UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

AEOD/E114

JUN 2 4 1981

This is an internal, pre-decisional document not necessarily representing a position of AEOD or NRC.

MEMORANDUM FOR: Carlyle Michelson, Director
Office for Analysis and Evaluation
of Operational Data

THRU: Matthew Chiramal
Plant Systems Unit
Office for Analysis and Evaluation
of Operational Data

FROM: Frank Ashe
Plant Systems Unit
Office for Analysis and Evaluation
of Operational Data

SUBJECT: CONTROL SYSTEM FAILURES THAT COULD CAUSE OR EXACERBATE NUCLEAR POWER PLANT ACCIDENTS

During the morning session of the 253rd ACRS meeting held on May 7, 1981, the committee met to discuss the subject issue. This discussion was in response to a request stated in a letter dated December 12 1980 from Dr. Ahearne regarding this issue. Representatives from the Office of Nuclear Reactor Regulation (NRR) and a member from the Office of Nuclear Regulatory Research were present. NRR representatives provided two presentations, these being: a summary of NRC staff position on review of control systems and a status report and conceptual outline of Task Action Plan A-47, "Safety Implications of Control Systems" (Enclosures 2 and 3 respectively). Enclosure 2 also provides a specific discussion of two issues which have been raised, these being 1) de-rating plant operating power levels until additional reviews of the consequences of control system failures can be completed and 2) the desirability of performing failure modes and effects analyses on each vendor's control system design. NRR does not presently plan to adopt either of these recommendations.

The member from the Office of Nuclear Regulatory Research expressed a more conservative view regarding priority, formulated course of action and possible safety consequences due to control system failures than those outlined and stated by the NRR staff representatives. Further, the member from the research office indicated that recent information raised concerns relating to structural integrity of an irradiated reactor pressure vessel to include fracture during overcooling and/or overpressurization transients. These transients being caused by control and/or protection systems actions and/or inactions. In addition, this member indicated that the Office of Nuclear Regulatory Research would initiate actions to include possible contractual arrangements to obtain findings which further define concerns associated with structural integrity of an irradiated reactor vessel due to pressurized thermal shock phenomena.

Enclosure 1 provides comments from the plant systems unit concerning this issue and includes comments relating to Enclosures 2 and 3. In general, we are in agreement with the course of action being followed for this issue as modified by these comments. These comments may be provided for consideration during the comment period for the final drafts of Task Action Plan A-47, "Safety Implications of Control Systems" and/or the revised Section 7.7 of the Standard Review Plan, "Control Systems not Required for Safety" (to include possible title revision of this section). For convenience, a list of references which relate to this issue is also included.

Frank Ashe
Plant Systems Unit
Office for Analysis and Evaluation
of Operational Data

Enclosures:
As Stated

cc w/enclosures:
J. Heltemes
M. Chiramal

ENCLOSURE 1

Comments From The Plant Systems Unit
Concerning Control Systems Failures That Could
Cause Or Exacerbate Nuclear Power Plant Accidents

1. Enclosure 2 presents an accurate description of how control systems have been traditionally viewed by the nuclear regulatory technical review staff. In general, review and evaluation of control system designs have not been performed, this view being predicated on the philosophy of separate control and protection systems and that protection system actions bound control system actions such that core design limits are not exceeded. However, in actual plant designs total separation of these two systems is not obtained and as such hidden influences exist between these two systems (that is, control system actions which influence protection system actions and protection system actions which infuence control system actions). These influences have not been well defined in the past and as such their safety consequences could not be assessed. In an attempt to closer define these influences the NRR technical staff has outlined the following four items for usage during reviews of plant control systems:

    1. Confirm that the plant accident analyses in Chapter 15 of the SAR do not rely on the operability of control systems to assure safety.

    2. Confirm that the safety analyses include consideration of the effects of both control systems action and inaction in assessing the transient response of the plant for accidents and anticipated operational occurrences.

    3. Confirm that consequential effects of anticipated operational occurrences and accidents do not lead to control systems failures which would result in consequences more severe than those bounded by the analyses in Chapter 15 of the SAR.

    4. Confirm that the failure of any control system component or any auxiliary supporting system for control systems will not cause plant conditions more severe than those bounded by the analyses of anticipated operational occurrences in Chapter 15 of the SAR (the evaluation of multiple independent failures is not intended).

Traditionally, items 1 and 2 have been considered extensively during technical reviews by the regulatory staff, however items 3 and 4 have not. Since items 3 and 4 require extensive knowledge of plant specific physical layouts of equipment and details relating to computer codes used for the accident analyses respectively, it is highly questionable as to whether any plant review can give much consideration to these items within the present framework of the review process. As such, a limited system's process variable type of analysis may yield more meaningful results - particularly for the main feedwater system.

2. At the ACRS meeting the member from the research staff did not make a firm technically based argument to support the recommendations of 1) derating plant operating power levels until additional review of the consequences of control system can be completed and 2) the desirability of performing failure modes and effects analyses on each vendor's control system design. However, this member did note an interesting concern regarding structural integrity of an irradiated vessel and how pressurized thermal shock phenomena may effect this integrity; the latter being caused by primary system parameter variations due to control and/or protection system actions. In this regard, the idea that the Office of Nuclear Regulatory Research is attempting to obtain findings which further define concerns associated with structural integrity due to this phenomena is good. It appears that these actions should be aimed at further definition under equivalent operating conditions of nil-ductility temperature limits associated with the reactor pressure vessel.

3. The value of a general Failure Modes and Effects Analysis of control systems from each of the NSSS vendors is questionable since from an operational data viewpoint perturbations by control systems are generally initiated by ancilliary devices such as process sensor transducers, final actuation device controllers, final actuated equipment, and power supplies rather than the central processing units of the control systems. Further, the wide variations in the functional characteristics of these devices their different failure modes and the actual arrangement of these elements in a particular control system, tend to negate general conclusions based on general analyses. Accordingly, plant specific failure modes and effects analyses which concentrates on these ancillaries and incorporates the central processing units as a black box would perhaps yield additional meaningful information concerning this issue. Finally, to assist in determining if control systems are inherently designed correctly (that is, given a set of process variable conditions does the control system act to maintain, change or limit these variables desireably, assuming that it responses as designed?) limited systems type process variable analyses would be helpful.

4. With regard to Enclosure 3 which contains a conceptual outline of Task Action Plan A-47, Safety Implications of Control Systems, this outline implicitly contains only tasks which relate to the reactor systems area. Since the problem of control systems as defined is the desirable and acceptable control of process variables (e.g., pressure, temperature), explicit tasks relating to this area should also be included in this action plan.

5. Finally, as an interim item, AEOD may wish to verify or monitor primary system parameters namely temperature and pressure during selected operating plant transients due to control system actions, so as to assure that the rate of change of these parameters do not exceed that of the corresponding curves as specified in the plant's technical specifications. Measurements of these parameters during transient conditions should be taken from monitors which are physical located nearest to the reactor pressure vessel, as far as practical.

REFERENCES

1. Issues 6 and 15, "Protection Against Single Failures in Reactivity Control Systems" and "Overpressurization", respectively of NUREG-0138 (Staff Discussion of Fifteen Technical Issues Listed In Attachment To November 3, 1976 Memorandum From Director, NRR to NRR staff), date published November 1976.

2. Issues 22 and 23, "Systematic Review of Normal Plant Operation and Control Systems Failures" and "Integrity of Steam Generator Tubes", respectively of NUREG-0153 (Staff Discussion Of Twelve Additional Technical Issues Raised By Responses To November 3, 1976 Memorandum From Director, NRR To NRR Staff), date published December 1976.

3. BAW-1564, Integrated Control System Reliability Analysis, dated August 1979.

4. Memorandum from Demetrios L. Basdekas to Commissioner John F. Ahearne, dated September 4, 1979, Safety Implications of Control Systems and Plant Dynamics.

5. Letter from Morris K. Udall, Chairman, Subcommittee on the Energy and the Environment to the Honorable John Ahearne, Chairman, Nuclear Regulatory Commission dated February 7, 1980.

6. Letter from Demetrios L. Basdekas, Reactor Safety Engineer, to the Honorable Morris K. Udall, Chairman, Subcommittee on the Energy and the Environment, dated May 28, 1980.

7. Memorandum from Demetrios L. Basdekas, Reactor Safety Engineer, to James R. Tourtellotte, Assistant Chief Hearing Counsel, dated October 10, 1980, Safety Implications of Control Systems and Plant Dynamics, And Their Relevance To The TMI-1 ASLB Hearing.

8. Letter from Demetrios L. Basdekas, Reactor Safety Engineer, to the Honorable Morris K. Udall, Chairman, Subcommittee on Energy and the Environment, dated April 10, 1981.

9. Letter from Morris K. Udall, Chairman, Subcommittee on Energy and the Environment, to the Honorable Joseph Hendrie, Chairman, Nuclear Regulatory Commission, dated May 1, 1981.

10. Letter from J. Carson Mark, Chairman, Advisory Committee on Reactor Safeguards, to Honorable Joseph M. Hendrie, Chairman, U.S. Nuclear Regulatory Commission, dated May 12, 1981 (In response to the requested from Dr. Ahearne in a letter dated December 12, 1980).

11. Letter from William J. Dircks, Executive Director for Operations, to Dr. J. Carson Mark, Chairman, Advisory Committee on Reactor Safeguards, dated May 29, 1981, Unresolved Safety Issue: Safety Implications of Control Systems, Task A-47.

ENCLOSURE 2

Prepared on 5/5/81

SUMMARY OF NRC STAFF POSITION ON

REVIEW OF CONTROL SYSTEMS

Two meetings of the Electrical Systems Subcommittee have been held at which the staff has:

1) summarized past practice with respect to the review of control systems.
2) summarized staff actions currently in progress or planned for the near future on control systems.
3) Answered subcommittee questions on the staff approach to the review of control systems.

Today, I would like to briefly recap what was said at the subcommittee meetings concerning staff philosophy on the review of control and protection systems and delineate actions underway or planned for the near future to address the effects of control systems on plant safety. I will then specifically discuss two issues which have been raised, these being:

1) de-rating plant operating power levels until additional review of the consequences of control system failures can be completed
2) the desirability of performing failure modes and effects analyses on each vendor's control system design.

The philosophy on the separation of protection systems and control systems was developed in the 1960s and early 1970s through interactions between the regulatory staff and industry. The interactions occurred primarily through the development of industry standards such as IEEE-279. The staff did not dictate a particular philosophy, but rather explored through the standards committees and early plant licensing reviews various approaches which could be taken towards reactor protection.

Contact:
C. Rossi
X29431

A brief, simplified description of the approach towards protection and control is as follows. A nuclear power plant must satisfy utility requirements for the economic production of power. These requirements include plant operation with a limited number of operators, high plant availability with few unplanned shutdowns, and the ability to follow the utility grid load demand. The requirements for operation are based largely on matching the capabilities of non-nuclear plants. Plant control systems to accomplish the desired economic operational characteristics are established. The control systems, of course, have to be capable of allowing the plant to perform normal operations with margin to plant safety limits.

To assure that safety limits are not exceeded should any system used for normal operation fail, various protective functions such as reactor trip and decay heat removal have been established in the Commission regulations. Systems whose primary purpose is to accomplish the protective functions are provided to fulfill these requirements.

One, thus, has two somewhat differing objectives. The first is to allow normal plant operation within a utility grid which is also supplied by many non-nuclear plants. For this, control functions have been established. The second objective is to insure that even with failures of the operational equipment, safety limits are not exceeded. For this, protective functions have been established to assure plant safety.

Once control functions and protective functions are defined, a decision has to be made as to whether the same systems should be used for both or whether separate systems should be used. The philosophy developed through the standards committees was one in which the protection systems were treated separately. This allowed a set of guidelines to be established with the intent of insuring that

protection functions are accomplished with a very high degree of reliability. Having a specific, well defined group of protection systems to accomplish required safety functions allows both industry and the regulatory agency to concentrate their efforts and make effective use of limited resources in accomplishing safety goals.

In development of the philosophy, it was recognized that some limited ties between protection systems and control systems are appropriate and even unavoidable. For example, the systems will always be interrelated through the fluid process systems. Additional interfaces such as the use of the same sensors for protection and control were considered acceptable providing appropriate rules are followed. General Design Criterion 24 and IEEE-279 permit limited interconnections between protection and control systems and define rules for implementing these interconnections.

NRC staff reviews have been performed on currently licensed plants with the goal of insuring that control system failures will not prevent automatic or manual initiation and operation of any safety system equipment required to trip the plant or maintain the plant in a safe shutdown condition following any "anticipated operational occurrence" or "accident." The approach has been to either provide independence between safety and non-safety systems or to require isolating devices such as isolation amplifiers between safety and non-safety systems such that failures of non-safety system equipment cannot propagate through the isolating devices to impair operation of the safety system equipment. In addition, a specific set of "anticipated operational occurrences" and "accidents" have been analyzed to demonstrate that plant trip and/or safety system equipment actuation occurs with sufficient capability and on a time scale such that the consequences are within specified, acceptable limits. In these analyses, conservative initial plant conditions,

core physics parameters, and instrumentation setpoints have been assumed. Conservative core parameters(for example, heat fluxes, temperatures, pressures, and flows) which could result in core damage are also assumed. Where active control system operation would mitigate the consequences of a transient, in general, no credit is taken for the control system operation. Where active control system operation would not mitigate the consequences of a transient, no penalties are taken in the analyses for incorrect control system actions caused by control system equipment failures. In the case of control systems, for example, the loss of forced reactor flow is analyzed assuming the reactivity control systems either operate properly or do not operate at all, whichever is the worst case. A loss of forced reactor flow occurring simultaneously with an inadvertent rod withdrawal is not considered. Among the specific set of "anticipated operational occurrences" analyzed are occurrences resulting from both mechanistic and non-mechanistic control system failures. The conservative analyses performed are intended to demonstrate that the potential consequences to the health and safety of the public are within acceptable limits for a wide range of postulated events even though specific actual events might not follow the same assumptions made in the analyses.

In general, systematic evaluation of control systems designs have not been performed to determine whether single failure or single event induced multiple control system actions could result in a transient such that core limits established for "anticipated operational occurrences" are exceeded. Single failures or events which could induce multiple control system actions would presumably include events such as a loss of power supply.

If single failure or event induced multiple control system actions such as discussed above do indeed exist, experience with operating plants indicates that incidents resulting in transients more severe than currently analyzed as

"anticipated operational occurrences" have a low probability.

Systematic evaluations of control system designs have not been performed to determine whether postulated accidents could cause control system failures resulting in control actions which would make accident consequences more severe than presently analyzed. Licensees have, however, been requested to review the possibility of consequential control system failures which exacerbate the effects of high energy line breaks and to take action where needed, to assure that the postulated events would be adequately mitigated. Accidents could cause control system failures by creating a harsh environment in the area of the control equipment or by physically damaging the control equipment. Also, control equipment damage and a transient could have a common cause through some event such as a fire. It should be emphasized that the issue is not whether reactor trip or safety system equipment action would be defeated by control system failures, but whether control system failures could cause a transient to proceed in a manner potentially more severe than currently analyzed. Systematic reviews of safety systems have been performed with the goal of insuring that control system failures (single or multiple) will not defeat trip or safety system action.

The consensus judgment of the NRC staff is that the risk associated with control system failures is not sufficient to require immediate corrective actions. However, to provide added assurance that the current licensing practices are adequate, the following actions are underway:

1) The Commission has designated the "Safety Implications of Control Systems" as an Unresolved Safety Issue.

2) B&W has completed a failure modes and effects analysis and review of operating experience for their Integrated Control System (ICS) and

reported the results in B&W Report BAW-1564, "Integrated Control System Reliability Analysis." B&W made several recommendations regarding control system improvements which could be made to improve overall plant performance. Licensees with B&W plants were requested to evaluate the B&W recommendations and report their follow-up actions to the staff. Responses have been received and reviewed. Meetings are being arranged with licensees to evaluate the responses in greater depth. The first of these meetings is scheduled with Duke Power Company at the end of this month.

3) In September, 1979, all licensees were asked to review the possibility of consequential control system failures which could exacerbate the effects of high energy line breaks and identify appropriate actions, where needed, to assure that these events would be adequately mitigated. The review was requested as a result of postulated scenarios involving consequential control system failures identified by Westinghouse. All licensees responded to the request and the responses were screened. On the basis of the review, no specific event leading to unacceptable consequences was identified and, in general, control equipment locations were such that consequential failures would be unlikely. Some licensees, however, did make changes to operating procedures to address the possibility of control failures. Although in-depth, systematic reviews were not made by the staff, with considerable reliance being placed on the reviews conducted by the licensees, the Systems Interactions Program includes plans for such reviews. This item

is also currently being pursued on operating license applications.

4) I&E Bulletin 79-27 was issued to licensees requesting that evaluations be performed to ensure the adequacy of plant procedures for accomplishing shutdown upon loss of power to any electrical bus supplying power for instruments and controls. In their responses to the bulletin, licensees have indicated that corrective action has been taken including hardware changes and revised procedures, where required, to assure that the loss of any single instrument bus would not result in the loss of instrumentation required to mitigate such an event. As part of OL licensing reviews, we are requesting similar reviews by OL applicants.

5) The Office of Standards Development is coordinating efforts with the IEEE to establish design criteria for systems important to safety which are not covered by and do not need to meet all of the rigorous standards for safety system equipment but nevertheless are sufficiently important to safety to be included in the NRC review process.

6) Implementation of Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During And Following An Accident," NUREG-0737, "Clarification of TMI Action Plan Requirements," and NUREG-0696, "Functional Criteria for Emergency Response Facilities" will significantly upgrade both the quantity and quality of information available to the operator to diagnose and respond to control system failures.

7) Standard Review Plan Section 7.7 calls for staff reviews to assure that failures of control systems will not impair the capability of

the protection system in any significant manner or cause plant conditions more severe than those for which the plant safety systems are designed. The staff has pursued these reviews primarily to ensure that electrical interconnections between protection systems and control systems are implemented such that failures in control system equipment cannot impair the operation of protection system equipment. The Chapter 15 design basis events analyses have also been reviewed to assure that sufficient conservatism has been assumed so that these analyses adequately bound the consequences of single control system failures. The Instrumentation and Control Systems Branch is currently reviewing control systems designs of OL applicants to confirm that the Chapter 15 design basis analyses also bound multiple control system failures, initiated by credible malfunctions of common power sources or sensors. In addition we have requested that the potential for control system malfunctions caused by high energy line breaks be reviewed by OL applicants. Section 7.7 of the Standard Review Plan is being revised to be more explicit on criteria applicable to control systems. Specifically, the criteria shown on this viewgraph will be delineated in Section 7.7 and reviews of plants currently under licensing review will be performed with the goal of verifying that the criteria are met.

At this time, we know of no specific control system failures or actions which would lead to unacceptable consequences. I have described a variety of efforts underway to determine the potential safety consequences of control system failures. Should these reviews indicate that additional criteria for control system designs are necessary or that specific problems require resolution, appropriate action will be taken for plants in the licensing process and for plants now in operation.

I would now like to discuss two specific issues which have been raised concerning control systems. The first is a suggestion that plant operating power levels be reduced until additional review of the consequences of control system failures are completed. Reducing plant operating power levels and making reactor trip setpoints more limiting would provide additional margin to core design limits and reduce residual heat generation after a transient, accident, or normal shutdown. Additional margin to core design limits would increase the probability of maintaining the conservative limits used for "anticipated operational occurrences" -- basically no core damage -- for multiple control system failures. Since operating experience has shown that multiple control system failures resulting in transients more severe than currently analyzed as "anticipated operational occurrences" have a low probability, power reductions to provide additional margin to core design limits are not justified. Reducing residual heat generation after plant trip would provide the operator with more time to cope with confusing indications or transients after shutdown for situations where required operator time is primarily dependent upon the integrated residual heat produced. However, I would like to reiterate that there is today no known specific control system failure or action which would lead to unacceptable consequences. There is, thus, no basis for selecting a reduced power level other than "lower is safer". The staff conclusion is that power reductions are not warranted.

Now, let me turn to Failure Modes and Effects Analyses. Failure Modes and Effects Analyses have been required for B&W plants because the control on these plants is based upon simultaneous close coordination of several key plant parameters. This close coordination is believed to be necessary because of the transient response of these plants which results from having smaller steam generator fluid inventories. The analysis of the Integrated Control System indicated that the system has a low failure rate and the system does

not appear to precipitate a significant number of plant upsets. Furthermore, no specific event initiated by the Integrated Control System was identified which would have unacceptable safety consequences. The staff does have some additional concerns about the effects of failures in systems with which the Integrated Control System interfaces - for example, the power supplies to the system. As stated before, these concerns are being pursued.

At this time, the staff considers the approach which was previously described to be a better approach in determining if and where control systems may cause safety problems, rather than requesting Failure Modes and Effects Analyses for the other NSSS vendors. As the unresolved safety issue resolution proceeds, it may be that Failure Modes and Effects Analyses will be useful. However, we believe that many types of analyses, not just FMEA, will provide the tools to review control systems, and bring the issue to the point of resolution.

TABLE 1

STANDARD REVIEW PLAN

GUIDANCE FOR CONTROL SYSTEM REVIEW

1. CONFIRM THAT THE PLANT ACCIDENT ANALYSES IN CHAPTER 15 OF THE SAR DO NOT RELY ON THE OPERABILITY OF CONTROL SYSTEMS TO ASSURE SAFETY.

2. CONFIRM THAT THE SAFETY ANALYSES INCLUDE CONSIDERATION OF THE EFFECTS OF BOTH CONTROL SYSTEMS ACTION AND INACTION IN ASSESSING THE TRANSIENT RESPONSE OF THE PLANT FOR ACCIDENTS AND ANTICIPATED OPERATIONAL OCCURRENCES.

3. CONFIRM THAT CONSEQUENTIAL EFFECTS OF ANTICIPATED OPERATIONAL OCCURRENCES AND ACCIDENTS DO NOT LEAD TO CONTROL SYSTEMS FAILURES WHICH WOULD RESULT IN CONSEQUENCES MORE SEVERE THAN THOSE BOUNDED BY THE ANALYSES IN CHAPTER 15 OF THE SAR.

4. CONFIRM THAT THE FAILURE OF ANY CONTROL SYSTEM COMPONENT OR ANY AUXILIARY SUPPORTING SYSTEM FOR CONTROL SYSTEMS WILL NOT CAUSE PLANT CONDITIONS MORE SEVERE THAN THOSE BOUNDED BY THE ANALYSES OF ANTICIPATED OPERATIONAL OCCURRENCES IN CHAPTER 15 OF THE SAR (THE EVALUATION OF MULTIPLE INDEPENDENT FAILURES IS NOT INTENDED).

ENCLOSURE 3

NRC STAFF STATUS REPORT

ON UNRESOLVED SAFETY ISSUE (USI) - TASK A-47

"SAFETY IMPLICATIONS OF CONTROL SYSTEMS"

FOR THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS MEETING OF

MAY 7, 1981

A. J. Szukiewicz
Generic Issues Branch, DST

STATUS ON A-47

- TASK ACTIVITY ON A-47 DELAYED DUE TO FULL TIME INVOLVEMENT NECESSARY TO COMPLETE USI A-24 (ICSB IS ACTIVELY PURSUING CONTROL SYSTEMS INTERACTION ON SPECIFIC CASE-BY-CASE REVIEWS ON OPERATING REACTORS AND NTOLS).

- FULL TIME ACTIVITY ON A-47 EXPECTED BY JUNE 1, 1981.

ACTION PLAN SCHEDULE

- PREPARE DRAFT TASK ACTION PLAN ON A-47 BY JULY 17, 1981
  PREPARE A SUMMARY OF RELATED ON-GOING ACTIVITIES BY OTHER BRANCHES (E.G., ICSB, RES)

- COMPLETE TASK ACTION PLAN (FOR STAFF CONCURRENCE) BY AUGUST 31, 1981

CONCEPTUAL OUTLINE OF TASK ACTION PLAN A-47

Task 1. Evaluate Control System Failures that Lead to Steam Generator and/or Reactor Overfill Transients.

Task 2. Evaluate Control System Failures that Lead to Reactor Overcooling Transients.

Task 3. Evaluate other Control System Actions that May Have Safety Implications (This task will be the major effort of the Action Plan).

TASK 1

- EVALUATE CONTROL SYSTEM FAILURES THAT LEAD TO STEAM GENERATOR AND/OR REACTOR OVERFILL TRANSIENT

1. IDENTIFY CONTROL SYSTEMS WHOSE FAILURES COULD LEAD TO STEAM GENERATOR AND REACTOR OVERFILL TRANSIENTS (NSS AS WELL AS BOP DESIGNS).

2. ESTABLISH CRITERIA FOR DETERMINING THE SAFETY IMPACT OF THE IDENTIFIED CONTROL SYSTEMS. FOR EXAMPLE CAN A FAILURE CAUSE A TRANSIENT WHICH:

   A. MAY VIOLATE THE INTEGRITY OF THE STEAM PIPING OR DEGRADE SAFETY SYSTEM OPERATION (CAVITATE AUX. FEEDWATER PUMPS).
   B. MAY CAUSE RPS PRESSURE-TEMPERATURE LIMITS TO BE EXCEEDED.
   C. CAUSE UNWARRANTED CHALLENGES TO THE RPS.
   D. MAY CAUSE PARTIAL PERFORATION OR MELTING OF THE FUEL CLADDING.

3. GROUP THE CONTROL SYSTEMS IN THEIR ORDER OF IMPORTANCE (I.E., IMMEDIATE OR DELAYED EFFECTS ON OVERFILL).

4. IDENTIFY FAILURE MECHANISMS OF THE CONTROL SYSTEMS ESTABLISHED IN (3) -- FMEA, EVENT OR FAULT TREE ANALYSIS OR OTHER METHODS COULD BE USED.

5. DEFINE CRITERIA FOR CORRECTIVE ACTION TO MINIMIZE THE CONSEQUENCES OF THE TRANSIENT, E.G.,

   A. PROVIDE ADDITIONAL SAFETY ACTION (HIGH LEVEL TRIP OR HIGH LEVEL MODULATING CONTROLS).
   B. SEPARATE POWER SUPPLIES.
   C. PROVIDE ADDITIONAL REDUNDANCY, DIVERSITY AND/OR QUALIFICATION.
   D. IMPROVE OR PROVIDE ADDITIONAL TESTING OR SURVEILLANCE.

Task 2

Evaluate Control System Failures that Lead to Reactor Overcooling Transients

- Identify the control systems that can cause primary system overcooling transients.
- Establish criteria for determining the safety impact of the identified control systems. For example, failure that could lead to (1) a rapid loss of pressurizer level and reactor coolant temperatures, (2) primary system over-pressurization.
- Identify failure mechanisms of the control systems -- FMEA event or fault tree analysis or other methods could be used.
- Define criteria for corrective action to minimize the consequences of the transient(s) (e.g., provide additional safety action such as additional pressure relief capability at specific conditions or provide safety systems that would override, with margin, the control systems, etc.)

TASK 3

EVALUATE OTHER CONTROL SYSTEM ACTIONS THAT MAY HAVE SAFETY IMPLICATIONS

- IDENTIFY CONTROL SYSTEMS WHOSE FAILURE COULD CAUSE PRIMARY REACTOR SYSTEM TRANSIENTS. (REVIEW THE SYSTEMS OF THE 4 NSS SUPPLIERS AND REVIEW THE BOP DESIGNS.)

- ESTABLISH CRITERIA FOR DETERMINING THE SAFETY IMPACT OF THE IDENTIFIED CONTROL SYSTEMS.
  FOR EXAMPLE, FAILURES THAT MAY CAUSE TRANSIENTS THAT:
  1. MAY CAUSE RPS PRESSURE-TEMPERATURE LIMITS TO BE EXCEEDED,
  2. CAUSE UNWARRANTED CHALLENGES TO THE RPS,
  3. MAY CAUSE PARTIAL PERFORATION OR MELTING OF THE FUEL CLADDING.

- GROUP THE CONTROL SYSTEMS IN ORDER OF THEIR IMPORTANT (I.E., 1ST OR 2ND ORDER EFFECTS ON THE PRIMARY SYSTEM.)

- IDENTIFY COMBINATIONS OF THE CONTROL SYSTEMS THAT COULD CAUSE UNACCEPTABLE EFFECTS (I.E., LOSS OF FEEDWATER AND CONTROL ROD WITHDRAWAL).

- GROUP THE CONTROL SYSTEM COMBINATIONS AND ESTABLISH THEIR ORDER OF IMPORTANCE. (CRITERIA TO LIMIT THE NUMBER OF COMBINATIONS MAY BE NEEDED).

- IDENTIFY FAILURE MECHANISMS OF THE COMBINATIONS. FMEA EVENT TREE OF FAULT TREE ANALYSIS OR OTHER METHODS WOULD BE USED.

- DEFINE CRITERIA FOR CORRECTIVE ACTION TO MINIMIZE THE CONSEQUENCES OF THE TRANSIENT (E.G., PROVIDE ADDITIONAL SAFETY ACTION, PROVIDE SEPARATE POWER SUPPLIES, PROVIDE ADDITIONAL TESTING AND SURVEILLANCE, PROVIDE ADDITIONAL REDUNDANCY, DIVERSITY, AND/OR QUALIFICATION).