate and diverse means of reactivity shutdown. If, on the other hand, ATWS events are included in the design basis, additional margins are available and should be considered. First, conservative criteria or limits to define successful mitigation of the ATWS event, such as the system pressure limit, can be specified. Thus, a complete evaluation of the probability of exposure of the public to radiation should also include the probability, in some cases substantially less than one, that core melt would result even if these stated limits were violated. Second, all occurrences of core melt would not result in significant offsite consequences. The results of the RSS indicate that only about two per cent of core melt sequences result in any early fatalities although Part 100 exposure guidelines would be exceeded in most cases. This additional conservatism should also be considered.

In order to determine the impacts of any further delays in implementing changes to meet the staff ATWS requirements, the staff has estimated the probability that the ATWS criteria would be exceeded in the interim. This estimate is based on an assumed frequency of 2×10^{-4} per reactor-year of an anticipated transient occurring with a subsequent failure of the control rods to insert resulting in significant consequences. However, not all ATWS events would result in exceeding the proposed ATWS acceptance criteria in all plants. In Westinghouse plants similar in design to that studied

in the RSS (Surry), the probability of exceeding the criteria is low. Approximately half the Westinghouse plants are like Surry. It is assumed that the remainder of the Westinghouse plants would be appropriately modified by 1980. It is assumed that all of the B&W and CE plant would be appropriately modified by 1981. In boiling water reactors with a recirculation pump trip, the consequences of an ATWS event would be partially mitigated. It is assumed that all BWRs would have this feature installed by 1980. With these assumptions, the probability of a core melt resulting from an ATWS event in the next three years is about 10^{-2}. Based on the RSS, the probability of a core melt from all other causes is also about 10^{-2} in the next three years. Thus, the risk contribution from ATWS events during the two year period of implementation of the proposed staff requirements roughly equals the risk arising from other accidents for this period.

6. Reduction of ATWS Risk

The staff has concluded that some corrective measures to reduce the probability or consequences of ATWS events are required because, as discussed previously, the reliability of current scram systems cannot be shown to be adequate to meet the safety objective considering the rate at which these systems are challenged by anticipated transients. Three general means of attaining this objective are recognized, as discussed in the following sections. These are: reduce the frequency of occurrence of transients

that challenge the reactor protection system, increase the reliability of the protection system, or provide systems that mitigate the consequences of ATWS events. In developing corrective measures, the primary concern is common mode failures. Thus, if corrective measures are to be applied, they must be independent of current scram systems including the control rods and drives. Independence can be achieved through physical isolation and diversity in the concept, design, installation, operation and maintenance of equipment.

6.1 Reduction of the Number of Transients

One means of reducing the probability of ATWS events would be the reduction in the frequency of occurrence of anticipated transients. In order to achieve the proposed safety objective by this means, the frequency of transients requiring scram would have to be reduced by a factor of 100. Such a large reduction in the arrival rate of transients appears to be impractical. Since there are a large number of causes of anticipated transients, many of which are events external to the plant, the elimination of nearly all of them, i.e., 99%, would be costly if indeed practical. Furthermore, the difficulty of demonstrating that a reduction had been attained increases with the amount of the reduction.

6.2 Improvement of Scram Reliability

A second method of reducing the probability of ATWS events would be the improvement of the reliability of current scram systems. The staff proposed in WASH-1270 that only this method be used for plants docketed for construction permits after October 1, 1976. The intent of the position was that a second means of reactivity shutdown should be provided. This second means should be separate and diverse and therefore independent of the normal reactivity shutdown system. This method was thought to be preferable to all others, since for future reactors ATWS events would then be of such low probability that they need not be considered as design basis accidents, similar to the present treatment of reactor pressure vessel failure and some external events. By this approach the staff thought that the need to analyze the consequences of ATWS events in each plant and to review and continually update the detailed evaluation models used in these analyses would be avoided in the future.

Subsequently, the staff recognized that as a practical matter implementation of such an approach would still require analyses of the performance of a second reactivity shutdown system and the development of evaluation models. Discussion with vendors revealed substantial difficulty in achieving a second separate and diverse means of reactor shutdown. Two approaches seemed practical, installation of diverse mechanisms on some of the control rods or provision of systems that could inject a soluble neutron poison.

The WASH-1270 position recognized that a complete duplicate set of rods and drive mechanisms could not be installed in the space available in a reactor. However, based on some preliminary evaluations, the staff believed that only a portion of the rods might be sufficient to achieve the objective. Subsequently, it became clear that an evaluation model would be required to assess the effectiveness of this solution. The WASH-1270 position also recognized the difficulty of attaining any effective degree of diversity in the neutron absorber sections of the control rods. Thus, the position only required diversity of the control rod drive mechanisms and not diversity of the control rod absorber sections. Subsequent experience has shown that, although no significant number of rods have been affected, failures of core components have occurred that could impede motion of the control rods. If this approach were to be proposed by a reactor manufacturer, the staff would now also require diversity in the control rod neutron absorber sections.

An alternative approach is the use of a soluble neutron poison. PWRs routinely use borated water as a means of reactivity control. BWRs have an alternate shutdown system that uses a sodium pentaborate solution. The difficulty of these systems is that a high concentration of boron must be rapidly injected at high pressure in order to be effective. Some evaluation of these systems has been done, but a specific system has not yet been proposed. If an applicant proposed such a system, an evaluation

would also be required in order to assess the effectiveness of these types of systems.

Since the primary purpose of this position, that is, elimination of the need for evaluation models, could not be attained, the staff has reconsidered its position. As discussed in the next section, the safety objective can be reached by other means. Although still an acceptable way of achieving the safety objective if diversity of both the control rods and their drive mechanisms can be provided, the provision of a separate and diverse reactivity shutdown system need not be the exclusive means of dealing with ATWS in the future.

Three of the reactor manufacturers have proposed systems that partially meet the requirements of the WASH-1270 position for future reactors. These manufacturers propose to increase the reliability of the electrical portion of the scram system of their reactors by providing independent, separate and diverse means of initiating control rod scram. However, no changes to the current control rod and drive systems are proposed. We do not believe that these proposals can provide the desired assurance that the safety objective will be met unless we were to accept the premise that the rods and drives have an unreliability of approximately 10^{-7} per demand. As discussed previously, the reliability of the control rods and drives is difficult to quantify. Hence, these proposals would be difficult to

accept because such a low unreliability cannot be readily demonstrated and may not be attainable.

6.3 Mitigation of ATWS Consequences

The third method to achieve the safety objective for ATWS events does not reduce the probability of an ATWS event but does reduce the probability that such an event would result in unacceptable consequences. In this approach, systems are provided to mitigate the consequences of a failure to scram following anticipated transients. The purpose of these mitigating systems is to (1) limit the pressure rise following an ATWS event in order to preserve the integrity of the reactor coolant pressure boundary; (2) provide makeup water and core cooling; and (3) limit leakage of radioactive material by preserving containment integrity, and in the case of PWRs, steam generator tube integrity.

Overpressure protection in power reactors is now provided by the combined action of control rod scram to reduce power and safety valves to relieve pressure. If the control rods should fail to insert following a transient, such as turbine trip, other means of reducing power and, in some cases, increasing the pressure-relieving capacity must be provided. In a BWR, transients that isolate the reactor from the turbine or condenser result in a pressure increase. This increase in pressure compresses the steam bubbles in the reactor core, which in turn increases reactivity and causes

an increase in power. This positive reactivity feedback effect results in further increases in reactor system pressure unless some external means of reducing reactivity and power is provided. Increased safety valve relief capacity will delay but not prevent overpressure.

The method proposed by GE for rapidly decreasing the power in a boiling water reactor if the rods fail to insert is to trip the main coolant recirculation pumps. The resultant decrease in core flow would cause an increase in the volume of steam bubbles in the core and a subsequent decrease in power. Installed safety valve capacity is then sufficient to limit the pressure rise within acceptable limits. This pump trip would be initiated by a high pressure signal. Table II summarizes the calculations by GE of peak pressure and containment conditions. A detailed evaluation of these calculations is contained in Appendix XVI.

In a PWR, isolating the steam generators from the turbine or condenser would result in an increase in the primary coolant temperature and an accompanying expansion of the coolan This expansion can be great enough to completely fill the pressurizer and cause water rather than steam to be discharged through the safety valves resulting in a large pressure increase. However, the increase in the coolant water temperature can reduce the reactivity and cause a decrease in power. This negative reactivity feedback effect can reduce the power sufficiently to limit the pressure rise if sufficient safety valve capacity is provided.

In a PWR, the magnitude of the pressure increase is sensitive to the value of the moderator temperature coefficient, the relief valve capacity, the rate of heat removal in the steam generators and other factors. These factors vary widely between reactor designs, and thus the different vendor designs have significantly different pressure response characteristics in an ATWS event. The Westinghouse reactors have the greatest relief capacity and the largest steam generator heat capacity, and therefore the least pressure rise following an ATWS. The Combustion Engineering designs have a smaller relief capacity and steam generator heat capacity and therefore a larger pressure rise. The Babcock and Wilcox designs have once-through steam generators with the smallest heat capacity and a smaller relief capacity and therefore have the largest pressure rise. Table III summarizes the PWR reactor manufacturers' calculations of peak pressure. Detailed evaluations of these calculations are contained in Appendices XIV, XV and XVII.

The post-shutdown heat removal and inventory makeup systems in power reactors are designed to remove decay heat and some sensible heat. If the reactor power is not quickly reduced after the steam or feedwater systems are isolated as the result of a transient such as a turbine trip, the coolant will be soon boiled away and melting of the core could result. Therefore, if the rods fail to insert following a transient such as turbine trip, power must be reduced quickly to maintain core cooling as well as to limit pressure.

TABLE II

Summary of BWR Analyses

Transient	Peak Reactor Press. PSIG			Peak Containment Press. PSIG			Peak Containment Temp. °F		
	BWR4	BWR5	BWR6	BWR4	BWR5	BWR6	BWR4	BWR5	BWR6
MSIV Closure	1350	1270	1322	6.8	6.5	5.9	149	147	128
MISV Closure with safety valve stuck open	"	"	"	15	13.25	5.9	195	199	149
Limits	1500	1500	1500	56	46	15	160	160	190

TABLE III

Summary of PWR Analyses

Vendor	ATWS Event	Peak Reactor Pressure, psia
Westinghouse	Loss of load with one relief valve failed	3197 (system pressure)
Combustion Engr. 2560 MWt	Loss of feedwater with one relief valve failed	4508 (pressurizer pressure)
3800 MWt	Loss of feedwater	4087 (pressurizer pressure)
Babcock & Wilcox 145 FA	Loss of feedwater with one relief valve failed	5004 (core outlet pressure)
177 FA 205 FA	"	4978 (" " ")
3600 MWt	"	4555 (" " ")
3800 MWt	"	4372 (" " ")
Limit	—	3200

The reactivity effects of the moderator temperature in a PWR or the pump trip in a BWR are insufficient to make the core subcritical and reduce power to the decay heat level and within the capacity of the normal post-shutdown and makeup systems. Thus, maintenance of post-ATWS core cooling capability requires an additional means of reactivity reduction. Both types of reactors have boron injection systems that can be used to make the core subcritical and standby core cooling systems that can remove decay heat if the reactor system pressure rise is controlled within acceptable limits. In a PWR, the ECCS safety injection system can inject a high concentration boron solution at a rate sufficient to reduce power quickly. Heat can then be removed through the steam generators using the auxiliary feedwater system. In a BWR, the boron injection systems as currently designed are manually actuated and have a small capacity. An automatically and therefore more rapidly actuated system of larger capacity would be necessary to reduce heat generation to within the capacity of the standby core cooling system before the core becomes uncovered.

BWRs have a limited capability to cool the reactor at high pressure. For normal shutdown or in the event of a loss-of-coolant accident, they rely on the operation of the relief valves to reduce pressure to within the capacity of the low pressure emergency core cooling systems as a backup to the high pressure systems. However, following an ATWS event such as turbine trip, the relief valves are already fully open and reactor pressure cannot be reduced unless reactor power is greatly reduced. Furthermore,

the reliability of BWR high pressure coolant injection systems has been poor, on the order of 10^{-1} unreliability per demand. The response time, capacity and reliability of the BWR boron and high pressure coolant injection systems would need to be improved if they are to be relied upon to mitigate the consequences of ATWS events.

Leakage of radioactive material following postulated accidents is controlled by the containment. The containment structures are designed to withstand the pressure resulting from the reactor system blowdown following the design basis loss-of-coolant accident. Pressure would rise inside the containment following an ATWS event as a result of the steam and water discharged through safety and relief valves. If power is reduced sufficiently to prevent the core from uncovering, the containment pressure following an ATWS event would be considerably less than the containment design pressure.

The pressure suppression type containment used with BWRs may fail by a mechanism other than overpressure. In this type of containment, steam from the safety valves is discharged through pipes submerged in the suppression pool and quenched by the pool water. The steam quenching heats the suppression pool water and as the water is heated to near the saturation temperature, the steam quenching becomes unstable. This instability can result in large vibrations of the discharge pipes and the containment itself. The onset and magnitude of this instability varies among various

BWR designs. If these vibrations cause failure of the containment structure excessive leakage may result. In addition, the suppression pool serves as the source of water for core cooling. Failure of the containment could allow this water to drain out, and in some designs interrupt core cooling. GE has previously proposed to prevent these vibrations by limiting the pool temperature to below the threshold value at which steam quenching instability begins to occur. This requires a rapid reduction in core power following an ATWS. Thus, there is a second reason for a faster, higher capacity boron injection system. GE has also concluded that additional heat exchangers to cool the suppression pool water may be required. A detailed evaluation of this effect is contained in Appendix XVI.

7. Proposed Requirements

As a result of the recent review and reevaluation of the information currently available on the subject of ATWS, the staff recommends that there is a need to include consideration of postulated ATWS events in safety evaluations and that system modifications may be needed to achieve the safety objectives discussed previously. More definitive and specific guidance is, however, required for reactor designers and operators. An objective in the development of such regulatory requirements is to provide specific and meaningful guidance to designers and owners while still allowing freedom to create more effective and economic solutions. Requirements expressed only in terms of the ultimate objective, i.e., limiting

the potential exposure of the public to the release of radioactivity, allow the most freedom but they require further interpretation to identify acceptable design bases, methods and system parameters, that can be directly used by the system designer. The use of probabilistic methods can, in theory, provide additional freedom to the desigrer in meeting the desired objective, but considerable analysis is required to determine the system parameters necessary for the specification of equipment and components. As will be discussed, the staff proposes to use deterministic rather than probabilistic calculations and criteria for ATWS licensing requirements. Where possible, the criteria developed by the staff are in terms of system parameters rather than ultimate objectives. This approach will be seen to follow the approach described in the staff's 1975 status reports. The principal difference, aside from individual details, between the licensing requirements now proposed by the staff and those of the status reports is the more explicit and quantitative (although still approximate) probabilistic basis. In the status reports the reliance was more on engineering judgment supported by some event tree type analyses.

If a probabilistic safety assessment were developed, the objective would be to determine the probability of exceeding certain limits -- the acceptance criteria. An advantage of this approach in the development of licensing requirements is that, if the information concerning event frequencies and system reliability is available and the overall probability can be determined, the degree of conservatism can be quantitatively determined.

However, for the situations of interest in the evaluation of reactor safety, this information and the probability are not known precisely.

Where data on events that have occurred frequently are available, such data allow estimation of past event frequency and system reliability. Prediction of future probabilities can be based on this information provided that the future is like the past. For less frequent events, experience data do not give event frequency or system reliability estimates with sufficient accuracy to be useful in assessing the extent to which safety objectives are achieved. The previous discussion of scram reliability in Section 4 illustrates this point. Because no actual ATWS event has ever occurred in a nuclear power plant, it is evident that estimates of the frequency of ATWS events are uncertain. Thus, the uncertainty of totally probabilistic ATWS assessments is large and may not be any better than a deterministic approach supplemented by a probabilistic basis.

There are other practical difficulties in adopting a set of probabilistic ATWS requirements. First, the resources expended by the nuclear industry to generate probabilistic ATWS calculations would be considerably greater than for deterministic calculations. Similarly, the resources committed by the NRC to evaluate probabilistic ATWS calculations would also be greater. Finally, even if resources were committed to generate and evaluate such calculations, the review process would likely lead to the same kinds of protracted disagreements over details of the models, data and

data applicability. In our opinion, this last difficulty is the most significant disadvantage of reliance on probabilistic assessment. Nine years of dialogue between industry and the staff have not been sufficient to obtain a common point of view regarding ATWS objectives, methods, relevance of data, or applicability of models. The staff believes that in today's circumstances -- the current state of probabilistic technology, uncertainties regarding methods and data, disagreements between industry and NRC regarding the basis for regulation with respect to ATWS -- a simpler and more direct method should be applied that does not involve a complete probabilistic ATWS calculation for each plant.

The method proposed by the staff is the use of deterministic calculations and criteria to specify ATWS licensing requirements. In effect, this means that for each plant a selected set of ATWS events must be analyzed using specified methods in order to determine whether certain performance and engineering acceptance criteria can be met. These criteria are selected on the basis that they provide reasonable assurance of attaining the ultimate objective, limiting the release of radioactivity, without requiring a multitude of additional, complex and uncertain calculations to determine the degree and likelihood of core melt and release of radioactivity. In the proposed approach the analysis methods are specified to provide a consistent, explicit means of assessing with the desired degree of confidence whether the acceptance criteria are met.

The staff envisions that rulemaking would be initiated to formally establish ATWS acceptance criteria in the Commission's regulations and that guidance on acceptable analysis methods would be promulgated less formally in Regulatory Guides, so as to be more amenable to future change. Acceptance criteria proposed by the staff and the guidance on analysis methods and their bases are discussed in the following sections and in more detail in Appendices IV, V, VI, VII, VIII, IX and XI.

7.1 Acceptance Criteria

The staff recommends that all nuclear power plant designs should incorporate the design features necessary to assure that the consequences of anticipated transients would be acceptable in the event of a postulated failure to scram. The primary criterion for acceptability is that the calculated radiological consequences must be within the dose guideline values set forth in 10 CFR Part 100. In addition, more specific acceptance criteria have been developed for primary system integrity, fuel integrity, containment integrity, long-term shutdown and cooling capability, and the design of mitigating systems. The following subsections provide a discussion of these criteria and their bases, and of the changes from the criteria previously published by the staff in WASH-1270.

7.1.1 Radiological Consequences

The proposed criterion appropriate to offsite radiological doses resulting from ATWS events is:

> The calculated radiological doses from postulated ATWS events shall be within the guideline values set forth in 10 CFR Part 100. The doses shall be calculated in accordance with an acceptable dose calculation model and shall consider, among other things, the leakage from steam generator tubes and the damage to fuel rod cladding.

The purpose of this radiological dose criterion is to assure that calculated offsite doses are within acceptable limits even if core melting is not predicted. The dose guidelines set forth in 10 CFR Part 100 are used since ATWS events are to be considered as design basis accidents.

One source of radioactivity is the activity normally present in the reactor coolant during normal operation or following shutdown. In an ATWS event additional clad failures may occur and result in additional releases of some of the inventory of radioactive material contained in the fuel rods.

Leakage of radioactivity is possible through several paths. The radioactive coolant that is released to the containment can leak through the normal containment leakage paths such as penetrations and isolation valves. Another source of release to the environment in PWRs is through leakage or rupture of steam generator tubes. Since ATWS events can result in the

opening of the steam generator safety valves which vent directly to the atmosphere, and the reactor system pressure is higher than the pressure of the secondary side of the steam generators, reactor coolant can leak into the steam generators and be directly released to the environment. Leakage through all these paths needs to be considered in assessing the offsite radiological doses.

7.1.2 Primary System Integrity

The proposed criterion appropriate to assuring the continued integrity of the reactor coolant system during an ATWS event is:

> The calculated reactor coolant system pressure and temperature shall be limited such that the calculated maximum primary stress anywhere in the system boundary, except steam generator tubes, is less than that permitted by the "Level C Service Limit" as defined in Section III of the ASME Nuclear Power Plant Components Code. In addition, the deformation of reactor coolant pressure boundary components shall be limited such that the reactor can be safely brought to cold shutdown without violating any other ATWS acceptance criterion. The integrity of steam generator tubes may be evaluated based on a conservative assessment of tests and the likely condition of the tubes over their design life.

In considering ATWS events, one of the initial concerns was that the pressure increase accompanying the event might result in failure of the reactor vessel followed by melting of the core and a large release of radioactivity. In WASH-1270, the staff addressed this concern by including a general radiological dose criterion and a specific limit on system

pressure. This limit is intended to define a level below which there is high confidence that the vessel or other portions of the reactor coolant pressure boundary would not fail. The pressure is limited to that which would result in a primary stress no more than the "emergency condition" stress as defined in the ASME code and now called the "Level C Service Limit" stress. This criterion effectively limits the primary stress to the yield strength of the materials. Allowing stresses in excess of yield strength would, in many or most of the reactor coolant system components, necessitate the use of inelastic stress analyses which, although available, result in less easily defined margins. Limiting the primary stress to the yield strength is sufficient to limit general deformation of the system although some local yielding and deformation could occur at areas of structural discontinuity.

A recent change to the ASME Code places an additional restriction on the use of the Emergency Stress Limit (now Limit C Service Limit) for ferritic materials. For these materials primary membrane stresses resulting from pressure induced loads will be limited to 0.9 of the yield strength. There have been no similar code changes for nonferritic materials. It is expected that this change will be published in the Summer 1978 Addendum of ASME Section III. Currently, the NRC rule 10 CFR Part 50.55a that addresses the use of codes and standards does not require the use of revisions to Section III of the Code beyond the Winter 1976 Addendum. However, the rule is periodically revised to incorporate revisions to the Code and the

applicability of the Summer 1978 Addendum will be addressed in a future revision. Applicants will be required to meet these new limits in accordance with 10 CFR 50.55a.

The reactor coolant systems of all PWRs and BWRs contain components fabricated from both ferritic and nonferritic materials. Analyses performed to date have indicated that in all cases the "limiting" components in the system, that is, those that reach their limits imposed by the Level C Service Limit at the lowest system pressure, are those fabricated from nonferritic stainless steel materials. Analyses typically establish that components fabricated from ferritic materials can withstand substantially higher pressure before reaching the Level C Service Limit, as it was defined in the code up until the recent change noted above. It is the staff's judgment that the ferritic components when evaluated against the revised limit will still, in general, be shown to withstand higher pressures than their nonferritic counterparts within the limitations imposed by Level C Service Limit for these different material categories. In summary, it is our judgment that the allowable system pressures discussed for each of the types of plants throughout this report, although determined from evaluations made against the "old" Level C Service Limit, would not be expected to change substantially if at all when the new ASME code is used.

There is general agreement as to the acceptable stress limits to be used in the design of reactor coolant system components for normal plant

operating conditions, i.e., the Normal Condition Stress Limit (now Service Limit A) defined in the ASME Code; and the methods used for calculating stresses under these conditions are well standardized.

Because accident analyses are not typical of the majority of engineering analyses there are divergent views as to the appropriate criteria and methods to be applied to accidents such as ATWS. Thus the criterion proposed above has been criticized by some as overly conservative and by others as nonconservative. The view of one group is that for such a low probability event as ATWS the higher Faulted Condition Stress limit (now referred to in the Code as Level D Service Limit) would be sufficient to assure an adequately low overall probability of failure. Another view is that the Emergency Condition stress limit was never intended to apply for situations where, as for ATWS, the major portion of the load results from pressure within the component, where large deformations could occur at discontinuity areas.

The staff concludes that the margins available if the Level D Service Limit were adopted cannot be adequately defined so as to provide a reasonable assurance that failure would not occur under ATWS loads. The practical difficulty of performing and reviewing the required inelastic analyses must also be considered. In the staff view these are sufficient reasons not to adopt it.

The present criterion addresses, as did the earlier staff status reports, the second criticism by explicitly requiring a demonstration that deformations resulting from the pressure experienced in an ATWS event will not prevent long-term cold shutdown, or result in the violation of any other ATWS acceptance criterion. Of less serious consequence would be deformations that would cause leakage of the vessel closure seal or of other components such as manway covers, pump shaft seals and valve body to bonnet joints or would prevent safety or relief valves from closing. One of the most serious effects of the pressure transient resulting from an ATWS event could be the deformation of equipment, such as valves and pumps, such that functions necessary to shut down and cool the reactor during and following an ATWS event could not be performed. Although permanent deformation is the primary concern, the transient elastic deformation of equipment that must function during an ATWS also needs to be considered. The staff proposes that detailed analyses or tests would be required to demonstrate the operability of equipment.

7.1.3 Fuel Integrity

The proposed criterion appropriate to the limitation of fuel damage during an ATWS event is:

> Damage to the reactor fuel rods as a consequence of an ATWS event shall not significantly distort the core, impede core cooling and prevent safe shutdown. The number of rods which would be expected to have ruptured cladding shall be determined for the purpose of evaluating radioactive releases.

The primary purpose of fuel damage criteria is to provide assurance that the core does not become distorted to the point where cooling may be inadequate to prevent melting of the fuel and the potentially large release of radioactivity. Although not as significant, because the potential release of radioactivity is much smaller, a second purpose is to define the conditions at which the fuel rod cladding ruptures. However, the specification of fuel performance acceptance criteria in other than qualitative terms is difficult because currently available methods cannot accurately predict fuel rod behavior under abnormal conditions.

The earlier fuel damage limits proposed by the staff in WASH-1270 addressed three fuel performance parameters; external pressure, fuel pellet temperature, and clad temperature, only in terms of "significant cladding degradation or significant fuel melting" and "significant safety problem with the fuel". Although the vagueness of these terms has caused some confusion, the staff intended their meaning to be "damage of such magnitude that core cooling capability may be impaired".

Maintenance of core cooling capability means that any changes in the geometry of the fuel assemblies must be such that adequate coolant flow channels remain. Distortion of the fuel assemblies could result from the loss of cladding mechanical properties, either through oxidation or high temperature; general melting of the clad; extreme, co-planar fuel rod

ballooning; violent expulsion of molten fuel; severe mechanical impact; or spacer grid deformation.

In the absence of limits specifically derived for ATWS events, the staff proposes to use the clad temperature and oxidation limits specified in the ECCS acceptance criteria (10 CFR Part 50.46) in judging whether core cooling might be impaired. Furthermore, the calculated radial average enthalpy at any axial location specified for fast reactivity insertion accidents is also imposed. The calculated effects of any of the postulated ATWS events do not reach or even approach the 2200°F temperature and 17% oxidation limits specified in the ECCS acceptance criteria or the 280 cal/g enthalpy limit. Since there is no need or basis for deviating from these limits the staff proposes that they should also be used to assess the acceptability of calculated consequences of ATWS events.

Neither WASH-1270 nor Section 15.8 of the Standard Review Plan addresses the criteria to be used to determine clad perforation as an input to radiological dose calculations. Subsequent to the publication of WASH-1270, the vendors proposed specific fuel damage limits to define the conditions that would result in rupture. However, the staff concluded that these proposed limits did not include all of the pertinent parameters, contained large uncertainties, and were therefore unsuitable. Since none of the reactor manufacturers predicts cladding collapse, clad swelling or fuel melting, the development of fuel failure criteria is primarily concerned

with the rupture mechanisms of high temperature and pellet-clad interaction (PCI). Although the adoption of a realistic cladding temperature limit as a clad rupture criterion might be desirable, the staff has not been successful, to date, in developing one that would incorporate time and rate variables and be an adequate indicator of clad failure. Therefore, the staff proposes to retain the admittedly conservative criterion that rods expected to experience a departure from nucleate boiling (DNB) are assumed to fail. The number of rods expected to experience DNB can be determined by a summation of the probability of DNB on individual rods based on accepted statistical correlations of DNB data.

The second failure mechanism of concern, PCI, is even more difficult to quantify than a temperature limit. The PCI limit would be in the form of cladding stress, strain or strain-rate limit. However, the phenomenon is presently not well enough understood to permit development of such a limit. PCI failures during ATWS are more likely to occur in BWRs than in PWRs. During the typical ATWS event in a BWR, the transient power increase produces differential thermal expansion of the pellets against the cladding and possible clad failure. During most ATWS events in a PWR, flow is reduced, causing the clad temperature to increase resulting in differential thermal expansion of the clad away from the fuel pellets. Until definitive PCI limits are established, the staff proposes to review predictions of clad failure on a case-by-case in the light of current information to

assure that the number of fuel rods that might fail as a result of PCI is conservatively calculated.

7.1.4 Containment Integrity

The proposed criterion appropriate to the assessment of containment integrity during an ATWS event is:

> The calculated containment pressure, temperature and other variables shall not exceed the design values of the containment structure, components and contained equipment, systems or components necessary for safe shutdown. For boiling water reactor pressure suppression containments, the region of relief or safety valve discharge line flow rates and suppression pool water temperatures where steam quenching instability could result in destructive vibrations shall be avoided.

The primary purpose of the containment criterion is to assure that the integrity of the containment is maintained in an ATWS event. Since the safety valve discharge is vented to the containment, leakage from the containment could result in significant radiological doses, particularly if fuel rods should rupture during the event. Based on reactor manufacturer calculations, the design values of containment pressure and temperature are not the limiting conditions for ATWS events.

However, a further potential failure mode has been identified for BWR pressure suppression containments. Reactor operating experience indicated that potential instabilities in quenching of relief valve discharge flow

could occur for certain steam mass flow rates and suppression pool temperatures. These instabilities resulted in severe and potentially destructive vibrations of the valve discharge lines and the containment. Since the containment suppression pool serves as the source of water necessary to maintain core cooling following an ATWS event, structural failure of the containment could jeopardize core cooling as well as containment integrity. GE has proposed to prevent these vibrations by limiting the suppression pool temperature to below the threshold value at which steam quenching instability occurs. The staff is currently studying this proposal. Additional information may be required before an acceptable threshold temperature can be determined.

7.1.5 Long-Term Shutdown and Cooling Capability

The proposed criterion appropriate to the assessment of the capability to maintain the plant in a safe condition following an ATWS event is:

> The plant shall be shown to be capable of returning to a safe cold shutdown condition subsequent to experiencing an ATWS event, i.e., it must be shown that the reactor can be brought to a subcritical state without dependence on control rod insertion and can be cooled down and maintained in a cold shutdown condition indefinitely.

The purpose of this long-term cooling criterion is to assure that equipment is available to recover from postulated ATWS events. In general this equipment will be the same as provided for long-term cooling following a

loss-of-coolant or other accident. Since the long-term cooling systems are low pressure systems, recovery from an ATWS event requires cooling and depressurizing the reactor. The analysis of these systems for ATWS service should provide detailed information on reactor heat generation rate, operability and effectiveness of the boron injection systems, heat removal rates (particularly if the reactor system must operate under natural circulation conditions), sources and quantities of makeup water, time required for specific operator actions, and time required to achieve cold shutdown.

7.1.6 Mitigating Systems Design

The proposed criterion appropriate to the assessment of the systems required to mitigate the consequences of ATWS events is:

> Mitigating systems are those systems, including any systems, equipment, or components, normally used for other functions, relied upon to limit the consequences of anticipated transients postulated to occur without scram. These systems shall be automatically initiated when the conditions monitored reach predetermined levels and continue to perform their function without operator action unless it can be demonstrated that an operator would reasonably be expected to take correct and timely action. These systems shall have high availability and in combination with the reactor protection system shall provide two independent, separate and diverse reactivity shutdown functions. The mitigating systems shall be independent, separate and diverse from the reactor trip and control rod systems, including the drive mechanisms and the neutron absorber sections. The mitigating systems shall be designed, qualified, monitored and periodically tested to assure continuing functional capability under the conditions accompanying ATWS events including natural phenomena such as earthquakes, storms including tornadoes and hurricanes, and floods expected to occur during the design life of the plant.

The systems that can be provided to limit the consequences of an anticipated transient even in the event of a failure to scram have been briefly described above. The purpose of these mitigating systems is to limit the pressure rise in the reactor system and maintain core cooling following an ATWS event. In order to meet the safety objective, these systems must reliably perform their function. These requirements define the means of attaining the required reliability.

Safety systems are generally required to be automatic since limited reliance can be placed upon the ability of an operator to respond quickly and correctly to the multitude of signals and alarms resulting from an abnormal event. Although a well trained operator is more likely to respond correctly to the more common abnormal events, his assessment of and response to highly unusual events such as ATWS is less predictable. For this reason the staff proposes that operator action during this first ten minutes of an accident should not be relied upon. However, the staff proposes that operator action later in the course of an accident can be relied upon if it is shown that information on the conditions in the reactor and of the mitigating systems is available to the operator, that sufficient time is available to correctly assess the situation and take appropriate action, and that the operator has been trained in the proper actions. The assumption of operator action is limited to simple actions such as pushing a button to initiate safety injection for the PWRs or realigning the RHR valves in the BWR pool cooling mode.

The staff position regarding operator action has been developed in recognition that an adequate statistical data base for human error rates in nuclear plants does not exist. Increasing attention is being given to human reliability in an effort to adopt more definitive criteria for the role of the operator in mitigating the consequences of transients or accidents. A Regulatory Guide is currently being formulated in conjunction with staff review of the proposed Standard ANSI-N660, "Proposed ANS Criteria for Safety-Related Operator Actions." Increasing activities in human reliability studies sponsored by the NRC will assist the staff in developing a more rigorous basis for assessing operator involvement in plant safety and, as this information is developed, the staff may recommend that the requirements be modified.

Safety systems have generally been required to meet a single failure situation. The single failure criterion is one of several tools applied in system design and analysis to enhance reliability of those systems that are needed in a nuclear power plant for safe shutdown and mitigation of the consequences of postulated accidents. However, it is not sufficient by itself, and supplementary rules of design practice, such as IEEE standards, are utilized to assure high reliability systems.

The single failure criterion was developed without the benefit of numerical assessments of the probabilities of component or system failures. The Reactor Safety Study indicates that application of this criterion to the

plants that were studied did, for most systems, provide an acceptable degree of redundancy. However, the Reactor Safety Study also pointed out that factors such as complex system interactions, multiple human errors, maintenance and testing requirements also have an influence on reliability. One means of including these important factors in the evaluation of the suitability of the mitigating systems, and also of providing a rational basis for not including all failures, is the specification of a reliability criterion. Therefore, the staff does not propose to apply the single failure criterion in the evaluation of systems employed in the mitigation of ATWS events. For ATWS, failures to be considered in the analysis after the initiating event (ATWS) are based upon consideration of system reliabilities. This approach is believed to provide a more quantitative, and in that sense a better estimate, of the degree of safety achieved.

The staff has recommended a numerical objective of 10^{-3} per demand (at the 50% confidence level) as an acceptable value of mitigating system unavailability. Thus, evaluations of the consequences of ATWS events could include credit for only those systems that have unavailabilities of approximately 10^{-3} per demand or less. If multiple systems or systems with multiple trains are involved, failures of systems or trains that have an aggregate probability of more than 10^{-3} would be considered. The basis for this value is derived from the desired safety objective and the uncertainty in evaluation models as described in the following discussion in Section 7.2. In addition, the staff proposes to allow lesser values of

the reliability for systems required to operate only in specific ATWS events that have a significantly lower frequency of occurrence than the overall rate of ATWS events. For example, if the frequency of the loss of offsite power can be shown to be 0.2 per reactor-year or less, as is generally the case for many plants, then the unavailability of the systems, such as the diesel generators, that are required only following the specific event need be only approximately 5×10^{-2} (at the 50% confidence level). However, for some nuclear power plants, the occurrence of the loss of offsite power is more frequent and the higher reliability standard would have to be applied. Reliability estimates have generally been based upon Reactor Safety Study estimates, although other estimates have been accepted when justified. An acceptable way to demonstrate achievement of the required reliability for any mitigating system is to assure that the system meets the requirements of IEEE-279.

In ATWS mitigating systems, as in reactor protection systems, both independent and common mode failures are possible. Independent failures can be treated using current reliability analysis techniques. Although a quantitative evaluation of common mode failures is difficult to demonstrate, significant protection from these types of failures can be provided if the mitigating systems are independent, separate and diverse from the normal reactor trip and control rod systems that are postulated to fail. Providing independence and separation reduces the probability that common environmental conditions or interactions between systems will result in failure of both the control or scram systems and the systems provided to mitigate the ATWS event. The probability of occurrence of other common mode failures are

reduced if the systems are diverse by the use of equipment supplied by different manufacturers, or of different design, or operated in different modes. Although complete protection from common mode failures cannot be achieved, the staff believes that substantial and sufficient protection is possible through these means.

The primary concern in developing the staff position on ATWS is common mode failures in the reactor trip and control rod systems. The reactor trip system, which consists of the sensors, signal conditioning equipment, logic elements and scram breakers, has diversity in some portions. All reactor trip systems have multiple and diverse sensors, usually both flux and pressure sensors. The staff has concluded that, where appropriate, the diverse portions of the reactor trip system may be used to provide the required diverse reactivity shutdown function. For example, the proposed recirculation pump trip in a BWR is initiated by a signal from pressure sensors that also provide a signal to the reactor trip system. Since the reactor trip system also receives signals from neutron flux sensors, the staff concludes that use of the pressure sensor provides an acceptable diverse pump trip.

As discussed in Section 4.2, the staff proposes to adopt the position that the unreliability of the control rod system is approximately equivalent to the unreliability of the reactor trip system. This would assure that the safety objective would be attained by providing a diverse means of performing

the function of the control rod system. The relief and safety valves also perform a necessary function in limiting the pressures following anticipated transient. However, the long and successful performance of safety valves designed to ASME code requirements in both nuclear and general industrial services, leads the staff to propose that failure of these valves to open need not be considered in ATWS events.

One type of common mode failure that can be easily identified is failure resulting from the conditions that directly result from an ATWS event. Equipment in the containment, if required in an ATWS event, must function under the temperature, pressure, humidity and radiation conditions that will occur in the containment due to blowdown from the safety valves during an ATWS event. Therefore, equipment required in an ATWS event must be qualified for the expected conditions. Another type of common mode failure is failure resulting from events, primarily natural phenomena, that can affect the entire plant. Although safety systems have generally been designed to be protected from extremely severe, and generally also very unlikely, natural phenomena, the staff has concluded that ATWS mitigating systems need not be designed for such unlikely events in order to meet the ATWS safety objective. However, some natural phenomena that are expected to occur during the life of a plant would produce transients similar to the transients being considered, have an approximately equal rate of occurrence, and therefore should be considered in the design of ATWS mitigating systems.

7.1.7 Reactor Protection System Design

As discussed in Section 6.2, the staff in WASH-1270 proposed that a separate and diverse reactivity shutdown system would be an acceptable means of reducing the probability of ATWS events. The staff proposes to still accept this approach if the second reactor shutdown system is designed to meet the criterion stated in Section 7.1.6. However, this criterion requires all portions of the second reactivity shutdown system to be diverse from the normal reactivity shutdown system. The discussion in WASH-1270 indicated that the staff at that time did not require diversity in the control rod absorber sections, but only in the reactor trip system and the control rod drive mechanisms. In the present view of the staff, an adequate showing that the rods are sufficiently free from common mode failures has not been made. Table II-1 in Appendix II lists some common mode failures that have been observed in absorber rods, although no failure to scram due to these components has so far been observed. Therefore, the staff proposes that a second reactor shutdown system should be diverse from the reactor trip system and both the drives and the rods themselves. The second system could, in principle, use liquid poison or other means diverse from the rods and drives, if the performance could be shown to meet the acceptance criteria.

The staff position in WASH-1270 also required improvements in the reactor protection system even if other mitigating systems were provided to limit

the consequences of ATWS events. This previous position required the correcting of areas of reactor protection systems that might be particularly vulnerable to common mode failures. The staff now believes that these changes to reactor protection systems are not necessary to meet the safety objective which can be attained using reliable mitigating systems that have a greater degree of diversity from the reactor protection system.

7.2 Evaluation Models

Analyses of a set of postulated ATWS events are required to provide reasonable assurance that, considering the frequency of these events, the probability of additional component, equipment or system failures, and the uncertainties and possible temporal variation in initial conditions and system parameters, the ATWS acceptance criteria are not violated. This section provides a discussion of the staff recommendations regarding evaluation models used to make these analyses and the bases for these recommendations. More detailed discussion of the bases is provided in Appendix VII.

An ATWS frequency of 2×10^{-4} per reactor-year, combined with the proposed ATWS goal of 10^{-6} per reactor-year, suggests that no more than 1 in 200 ATWS events should result in calculated consequences exceeding the ATWS Acceptance Criteria. Such excessive consequences could arise from the existence of highly unfavorable values of plant parameters at the time of

the event or from the unavailability of mitigating systems during the course of the event sequence (e.g., the failure of several relief valves to open, or abnormally low auxiliary feedwater flow), or from combinations of such circumstances. It is evident that the reliability of ATWS mitigating systems and the uncertainty and variation in system parameters are important components in achieving the safety goal.

After publication of WASH-1270, all four NSS reactor manufacturers submitted analyses of the behavior of their plant designs during and subsequent to postulated ATWS events. The NRC staff reviewed these analyses and the computer codes which were used, performed independent verification analyses, and issued the 1975 Status Reports. In the status reports the staff recommended modifications to the reactor manufacturer's evaluation models and also discussed outstanding items that each vendor should address to satisfy the staff's ATWS requirements. General descriptions of the these analyses including major assumptions, initial conditions, cases analyzed, limiting events, descriptions of the manufactures' codes, the result obtained with the codes, and comparisons with results which were obtained using independent codes appear in Appendices XIV, XV, XVI and XVII.

In order to determine the acceptability of the reactor manufacturers' evaluation models and the results obtained with them, the staff reviewed the models, had independent analyses performed, and compared the calculated results of the models to a set of standard problems and existing experimental

data. The staff review of the models consisted of a review of the formulation of the equations used in the mathematical models, the management and detail of the noding used in the models, and the assumptions concerning initial conditions, values of parameters and performance of systems.

The staff contracted with Brookhaven National Laboratory to run independent sets of calculations of the worst ATWS event for each reactor manufacturer's designs using the RELAP3-B code with the vendors' input data. The staff, in conjunction with the N661 standards group, developed a set of standard problems which were analyzed by the three PWR manufacturers and the NRC. Comparisons were then made between the results of the staff's and the manufacturers' analyses of these problems. Existing experimental data (obtained from startup tests) were compared with the manufacturers' transient analysis codes. In addition to using results from startup testing, [illegible] additional component test data were compared with code predictions.

Although there are no directly applicable data representative of ATWS conditions, the multifaceted review described above provides confidence in the applicability and accuracy of the codes.

As [illegible]ed in the 1975 Status Reports, the objective was to obtain evaluation models that realistically predicted the course of ATWS events and conservatively predicted the consequences. Toward this end, nominal values of system parameters and realistic assumptions concerning physical

phenomena were used in order to avoid distortions in predicting the response of the reactor system. Previous analyses using many conservative assumptions and values of parameters resulted in unrealistically high predictions of the system pressure that could follow an ATWS event in a PWR. Such large distortions in the prediction of consequences can result in excessive or even unnecessary operating limitations or requirements for mitigating systems. Although conservative model assumptions may be justified and even necessary in the evaluation of extreme events, such as a loss-of-coolant accident, the response following an ATWS is relatively slow and is a limited extrapolation of transients that have actually been experienced by plants and therefore have been studied and modeled with some accuracy. This is not to say that new information may not be discovered and that modification or correction of the ATWS evaluation models will never be required. Rather, we expect that any future changes would not be expected to result in greatly different predicted consequences.

In the areas where experience is limited or parameters can vary widely, conservative assumptions have been included in the ATWS evaluation models. For PWRs, these areas are primarily the determination of the discharge flow of high pressure subcooled water through safety valves, the value of the moderator temperature coefficient of reactivity and the variation of heat transfer in the steam generators. Agreement has been reached on an appropriate safety valve discharge model, but the vendors still disagree as to the appropriate value of the moderator temperature coefficient. A

more detailed discussion of these parameters is presented in Appendices VIII and IX. The treatment of heat transfer appropriate to ATWS models remains to be confirmed by the staff using more detailed sensitivity studies.

The difficulty in specifying an acceptable value for the moderator temperature coefficient is a result of the large variation in this parameter during the life of a pressurized water reactor. After each refueling the coefficient at or near full power has a small negative value or, in some cases, a positive value which quickly decreases to a significantly more negative value during the next few days of operation. The value of the coefficient follows a generally decreasing (more negative) trend for the remainder of each refueling cycle with intermittent increases following power reductions or reactor shutdowns. This general pattern is followed for each refueling cycle.

There is general agreement that the single value of the coefficient selected for use in the evaluation of ATWS events should be a value that would not be exceeded (that is, be less negative) for more than a small fraction of the reactor operating history. The reactor manufacturers have proposed that this fraction be set at 5% of the time the reactor is critical (95 percentile value) while the staff proposes to set the fraction at 1% (99 percentile value). The difference affects the calculated system pressure by approximately 100 to 400 psi, depending on the reactor type.

There is also disagreement concerning the necessity of including the effects of failures in the mitigating systems in the analyses of ATWS consequences. As discussed previously in Section 7.1.6, the staff proposes that failures in the mitigating systems that have an aggregate probability of more than 10^{-3} be included in the analyses. Generally, this would require the inclusion of only a limited class of higher probability single failures, for example, the failure of one redundant train of a two-train system. The reactor vendors propose that no failures in mitigating systems be considered. The effect of these failures is to increase the calculated systems pressure by approximately 150 psi.

The basis for this staff position is that assuming the frequency of ATWS events is about 2×10^{-4} per reactor-year, and since there are several possible mitigating system failures, the probability of each of these failures must be less than approximately 10^{-3} in order to attain the 10^{-6} safety objective. The event trees in Appendices XIX, XV and XVII show the specific system failures and unreliabilities used in the evaluation of each PWR manufacturer's ATWS analyses. The manufacturers contend that the specification of a 99 percentile MTC, system unrealiabilities of 10^{-3} and other conservatisms results in a probability of less than 10^{-5} that, given an ATWS event occurs, the acceptance criteria would be exceeded. Considering that the staff objective, as discussed at the beginning of this section, is one in 200 or 5×10^{-3}, these requirements appear to be excessively conservative.

As a means of providing an estimate of the conservatism of the evaluation models, the staff undertook to make a statistical estimate of the uncertainty in the calculated system pressure in PWRs. This was done using a Monte Carlo technique to compute the probability distribution of the calculated pressure resulting from the variance of the system parameters. A more detailed discussion of this technique is given in Appendix VII.

A more precise and detailed calculation than actually carried out would have required the development of the probability distributions for all parameters and the functional relationship between system pressure and all of the parameters. Since such a calculation was impractical, the calculation was simplified by using only those parameters that have the greatest effect on the calculated pressure. Using these parameters, a response surface was developed as a simplified representation of the functional relationship between the parameters and the system pressure in a narrow range around the system overpressure limit. The parameters were assumed to be normally or uniformly distributed with variances estimated by the staff. Since the purpose of the study was to apply the results to reactors that had made appropriate modifications for the purpose of mitigating the consequences of ATWS events, the value of relief capacity used in each evaluation model was adjusted to produce a calculated peak pressure that would not exceed the 3200 psia acceptance limit with more than an approximate 0.005 probability. This required increased values of relief capacity in the B&W and CE models.

The calculated cumulative probability distributions are presented in Figures 1 through 4 of Appendix VII. Although some further adjustment of relief capacity would be necessary to produce distributions that have the desired 0.005 probability of exceeding the 3200 psia pressure acceptance criterion, the distributions are adequate to evaluate the conservatism of the ATWS analyses.

A comparison between the estimates of the probabilities of exceeding the pressures calculated using the deterministic prescriptions chosen by the staff and by the manufacturers and the probabilities determined from the cumulative distributions is shown in Table IV. For each PWR manufacturer, two deterministic calculations were made: one proposed by the staff, the other by the manufacturers. The staff proposal (identified as "Prescription 4" of Appendix VII) uses a 99 percentile value of the moderator temperature coefficient, nominal values of other parameters, and includes the effect of a single failure in a mitigating system. The manufacturers' proposal (identified as "Prescription 5" of Appendix VII) uses a 95 percentile value of the moderator temperature coefficient, nominal values of other parameters and does not include the effect of failures in the mitigating systems.

For these deterministic calculations, the probability of occurrence of a more severe event, given an ATWS, was estimated. For Prescription 5, this is 0.05, based upon the moderator temperature coefficient percentile. For

Table IV

Probabilities

Single Event vs. Cumulative Distribution
(From Table 7 of App. VII)

Manufacturer	B&W		CE		W	
Prescription	4	5	4	5	4	5
MTC Percentile	99	95	99	95	99	95
Sys. Reliability (%)	95	100	96	100	94	100
Calc. Press. (psia)	3335	3097	3071	2762	3233	2661
Single Event Probability	5×10^{-4}	5×10^{-2}	4×10^{-2}	5×10^{-2}	6×10^{-4}	5×10^{-2}
Cumulative Distribution Probability	5×10^{-3}	1×10^{-1}	2×10^{-3}	5×10^{-2}	5×10^{-3}	4×10^{-1}

Prescription 4, this is 0.01 for the moderator temperature coefficient, times the probability of the single failure. For the B&W plant, for example, the single failure considered has a failure probability of 0.05, giving a calculated resultant probability of 0.0005 that the calculated peak pressure of 3335 psi would be exceeded.

Also shown in Table IV are the probabilities predicted for these pressures from the calculated cumulative probability distributions discussed above. In all cases but one, the probability of exceeding each pressure as determined from the probabilistic distribution is higher than would be calculated for the single "prescription" event. In most cases, the discrepancy is large, a factor of 5 or 10.

Thus, the B&W Prescription 4, for example, appears to be excessively conservative because it has a probability of only 0.0005, or 1 in 2000, compared to the staff objective of 0.005 or 1 in 200. However, the probability distribution in this case gives a probability of 0.005 for this pressure, which is just equal to the objective.

The reason for the discrepancy between the probability distributions and the deterministic calculation is that there are many combinations of parameter values and system failures that can give pressures higher than a given value. The probability distributions take them all into account, whereas each deterministic calculation accounts for only one combination.

Therefore, if one chooses a single deterministic calculation to represent all combinations, the chosen calculation can appear to be overconservative.

For the reasons discussed at the beginning of Section 7 of this report, the staff has chosen to use deterministic calculations and criteria to specify ATWS licensing requirements. The evaluation model chosen by the staff is "Prescription 4." The basis for this choice is unquantified engineering judgment as well as the insights afforded by the probabilistic calculations discussed here and in Appendix VII. It is recognized that the "prescription" appears to be overconservative, but its use is justified by the comparisons between deterministic and probabilistic calculations. It is also recognized that the use of a single deterministic calculation will not always be precisely consistent with the probabilistic goal, because of the many approximations involved and also plant-specific differences. However, in view of the conservatism of the acceptance criteria, and based upon the studies in the appendices, the staff concludes that the use of a deterministic calculation of the consequences of ATWS events can provide adequate assurance of attaining the overall safety objective, if a prescription such as proposed by the staff is followed.

In general, the staff has found the BWR evaluation model to be conservative. However, the comparison of evaluation model results with the results of recent tests at an operating BWR, in which scram was deliberately delayed slightly following a turbine trip, did not confirm this conservatism. GE

is now revising its evaluation model to account for the deficiencies revealed in the tests. Although the staff expects these revisions will not significantly alter the results of previous calculations, the system response remains to be recalculated using the revised model after it has been reviewed and accepted by the staff.

8. Value-Impact Considerations

The recommended safety objective of an ATWS core melt frequency of 1×10^{-6} or less has been subjected to a value-impact analysis so as to present a full and complete basis for deciding the ATWS issue. Many of the values and impacts were reduced to economic terms for comparison even though they are subject to substantial uncertainty. One significant impact would be the capital costs of making ATWS modifications. A second impact, which could be significant depending upon the particular status of each plant, is the cost of delay or downtime required to make modifications. Major quantified values include averted direct radiological risks and costs of replacement power resulting from the affected facility and any other nuclear facilities that might be promptly shut down subsequent to an ATWS core melt. Some values remain intangible, subject to the reader's perception as to importance. The detailed value-impact study is presented in Appendix XII. A summary of the quantified impacts and values is given in Table V.

Table V

Summary of Value and Impact[1/]

ATWS Requirements

Design	1978 Dollars, Millions		
	Impact	Value	
		Direct	Indirect
B&W	Proprietary	1.2-5.1[3/]	1.5
CE	Proprietary	2.0-8.2[5/]	1.5
W	Proprietary	1.2-5.1[3/]	1.5
GE (BWR4)	37[6/]	19-47[5/]	23
GE (BWR5)	32[6/]	19-47[5/]	23
GE (BWR6)	9.2[6/]	19-47[5/]	23

1/This table is provided for summary purposes only. Footnotes to Tables 2.1 through 2.8 of Appendix XII are important and apply to this table.

2/For preconstruction plants. Also is probably the approximate cost of modifying CE plants in the preconstruction phase.

3/For preconstruction plants. Values multiplied by 1.61 for plants under construction and by 1.85 for plants in operation.

4/For plants under construction and operating. Also is probably the approximate cost of modifying B&W plants in the construction or operating phase.

5/For plants under construction. Values multiplied by 0.62 for preconstruction plants and by 1.15 for OL plants.

6/Likely cost of modifications in all phases (preconstruction, construction and operating).

The impacts of implementing the staff's recommended ATWS requirements, and included in Table V, are essentially the capital costs associated with making the modifications. The impacts associated with delay or downtime were not included in the table. Other kinds of impacts were considered and determined likely to be relatively small, such as radiological exposure to workers making the modifications, increased system complexity, and increased operating and maintenance costs subsequent to the modifications.

The capital costs are based on estimates supplied by the reactor manufacturers. For the B&W and CE designs the costs are for additional safety valves and control circuitry. For the GE designs the costs are for larger capacity boron and water injection systems, and control circuitry such as a recirculation pump trip. For the earlier GE designs (BWR4 and BWR5) an additional heat exchanger is required, which is not required in the latest design (BWR6). Based on a review of the estimates and a comparison of the B&W and CE estimated costs, the staff believes that the CE costs may be overestimated. The GE costs may also be overestimated. Recently GE presented the results of additional design analyses. These results indicate that less equipment may be required to meet the staff's ATWS criteria than was previously thought. If this is so, the cost of implementing the staff requirements in BWRs may be significantly less than the estimates of Table IV.

The impacts could be significantly greater and could substantially overshadow the capital costs of making the modifications, if implementation were to require extensive delays in plants currently under construction or downtime of operating reactors. The costs associated with such delays or downtime would result from additional interest during construction and/or replacing the electricity for these periods. If the installation of the necessary modifications can be scheduled over a reasonable period of time, possibly three or more years, it can probably be accomplished without adversely affecting plant operation. Some of the work is outside the containment and can be accomplished while the plant is in operation. The necessary work inside the containment could be accomplished during a refueling outage, although for some plants the outage might have to be extended. Therefore, the staff believes that implementation can be achieved without significant delay or downtime and these costs have not been included in the impact evaluation.

The cumulative impacts of the ATWS requirements depends on the number of plants to which they are applied. If Department of Energy estimates of nuclear power capacity in the year 2000 (380 plants) are used and assuming linear growth, an average of about 290 plants would be in operation during the 30-year period starting in 1978. The cumulative cost of modifying these plants would likely be less than $2 billion. However, during that 30-year period, more than 45 million million kWh of electricity would be generated by nuclear power plants assuming a 60% capacity factor. For

perspective, the 1978 present value of the sale price of this electricity would be more than $1 million million. Therefore, the impact is an amount that would add less than 0.2% to the bus-bar cost of the electricity produced.

The present worth of the values (averted risk) of ATWS events is based on the assumption that the frequency of ATWS events with potentially severe consequences is 5×10^{-5} per reactor-year in PWRs and 2×10^{-4} per reactor-year in BWRs. Although the staff has estimated the ATWS frequency to be 2×10^{-4} per reactor-year for all plants, an estimate for each type of plant has been made for this study. Considering the probability that (1) the moderator temperature coefficient of reactivity would be more favorable, (2) the auxiliary feedwater system would function, and (3) the primary coolant and core cooling systems would not fail to such an extent that serious consequences would result, the staff believes that a more realistic estimate for PWRs is a factor of four less than the previously stated value. However, a frequency of 2×10^{-4} per reactor-year is appropriate for BWRs.

The direct values of implementing the staff's ATWS requirements include the reduction in risk to the public health and safety (the possible radiation exposure of people both on and off theplant site) and the reduction of economic risk (the possible radiological damage to offsite property and loss of an electric generating station and the electric energy it can

generate). Over half of the direct values are associated with the averted radiological impacts on people and property of the plant site. The remainder are associated with the averted loss of the station and the electricity it could generate.

The radiological consequences of ATWS events that do result in core melt are different for PWRs and BWRs. The consequences differ because, assuming a core melt, the rate and time of release of fission products differs for the two types of plants. Therefore, the direct value differs for PWRS and BWRs because both the probability and consequences of ATWS events are different for the two types of designs.

Considering both the probability of ATWS events and the consequences of these events, the staff estimates that the risk of offsite radiation exposure is in the range of 50 to 500 person-rem per reactor-year for PWRs and 1000 to 3000 person-rem per reactor year for BWRs. In all cases a conservative value of $1000 per person-rem is used to convert exposure to economic terms.

The property damage that might result from an ATWS event consists of offsite and onsite damage. Again the damage differs for PWRs and BWRs, because the probability and radiological consequences of a core melt in the two types of reactors differ. The staff estimates that the offsite

property damage risks of ATWS core melts is $5,000 to $25,000 per reactor-year for PWRs and $50,000 to $200,000 per reactor-year for BWRs. The onsite damage costs consist of decontamination and decommissioning costs and are estimated to be $200 million assuming both units at a two unit station are affected by the accident.

The final element in the direct value is the differential cost of replacement power during the assumed eight-year period required to construct new plants and the appropriate portion of the capital cost of base load facilities needed to replace those lost as a result of the core melt accident.

Over 80% of the indirect values are the aversion of the differential costs of replacement power, assuming an ATWS accident at one plant results in a decision to shut down many other plants promptly to retrofit ATWS modifications. These costs are based on the assumption that 30 reactors would be promptly shutdown for a period of three months for PWRs and 12 months for BWRs following an ATWS event. The remaining indirect values represent an index as to possible adverse effects to the U.S. balance-of-payments due to increased oil imports that would likely result from such shutdowns.

There are substantial uncertainties in the direct values because of the uncertainty in the frequency, consequences, and health effects monitorization of ATWS events. Furthermore, the indirect values are based on the assumption that many unaffected plants would be shut down for modification

if an ATWS occurred which is subject to uncertainty as to how many would be shut down, as well as uncertainty as to the likelihood of occurrence of an ATWS core melt.

The cumulative values of implementing the staff's ATWS requirements over the next thirty years can be estimated. Assuming no ATWS modifications and, as previously discussed, that an average of 290 nuclear power plants would be in operation during the next 30 years, the chances of an ATWS-caused core melt with significant offsite consequences would be about four in seven. The present worth of both the direct and indirect risks of such an accident is between $4.5 and $8.5 billion, using numbers from Table IV.[1/] However, if all plants were modified so that the probability of an ATWS core melt were reduced to 1×10^{-6} per reactor-year, the chance of such an occurrence would be reduced to one in 125 during the next 30 years, and the total present value of the direct risks would be between $10 and $50 million. As stated previously, the total cost of such modifications would be substantially less than $2 billion to achieve this substantial risk reduction.

1/ For perspective purposes, this $4.5 to $8.5 billion should be compared to other risks commonly accepted today. The present worth property damage costs (excluding health effects) of automobile accidents in the United States could be projected to be about $80 billion during this same 30-year period.

It is clear that the numbers presented in Table IV could vary substantially in magnitude depending on the reader's perception as to the probabilities, consequences, and monitization of health impacts of an ATWS core melt. Also uncertain are future decisions that could be made by NRC regarding the speed of making ATWS modifications and/or the number of reactors that might be shut down for modifications, if such modifications were not required now and an ATWS core melt occurred at some future date. The staff believes that the results of the value-impact analysis supports a decision to require ATWS modifications for the following reasons:

1. The range of numbers presented in Table IV indicates that the value likely exceed the impact.

2. While there are substantial uncertainties in Table IV, it is not clear that there is any substantially greater likelihood for decreasing the value relative to the impact.

3. In the face of such uncertainties where there are substantial (although unlikely) consequences involved, it is prudent to propose a conservative decision that averts such risks.

As stated previously, the impact of the staff's ATWS requirements can be substantially increased if construction delay or downtime is required to make them. For example, if ATWS modifications were required to be made

immediately, this might require operating plants to be shutdown for one year. If these same modifications were allowed to be made over an extended period of time, they might be accomplished without extensive additional shutdowns. For example, if a two-year period were allowed for an individual plant, the incremental value of the immediate implementation would range from about $0.5 to $9 million (depending on the type of plant) due to the reduction in the risk of an ATWS event in the two-year period. The incremental impact of the immediate shutdown, however, would be $50 million for each plant due to the differential cost of the replacement power for a one-year period. Thus immediate implementation does not appear to be supported, unless other intangible factors are given very great weight.