operational experience. We would appreciate the opportunity to discuss this issue further with your staff and the approach EG&G is taking and, to solicit your cooperation in expediting this review effort. We also encourage your comments on the information provided to you. If you have any questions or comments, do not hesitate to contact me or Andrew Szukiewicz the Task Manager for A-47 (301/492-4713).

Sincerely,

/S/

Darrell G. Eisenhut, Director
Division of Licensing

Enclosures:
1. List of Information Needs
2. Task Action Plan USI A-47
(dated September 1982)

cc: w/enclosures:
See next page

DISTRIBUTION
Docket Files
NRC PDR
Local PDR
ORB-1 File
GIB Rdg
A-47 File
DEisenhut FSchroeder
OELD KKniel
EJordan PNorian
GRequa ASzukiewicz
CParrish SBruske (EG&G
NSIC
JTaylor
ACRS (10)
TSpeis
DST c/f
SVarga
GLainas

Concurred by Eisenhut on 6/17/83.

ORB 1
GRequa
6/13/83

DL:AD/OR
GLainas
6/14/83

OFFICE	DST:GIB	DST:GIB	DST:GIB	DST:ADGP	DST:D	DL:ADOR/ORB	DL:D
SURNAME	ASzukiewicz:cb	PNorian	KKniel	FSchroeder	TSpeis	SVarga	DEisenhut
DATE	5/18/83	5/18/83	5/18/83	5/20/83	5/20/83	6/ /83	6/ /83

#40

NRC FORM 318 (10-80) NRCM 0240 **OFFICIAL RECORD COPY** USGPO: 1981—335-960

DAD 016

JUN 20 1983

Docket No. 50-261

Mr. E. E. Utley, Executive Vice President
Power Supply and Engineering & Construction
Carolina Power and Light Company
411 Fayetteville Street
Raleigh, North Carolina 27602

Dear Mr. Utley:

On June 16, 1982, a meeting was held in Raleigh, North Carolina between Carolina Power and Light Company (CP&L) and members of the Nuclear Regulatory Commission (NRC) staff to discuss CP&L participation in developmental programs addressing Unresolved Safety Issue (USI A-47) "Safety Implications of Control Systems." At that time CP&L declined participation, but indicated in a subsequent meeting on July 19, 1982 that it would re-evaluate our program plan when completed and perhaps reconsider the decision to participate in A-47. Since that time the following milestones have been accomplished:

(1) In September 1982 an NRC approved Task Action Plan for USI A-47 was completed. This document describes the tasks that will be conducted to resolve this USI (copy of the plan is attached).

(2) A contract was issued to EG&G Idaho (INEL) to assist the staff in the review of the H. B. Robinson plant design. This contract will be managed directly through the Generic Issues Branch in the Division of Safety Technology, NRR.

A systematic review of the control and electrical power systems will be performed, and will inc ude the performance of failure mode and effects analysis (FMEA) to ide ify and define credible potential control system scenarios whose failu could lead to significant plant transients. The evaluation of the mo mplex control system failure scenarios will be performed on a plar ecific simulation. The computer programs are currently being modified to esent the control systems under consideration. We have chosen EG&G at Id alls to perform the evaluation for the H. B. Robinson plant design beca of their current on-going review and the computer modeling effort f SI A-49, "Pressurized Thermal Shock." As you know CP&L has included our A-49 effort (evaluating the potential for over-cooling

OFFICE ▶							
SURNAME ▶							
DATE ▶							

NRC FORM 318 (10-80) NRCM 0

OFFICIAL RECORD COPY

USGPO: 1981—335-96

transients at H. B. Robinson) as a significant element of your program on the pressurized thermal shock issue as described in your letter to Harold Denton dated December 7, 1982. The expertise gained as a result of the A-49 effort will be utilized by the EG&G A-47 review group.

A substantial reduction in the regulatory burden is achieved since the design information on the control systems for these two issues is, for the most part, the same. We have determined that there is already a considerable amount of design information available at EG&G on the design of the H. B. Robinson plant; however, some additional information is needed. In many cases, all that we need is verification, on a selected basis, that the information being utilized represents the as-built design. However, for some selected non-class IE instrumentation and control support systems we need information that is normally not provided in the FSAR. The attached listing identifies systems for which this appears necessary.

We wish to explore with CP&L possible ways we can improve the specificity of the information we need and minimize the impact on your resources in obtaining it. One approach might be to have cognizant NRC and/or EG&G personnel establish an informal working arrangement with a CP&L representative who has been involved with plant design drawings and design information. This working arrangement could significantly aid in improving the specificity of our requests for information by identifying, for example, the specific drawings that would provide the information needed for the study. EG&G engineers could be made available to review the available information at the plant site. Also, we intend to have the NRC resident inspector at H. B. Robinson assist us in obtaining the needed information, whenever possible, to minimize impact on your manpower.

In addition, our contractor (EG&G) has indicated that significant information may be obtained from Westinghouse. Westinghouse indicated that they would be willing to provide EG&G with the necessary information, provided that this type of information exchange would be acceptable to CP&L.

As you see, considerable additional planning and task definition has been accomplished since our first meeting on USI A-47 in Raleigh. The tasks identified in the USI task action plan include consideration of any applicable results from the Interim Reliability Evaluation Program (IREP), available Probabilistic Risk Assessment (PRA), and lessons learned from

Mr. E. E. Utley
Carolina Power and Light Company

cc: G. F. Trowbridge, Esquire
Shaw, Pittman, Potts and Trowbridge
1800 M Street, N.W.
Washington, D. C. 20036

U. S. Nuclear Regulatory Commission
Resident Inspector's Office
H. B. Robinson Steam Electric Plant
Route 5, Box 266-1A
Hartsville, South Carolina 29550

James P. O'Reilly
Regional Administrator - Region II
U. S. Nuclear Regulatory Commission
101 Marietta Street - Suite 3100
Atlanta, Georgia 30303

ENCLOSURE 1

LIST OF INFORMATION NEED
H. B. ROBINSON UNIT NO. 2

Systems for which electrical controls logic diagrams and instrument schematics are needed.

Turbine Electrohydraulic System
Main Feedwater and Condensate System
Steam Generator Blowdown System
Steam Generator Sampling System
Turbine Generator and Support System
Auxilliary Steam System
Main Condenser System
Main Condenser Evacuation System
Steam Dump System
Condenser Circulating Water System
Primary and Demineralized Water Makeup System
Service and Instrumentation Air Systems
Spend Fuel Pool Cooling and Cleanup System
Annunciator System
Backup Control System
Reactor Coolant Pump Control
Reactor Instrumentation
Steam Generator Level and Feedwater Flow Control System
Main Steam System
Nitrogen Purge System
120 Volt Instrument Buses
Station Normal Auxiliary Power
Steam Line Overpressure System
Pressurizer Overpressure Protection System
Chemical and Volume Control System (CVCS)
Station Emergency Auxiliary Power System
Process Computer (Schematics of Inputs and Output Terminals and List of Input and Output parameters are needed)

ENCLOSURE 2

TASK ACTION PLAN

(September 1982)

SAFETY IMPLICATIONS OF CONTROL SYSTEMS (TASK A-47)

Lead Organization:	Division of Safety Technology (DST) Generic Issues Branch (GIB)
Task Manager:	A. J. Szukiewicz, GIB, DST
Lead Supervisor:	Karl Kniel, Chief, GIB, DST
NRR Principal Reviewers:	Charles Rossi Instrumentation and Control Systems Branch Division of Systems Integration
	Frank Orr Reactor Systems Branch Division of Systems Integration
	A. S. Gill Power Systems Branch Division of Systems Integration
	James T. Beard Operating Reactors Assessment Branch Division of Licensing
	Chelliah Erulappa Reliability and Risk Assessment Branch Division of Safety Technology
	William G. Kennedy Procedures and Test Review Branch Division of Human Factors Safety
AEOD Lead Reviewer:	Matthew Chiramal Plant Systems Unit
RES Lead Reviewer:	Demetrios Basdekas Division of Facility Operations
Applicability:	Light Water Reactors (Pressurized Water Reactors and Boiling Water Reactors)
Projected Completion Date:	March 1984

1. DESCRIPTION OF PROBLEM

Non-safety grade control systems are used to maintain the plant within the necessary pressure and temperature limits during normal shutdown, startup, and load varying power operation. The control systems are not relied upon to perform any safety functions following postulated accidents but are required to control plant processes that could have a significant impact on plant safety. Those control systems include the reactivity control systems, and reactor coolant pressure, temperature, level, flow and inventory controls (that is, borated water controls). In addition, they include secondary system pressure and flow controls (pressurized water reactor) as well as the associated support systems such as electric, hydraulic and/or pneumatic power supply systems.

During the licensing process, the staff performs an audit review of the non-safety grade control systems, on a case-by-case basis, to assure that an adequate degree of separation and independence is provided between these non-safety grade systems and the safety systems, and that effects of the operation or failure of these systems are bounded by the accident analysis in Chapter 15 of the plant's Safety Analysis Report (SAR). Typical events that are addressed by the licensees, and are evaluated by the staff in the audit review include, but are not limited to: (1) the feedwater system malfunctions that result in a decrease or an increase in the feedwater flow (including the loss of the normal feedwater flow); (2) the steam pressure regulator malfunctions or failures that result in an increase or a decrease in the steam flow (including the turbine trip event); (3) a spectrum of reactivity addition events; and (4) chemical and volume control malfunctions that increase the reactor coolant inventory or decrease the boron concentration.

On this basis it is generally believed that control system failures are not likely to result in loss of safety functions that could lead to serious events or result in conditions that the safety systems are not able to mitigate. Indepth studies for all the non-safety grade systems

have not been performed however, and there exists some potential for accidents or transients being made more severe than previously analyzed, as a result of some of these control system failures or malfunctions.

The control system failures or malfunctions may occur independently or as a result of an accident or transient under consideration. Failures or malfunctions may also occur as a result of a common mode or a system interaction that could make recovery to normal safe shutdown conditions difficult.

Two potential concerns have already been identified in which a failure or malfunction of the non-safety grade control system can (1) potentially cause a steam generator or reactor vessel overfill, or (2) can lead to a transient (in PWRs) in which the vessel could be subjected to severe overcooling. In addition, there is the potential for an independent event like a single failure, (such as a loss of power supply, a short circuit, open circuit, control sensor failure) or a common mode event (such as a harsh environment caused by an accident or a seismic event) to cause a malfunction of one or several control systems which would lead to an undesirable control action, or provide misleading information to the plant operator. These concerns will be reviewed and evaluated as part of the tasks discussed in the following sections. It should be recognized that the effects of control system failures during accident or normal plant operation may differ from plant to plant, and therefore it may not be possible to develop generic solutions to these concerns. It is possible, however, to develop generic criteria that can be used for the plant specific reviews.

The purpose of this Unresolved Safety Issue (USI) is to perform an indepth evaluation of the control systems that are typically used during normal plant operation and to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures.

2. PLAN FOR PROBLEM RESOLUTION

In order to best utilize NRC's capabilities and resources, the resolution of the activities described in detail in the following sections will be conducted under contract with the National Laboratories. The responsibility for resolution of this safety issue rests with the Office of Nuclear Reactor Regulation (NRR), but will involve both NRR and the Office of Nuclear Regulatory Research (RES) staff effort to manage and review the adequacy of the evaluations conducted. To scope the issue to a manageable level and bound the generic review to a reasonable completion schedule, Task A-47 will evaluate the non-safety grade systems of three PWR designs and one BWR design.

The task will review the plant designs of the manual and/or automatic control systems for each of the four nuclear steam system supplier (NSSS) designs [Babcock and Wilcox (B&W), Combustion Engineering (CE), General Electric (GE) and Westinghouse (W)] and will include the review of any manual and/or automatic control system that interfaces with the NSSS design or dynamically interacts with the primary reactor fluid system and the secondary steam system. These associated control systems may be supplied or designed by different manufacturers or architect engineers than the NSSS. Two PWR non-safety grade control system plant designs (that is, B&W and CE) will be evaluated by Oak Ridge National Laboratory (ORNL) under contract with RES (FIN No. B-0467). The GE BWR designs will be evaluated by EG&G-Idaho under contract with NRR (FIN No. A-6477). The decision on where the W evaluation will be performed is to be made later on the basis of progress at the two labs.

The task will, for each type design: (1) identify the non-safety grade control system(s) whose failure or misoperation can, (a) cause transients or accidents identifyed in Chapter 15 of the Final Safety Analysis Report (FSAR) to be made potentially more severe than previously analyzed; (b) create the potential to negate the timely action of the automatic protection system or the manual operation of any equipment required to achieve a safe shutdown condition; (2) establish and define the order of importance of the control system(s) identified as having

safety significance; (3) describe the mechanism(s) contributing to the credible failure modes, (that is, loss of power supply or the environmental effects on the control systems); (4) verify the adequacy of the existing design criteria, described in Standard Review Plan Section 7.7, "Control Systems," or develop and propose additional criteria and guidelines to improve system reliability or minimize the consequences of the control system failures that have been identified as safety significant.

To evaluate control system actions that have safety implications, the work effort will focus on the following activities.

- Evaluate control system failures that could lead a steam generator or a reactor vessel overfill transient. (subtask 1 of task 7)

- Evaluate control system failures that could lead a reactor overcooling transient. (subtask 2 of task 7)

- Evaluate (all other) non-safety grade control systems that have safety implications. (overall task)

- Evaluate the effect of loss of power supplies to the control systems. This would include the electrical alternating current (ac) and direct current (dc) supplies also and the pneumatic and hydraulic supplies. (Task 4)

The major activity will be to identify and evaluate non-safety grade control systems that have safety implications. The tasks associated with the activity are outlined below. Subtasks 1 and 2 focus on specific areas of concern identified as part of the overall activity. Additional tasks or subtasks may be identified as the program develops; if other tasks are developed, the Task Action Plan will be revised. 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.

Task Action Plan A-47 has been developed to utilize, whenever possible, any applicable data developed by the following current ongoing activities.

- Resolution of USI A-49 "Pressurized Thermal Shock" (PTS).

- RES activities with ORNL regarding Safety Implications of Control Systems (FIN No. B-0467).

- Systems Interaction Program - A study conducted by the Reliability and Risk Assessment Branch of the Division of Safety Technology (RRAB/DST). TMI Action Plan Item II.C.3 and USI A-17.

- RES activities with Sandia National Laboratories evaluating plant electrical systems interactions (FIN No. A-1324).

The interface between the Task A-47 program and these activities is discussed in more detail in the appropriate tasks.

Task Description

Evaluate Non-Safety Grade Control Systems that Have Safety Implications

This activity will evaluate non-safety grade control systems and identify any non-safety grade control systems whose failure may lead to transients or accidents more severe than those analysed in Chapter 15 of the plant FSAR and to identify non-safety grade control system failures which could produce an unacceptable frequency of occurrence of those transients bounded by Chapter 15. The control systems evaluation will review the designs of each of the four NSS suppliers (B&W, CE, W, GE) and will include the control systems which may be designed by other suppliers but interface with the NSS control system design or dynamically interact with the reactor primary or secondary system. This activity will consist of the tasks listed below. The flow diagram (Figure 1) illustrates the interactions between these tasks.

Task 1 Identify the Systems Whose Failure Can Lead to Significant Primary System Transients

Conduct a review of the automatic and manual control systems that are used during startup, shutdown and normal load varying operations and identify all systems whose failure or malfunction has the potential for causing pressure, temperature, flow and power transients in the primary reactor system. Identify also any control systems whose failure or malfunction before, during or after any transient or accident analysed in Chapter 15 of the FSAR could cause more severe consequences then presently analysed. Gross analysis based on tools such as FMEA, dependency tables or diagrams, functional and system event trees and fault trees and/or any other analytical tools judged to be adequate will be used initially on a system level basis for the purpose of identifying the significant control systems. During this phase, non-mechanistic "worst-case" failure modes of the control systems will be assumed. The major components (such as valves, pumps, control drives, etc.,) whose failure can cause a system malfunction will be identified.

The criteria that will be used for selecting and categorizing the safety significant control systems will be identified. A review of the applicable Licensing Event Reports (LER's), NRC Bulletin and Orders, and NSS emergency procedures and operating guidelines will be conducted. The results of this review will be factored into the criteria selection process and will help to identify safety significant systems. The control systems identified will be compared with those systems described in 1) the IREP study, 2) the applicable studies conducted by selected Near-Term Operating License (NTOL) applicants in response to the Instrumentation and Control Systems Branch control system concerns identified during the NTOL review and 3) the probability and risk assessment (PRA) studies conducted by the utilities on similar designs.

The control systems identified via the activities described above will be compared with the systems identified in the analysis in

Chapter 15 of the FSAR. The safety impact and the order of importance of the systems identified will be described and categorized to define for example, system whose failures initiate significant transients by themselves (i.e., spills, blowdown, etc.,) or systems whose failures can occur concurrent with transients resulting from other initiators. Failures will be limited to independent single failures or multiple failures resulting from a common initiator. An additional independent single failure may also be included if, as part of a specific scenario analysis, it is apparent that such failure is highly likely and the attendant consequences significant. Operator misoperation of control systems is outside the scope of this task if existing procedures, the information available to the operator, and the time for the operator to accomplish the action is sufficient. The control systems whose failure or malfunction may be considered less important or inconsequential or highly unlikely to warrant further study will be identified and the basis for such conclusions will be documented. For example, there may be control systems whose failure produce transients that are enveloped by the limiting transients assumed in Chapter 15 analyses, and therefore, failure of these systems would be of little relative consequence. There may also be failures whose probability of occurrence in a given sequence or at a particular point in time may be so unlikely as not to warrant further study.

As a result of these activities a set of control systems potentially significant to safety will be identified for further computer study in order to identify important failure sequences and to investigate the dynamic plant behavior as a result of these failures (see Task 2). Applicable information data developed by other ongoing NRC activities conducted by (1) RES through contracts with ORNL and Sandia, (2) Instrumentation and Control Systems Branch (ICSB) case reviews, (3) the RRAB System Interaction Study for Indian Point Unit #3 and (4) the IREP Study for Calvert Cliffs 1, Millstone 1, Arkansas Nuclear One Unit 1 and Browns Ferry Unit 1 will be assessed as part of this task. The data developed from these activities that identifies significant control systems and assesses their reliability will be considered in the evaluation of this task.

Task 2 Conduct Computer Simulation Studies for Evaluating Combination of Systems Failures

Develop an analytical model to simulate the reactor transients, as a result of control system failures or malfunctions, using existing codes whenever possible. The model should include the plant characteristics of the primary reactor fluid and the secondary steam system and the feedwater system as well as the major elements of the control systems. The objective of these simulations will complement the system level FMEA activity (described in Task 1) in identifying and evaluating the sequences and combinations of control system failures important to safety. It is anticipated that the plant dynamic simulator will minimize the need for extensive use of the analytical techniques (described in Task 1) to study the interactive control system failures resulting from simultaneous and/or sequential faults.

As part of the activities conducted at ORNL through NRR/RES (FIN No. B-0467), ORNL will develop a hybrid computer model to simulate the behavior of a PWR type plant. Concurrently, as part of the activities conducted at EG&G Idaho Falls (FIN No. A-6477) EG&G will develop a digital computer model to simulate the dynamic behavior of a BWR type plant with an option to develop a model to simulate a PWR design to study other PWR designs. The models will be oriented toward identification and evaluation of the impact of system interaction and failure dependencies of control systems identified in Task 1. The models will employ the use of different codes. EG&G will utilize existing RELAP 5 codes and ORNL will utilize a hard-wired analog computer for modeling the control systems and a RETRAN code for the plant dynamic model. Extensive use of existing and verifiable codes and models will be utilized. Additional modeling will be developed for the control systems and for the necessary secondary flow loops. We plan to modify the models as necessary to simulate the plant specific characteristics of the four plants under review. Computer simulations of postulated scenarios will be performed to determine if plant operating or safety limits (identified in the

specific Technical Specifications and in NUREG-0800) are exceeded. When plant operating or safety limits are exceeded then the respective event sequences will be identified and considered in Task 5. and/or 6. As a result of this task it is anticipated that the lists of systems identified in Task 1 will be modified. During this phase an assessment will be made as to the possibility of utilizing any other dynamic models in part or in whole, already developed by others to simulate the plant specific characteristics of the plants under review or for verification testing of the models that will be developed. The benefits of using the models developed for the LOFT project, or the use of the Tennessee Valley Authority (TVA) simulators, or the capability to use the NSSS vendor engineering simulators will be evaluated.

Task 3 Identify the Failure Modes of the Safety Significant Systems

Identify the potential failure mechanisms (i.e., root causes) of the control systems that have been identified as a result of the collective activities described in Tasks 1 and/or 2. The information learned as a result of the LER reports, the IE Bulletins and Orders and other applicable documents (such as failure rate data) will be factored into the evaluation to identify credible failure modes and to assess the likelihood of their occurrence. Additional FMEA and fault tree analysis may need to be performed on a sub-system (i.e., component) level on selected systems to identify the mechanistic failure modes that can occur and to assess methods for corrective actions. The need for additional analysis will be evaluated on a case-by-case basis. The relative importance of the control system, its complexity and its dependence on environmental conditions and on other systems will be a factor for implementing any additional analysis. During this phase failure modes due to short/or open circuits, loss of environmental support systems, loss of power supply, abnormal environmental or seismic effects will be considered. Operator action will be addressed to the extent of assessing if credit can be given to the operator in mitigating certain selected transients caused by control system failures. This assessment will

be limited to assuring that the procedures to mitigate these limited transients are adequately written and relatively simple for the operator to correctly accomplish the task in the time allowed, and that sufficient information and time is available to the operator to assess the conditions that exist.

Task 4 Evaluate the Effects of Loss of Power Supply to the Control Systems. (Including electric (ac and dc) pneumatic, and hydraulic power sources.)

Numerous incidents have occurred in nuclear generating plants involving loss of power in the non-safety grade instrumentation and control systems. These incidents resulted in reactor and turbine trip; the opening of the pressurizer power operated relief valves, and code safety valves; discharge of a significant amount of primary coolant into the containment building; and, the loss of display instrumentation in the control room. The transients and the loss of equipment function produced as a result of these incidents significantly impact the operator's ability to proceed to safe shutdown conditions in an orderly manner. The purpose of this task is to evaluate the effects of loss or degradation of the safety-grade or non-safety grade power supplies which provide power to the non-safety grade instrumentation and control system identified in Task 1 and 2. The evaluation will include the effects of the loss of ac and dc electrical power sources and loss of any applicable pneumatic and hydraulic power sources that operate any important valves. The evaluation will be limited to the loss or degradation of a single power supply and multiple power supply failures that result from a single (source) failure or event. The control systems of the four plant designs will be reviewed. The review of this task will be integrated as part of a review effort associated with the other tasks identified in this plan, and will consist of the following:

a. Coordinate activities with the findings of USI-44, "Station Blackout," and NUREG-0666, "A Probabilistic Safety Analysis of

dc Power Supply Requirements for Nuclear Power Plants," April, 1981, and integrate any applicable requirements and information developed as a result of that activity.

b. Consider the licensees' evaluations and responses to IE Bulletin 79-27, "Loss of Non-Class IE Instrumentation and Control Power System Bus During Operation," November 30, 1979. This subtask will complement the review of IE Bulletin 79-27 and evaluate ac and dc bus power supply failures of the relevant power distribution systems (not limited to 120v systems) on important non-safety equipment and systems. If the non-safety grade equipment is powered from a safety bus, the effects of bus degradation on the safety loads connected on that bus will also be evaluated.

c. Identify and document the control systems that have a significant safety impact due to power supply failures (this will be a specific subgroup of the systems identified in Tasks 1 and 2. Evaluate the effects of a loss of power to the display instrumentation of these systems. Using the criteria and guidance proposed in Reg. Guide 1.97, "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environment Conditions During and Following an Accident," determine to what extent the problems found would be resolved by implementing this guide. Verify the adequacy of existing criteria or develop additional criteria (if ncessary) to minimize the consequence of such power failures. Assess the reliability of the non-safety grade electrical bus, by evaluating the existing operating history. The effects of the non-safety grade bus failures during startup, shutdown, normal power operation and during accident and transient modes of operation will be considered in the evaluation.

d. Develop and propose criteria (or guidelines) to improve the reliability of non-safety grade power supplies (if necessary) and propose recommendations to improve the capability of the

systems to cope with the effects of the system failures identified in subtask c. Integrate the applicable requirements and information developed as a result of the IREP studies conducted on Calvert Cliffs 1, Millstone 1, ANO-1 and Browns Ferry 1, and those identified in subtask a. In addition, integrate the applicable information that is developed as a result of the Sandia studies (FIN No. A-1324).

Task 5 Determine the Need for Control or Protection System Improvements

Verify the adequacy of the existing criteria for control systems, defined in (a) the Standard Review Plan Section 7.7 (NUREG-0800) and (b) applicable Branch Technical positions. Review the activities and approaches used by the international community to (1) minimize control system failure and (2) improve control system reliability. Evaluate the need for additional non-safety grade control systems or the need for additional safety grade protection systems. During this phase, assessing the need for improved or additional operator action to recognize and to mitigate specific transients resulting from control system failures will be made. Recommendations concerning improvements to the existing control, protection and power systems, and the need for additional equipment, such as high level alarms, level controls or interlocks to minimize postulated faults will be justified on the basis of cost effectiveness and risk to safety. The adequacy of existing staff positions regarding certain design requirements for control systems such as the sharing of common sensor lines between safety and non-safety systems will be evaluated in light of the knowledge gained through the operating history (i.e., via LER's and Bulletins, etc.). The need for improved or additional surveillance testing to improve the reliability of the non-safety systems will also be evaluated and proposed if warranted.

Task 6 Provide Design Criteria for the Evaluation of Control Systems

Develop and propose (if necessary) additional criteria or guidelines to improve system reliability and minimize control system failures that (1) could lead to transients more severe than predicted in the plant FSAR accident analysis, and (2) could cause transients that would significantly affect the availability of plants (such as blowdowns, spills, etc.)

As a result of this study and at the completion of this task, a report will be issued describing the conduct and conclusions of tasks identified above. Recommendations (if any) for control system or protection system modifications will be provided separately as proposed revisions or additions the to Standard Review Plan, the Regulatory Guides, or the NRC Regulations.

Task 7 Identify Control Systems That Could Lead to Steam Generator Reactor Vessel Overfill and Overcooling Transients

As part of the overall review effort, the initial focus will be to:

- Evaluate Control Systems that could lead to a steam generator or reactor vessel overfill transient. (subtask 1)

- Evaluate control system failures that could lead to reactor overcooling transient. (subtask 2)

- Identify the lessons that have been learned from past control system failures from the LER's, the Bulletins Orders, the applicable applicant responses and from independent utility studies.

The objective of subtask 1 is to identify automatic and manual control systems whose failure have the potential for causing steam generator or reactor vessel overfill. The objective of subtask 2 is to identify those control systems whose failure or malfunction

can contribute to an overcooling transient in the primary system of sufficient magnitude to initiate repressurization via the automatic initiation of the safety injection systems. The criteria that will be used for selecting and categorizing significant control systems for these tasks will be defined. A candidate criteria for identifying significant systems for subtask 1 may be one whose failure or malfunction may lead to water ingress (or significantly increase moisture carryover or steam quality in the main steam line steam space). This water ingress may lead to a loss of existing safety systems (i.e., the loss of auxiliary feed pump turbines) or cause undue stress to the steam lines. The screening criteria for subtask 2 will be developed with assistance from Task A-49. This assistance will be in the form of defining important event sequences and describing unacceptable pressure-temperature conditions that may occur as a result of selected control failures. The approach and methodology outlined in Tasks 1 through 6 will be utilized for resolution of these subtasks.

As part of a separate subtask conducted for Task A-49, RES has contracted ORNL (FIN No. B-0468) to perform a study of PTS, including as one subtask, the control and safety system design for each of the three PWR vendors (the same plants will be studied for this task.) One purpose of the contract is to provide details of the control and safety functions that could contribute to pressurized thermal shock events. We plan to utilize the control system information developed on that subtask and include their findings in our evaluation. At the same time, we expect that the results from A-47 related efforts, including those under Fin No. B-0467 at ORNL and A-1324 at Sandia (see Section 5) to contribute to the resolution of A-49.

Proposed recommendations in the form of guidelines or criteria will be developed (if necessary) for control system modification or for additional protection system functions which would minimize the impact of control system failures or malfunctions that could contribute to significant steam generator or reactor vessel overfill transients and/or pressurized overcooling transients.

As a result of these studies and at the completion of subtasks 1 and 2 a report will be issued describing the technical results and findings. A report will also be issued to summarize the lessons learned from the study of the applicable LERs, Bulletins and Orders and from the other information identified in Task 1. Recommendations for new or modifications to existing requirements (if any) will be provided separately as proposed revisions or additions to the Standard Review Plan or the Regulatory Guides.

3. BASIS FOR CONTINUED OPERATION OR LICENSING PENDING COMPLETION OF PROGRAM

As previously noted, the NRC staff has performed instrumentation and control system reviews on licensed plants and is currently reviewing on a case-by-case basis, the Near Term Operating License (NTOL) plants. The goal of the reviews is to verify that the control system failures (either single or multiple failures) will not prevent automatic or manual initiation and operation of any safety protection system equipment required to trip the plant or maintain the plant in a safe shutdown condition following any "anticipated operational occurrence" or "accident." These reviews are performed utilizing, in whole or in part, the guidelines and criteria identified in Standard Review Plan Section 7.7.

With the recent emphasis on the availability of post-accident instrumentation (Regulatory Guide 1.97), the staff reviews evaluate the designs to assure that control system failures will not deprive the operator of information required to maintain the plant in a safe shutdown condition after any "anticipated operational occurrence or accident." For the NTOL reviews, the applicants are requested to evaluate their control systems and identify any control system whose malfunction could impact plant safety. The licensees are requested to identify the use (if any) of common power supplies, and the use of common sensors or common sensor impulse lines whose failure could have potential safety significance. The results of these reviews and the staff's evaluation for the NTOLs are documented in the Safety Evaluation Reports on a case-by-case basis.

In addition, a specific set of "accidents" has 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 potential consequences to the health and safety of the public are within acceptable limits. In these analyses, conservative assumptions have been used. The conservative analyses performed and the "accidents" chosen for the analyses 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.

Several activities that have been completed or are still ongoing which address the effects of control system failures have been conducted by the NSSS vendors. B&W has completed a failure modes and effects analysis and a 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," August 1979. The staff completed its review of BAW-1564 through a technical assistance contract with ORNL (Memorandum, R. Satterfield to P. S. Check, "Assessment of B&W Report 1564, 'Integrated Control System Reliability Analysis'," May 9, 1980). As a result of this review, both the staff and ORNL concluded that the ICS itself had a relatively low failure rate and did not appear to initiate a significant number of plant upsets. Failure statistics revealed that only approximately 6 of 162 hardware malfunctions resulted in reactor trip. ORNL has further concluded that the B&W analysis shows that anticipated failures of and within the ICS are adequately mitigated by the plant safety systems and many potential failures would be mitigated by crosschecking features of the control system without challenging the plant safety systems. In BAW-1564, B&W recommended six actions regarding control system improvements which could be made to improve overall plant performance. In November 1979, the licensees with B&W plants (except Three Mile Island Unit 1) were requested to evaluate the B&W recommendations and report their followup actions. Subsequently, the responses have been reviewed and found acceptable by ICSB.

Also, the licensees have been requested (IE Information Notice 79-22, "Qualification of Control Systems," September 14 and 17, 1979) to review the possibility of consequential control system failures which exacerbate the effects of high energy line breaks (HELB) and adopt design changes or new operator procedures where needed, to assure that the postulated events would be adequately mitigated. 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 did make changes to their operating procedures to address the possibility of control failures. As part of the staff's ongoing review of the adequacy of the equipment qualification program on NTOLs, and in response to IE Bulletin 79-01, "Environmental Qualification of Class IE Equipment," February 8, 1979, for all operating reactors, the staff is re-evaluating the qualification programs to assure that equipment that may potentially be exposed to HELB environments have been adequately qualified or an adequate basis has been provided for not qualifying the equipment to the limiting hostile environment.

The equipment qualification evaluations are conducted on a case-by-case basis. The staff reviews for all operating plants will be documented in the supplemental Safety Evaluation Reports. For NTOLs, the staff reviews will be completed before operating licenses are granted.

In addition, IE 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 instrumentaton required to mitigate such an event. As part of Operating License (OL) licensing reviews, ICSB is requesting that similar reviews be conducted by the NTOL applicants.

Based on the activities identified above and the ongoing NTOL case review activities, continued licensing and operation of PWRs and BWRs is acceptable pending completion of this program.

4. NRC TECHNICAL ORGANIZATIONS INVOLVED

A. Division of Licensing (DL)

DL will provide the coordination necessary to expedite and collect system design information on four operating reactors. The information needs will be to procure system piping and instrumentation designs and flow and logic diagrams for the non-safety grade control systems. Associated control equipment support system design schematics, such as power supply systems, will also be needed. DL will provide assistance to the Task Manager for setting up and coordinating with the utility personnel, information meetings and site visits that may be necessary. DL will also provide assistance to the Task Manager for integrating any relevant experience and any new requirements resulting from the activities identified in Task A-47. DL will contribute to the review and approval of any licensing requirements and guidelines developed as a result of this USI, and will provide review and comment on the technical evaluations provided by the Task Manager.

Manpower Requirements

	Total	FY83	FY84
Operating Reactors Branch No. 1	0.20 my*	.15	.05
Operating Reactors Branch No. 3	0.20 my	.15	.05
Operating Reactors Branch No. 4	0.20 my	.15	.05
Operating Reactors Branch No. 2	0.20 my	.15	.05
Operating Reactors Assessment Branch	0.30 my	.20	.10

* Assumed 1 man-year = 40 man weeks.

B. Division of Systems Integration (DSI)

DSI will provide review and comment on technical evaluations provided by the Task Manager in the areas of instrumentation and control, electrical power, the reactor and auxiliary plant designs, and accident analysis. The Instrumentation and Control Systems Branch and the Power Systems Branch will provide assistance for the purpose of integrating relevant experience and any new requirements and guidelines stemming from the completion of the subtasks described in Task A-47. The Reactor Systems Branch and the Auxiliary Systems Branch will assist in the development of the selection criteria to be used for establishing safety significant control systems (described in Task 1) and will verify completeness of non-safety grade control systems that may be needed in mitigating the accidents and transients analyzed in Chapter 15 of the plant FSAR. In addition DSI will contribute to the formulation, review and approval of the recommendations, and guidelines developed at the completion of the tasks (described in Task A-47). DSI will also review and comment on the draft and final NUREG Report.

Manpower Requirements

	Total	FY83	FY84
Instrumentation and Control Systems Branch	0.35 my	.30	.05
Power Systems Branch	0.25 my	.20	.05
Reactor Systems Branch	0.50 my	.4	.10
Auxiliary Systems Branch	0.175 my	.125	.05

C. Division of Human Factors Safety (DHFS)

DHFS will provide review and comment on those technical evaluations involving man/machine interfaces. DHFS will contribute to the formulation, review and approval of recommendations and guidelines involving man/machine interfaces developed at the completion of the tasks. In this area DHFS will contribute in the development of maintenance or testing requirements (if warranted) for non-safety control systems.

Manpower Requirements

	Total	FY83	FY84
Human Factors Engineering Branch	.15 my	.15	0
Procedures and Test Review Branch	.15 my	.15	0

D. Division of Safety Technology (DST)

DST will provide overall management of the program to resolve this USI. Provides liaison between NRR and RES and provides coordination of activities performed within NRR which are part of this Task Action Plan. DST has primary responsibility for the review of the draft recommendations and guidelines and for coordination of the internal management and the public review process required to adopt the recommendations and guidelines into licensing requirements. DST will provide review, comment and technical support on those issues/evaluations provided by the Task Manager involving reliability and risk assessments, and cost/benefit assessments related to non-safety control systems.

DST will provide assistance to the Task Manager for the purpose of integrating relevant experience and any new requirements stemming from the completion of those activities related to Task A-47 for which DST has responsibility. Those activities include RRAB system interaction studies, and the Task A-49 and Task A-44 activities referenced in previous sections of this plan.

In addition, RRAB will provide technical support in the area of reliability and risk assessments on non-safety control systems that have been identified as safety significant. The Safety Program Evaluation Branch will provide technical support on the cost/benefit evaluations associated with the recommendations and positions developed on each of the subtasks. DST will also coordinate the revision and publication of the NUREG report and coordinate the issuance of other licensing documents such as Regulatory Guides, Rules, and the Standard Review Plan with the Division of Engineering Technology.

Manpower Requirements

	Total	FY83	FY84
Generic Issues Branch	2.25 my	1.50	.75
Reliability and Risk Assessment Branch	.15 my	.125	.025
Licensing Guidance Branch	.15 my	.10	.05
Safety Program Evaluation Branch	.3 my	.3	.00
Research & Standards Coordination Branch	.15 my	.10	.05

E. Office of Analysis and Evaluation of Operational Data (AEOD)

AEOD will provide review and comment on the technical evaluations provided by the Task Manager. AEOD will provide assistance to the formulation, review and comment of the recommendations and guidelines developed (primarily on subtask 1). AEOD will also provide assistance to the Task Manager for the purpose of integrating relevant experience for which AEOD has responsibility.

Manpower Requirements

	Total	FY83	FY84
Plant Systems Unit	.15 my	.10	.05

5. ASSISTANCE FROM RES DIVISIONS

Close coordination and cooperation will be required on Task A-47 between NRR and RES. RES assistance will be required from the Division of Facility Operations, Instrumentation and Control Branch (ICB). ICB through contracts with ORNL, will develop the generic PWR simulator models (discussed in Tasks 1 through 3) as a specific input for the activities outlined in Task A-47. In addition, RES (FIN No. B-0467) will conduct a review on two or three PWR designs discussed in this Task Action Plan and will perform the activities identified in Tasks 1 through 7 on each of these plants in conformance with the schedule identified in Figure 1. RES will also provide a draft report on each of the plants reviewed. The report will include the content of the information described in Tasks 1 through 7.

Any control systems identified by RES to be generic will be identified in Task A-47. In addition the Division of Risk Analysis will provide technical input from Task A-44, "Station Blackout" relative to loss of power to the vital buses associated with non-safety control systems. Also, any applicable information developed by the Sandia plant electrical systems study (FIN No. A-1324) that would enhance a more complete understanding of significant interactions between the electrical power and the electrical control systems will be factored into the overall evaluation if the information is available and compatible with the schedule for resolution of this task.

Manpower Requirements

	Total	FY83	FY84
Instrumentation and Control Branch	.85 my	.55	0.3
Division of Risk Analysis	.225 my	.15	.075

(The manpower requirements for RES/ORNL activities are summarized in Table 1).

6. TECHNICAL ASSISTANCE

Technical assistance to the program will be required for the activities identified in Tasks 1 through 7. Contracts will be made with the National Laboratories to conduct the studies and activities described in Section 2 of this Plan. Funding will be provided by the Office of Nuclear Reactor Regulation and the Office of Nuclear Regulatory Research. The estimated costs are shown in Table 1. The proposed schedule for Task resolution is shown in Figure 2. Should additional evaluations of other plant designs be needed, a significant cost increase will take place. Such costs are not included in the cost estimates shown in Table 1.

The funding associated with the RES activities related to Task A-47, (specifically FIN No. B-0467 and FIN No. B-0468) are funded directly by the Division of Facility Operations, Office of Nuclear Regulatory Research. These related activities are a part of a large overall research program which is beyond the scope of Task Action Plan A-47.

7. INTERACTIONS WITH OUTSIDE ORGANIZATIONS

Interaction with outside organizations will include the NSSS vendors, utilities, the architect/engineers, the Electric Power Research Institute (EPRI), ORNL, Sandia Laboratories, and EG&G-Idaho.

The activities of Task A-47 will be coordinated with the appropriate ACRS subcommittee. Significant information will be provided to the subcommittee as it becomes available and meetings will be scheduled at appropriate times. Peer review will be conducted through ACRS briefings and by establishing a peer review panel (if necessary) selected from outside NRC having appropriate expertise. In addition, as Task 5 progresses, it will be necessary to establish a strong interaction and information exchange with the international community. Attendance at international conferences and/or site visits to selected foreign utility agencies and consultants is anticipated.

8. POTENTIAL PROBLEMS

A. Traditionally, the licensees were not required to provide design and operating experience on non-safety grade control systems, and therefore complete information on the final "as built design" for these systems (i.e., schematics, flow logic diagrams and system descriptions) and operating experience may be difficult to obtain.

B. Performance of selected tasks described in Tasks 1 through 7 by NRR will require participation from members of DSI, DL, and RES at various intervals throughout the program. Assignments of selected personnel, at specific intervals, will be required. Close coordination and cooperation is needed within NRR (e.g., Task A-49) and between NRR and RES (e.g., ORNL).

C. Development of appropriate reliability/safety goals for specific non-safety grade control systems and translation of these goals into licensing requirements.

D. Uncertainty as to the applicability or compatability of the information that will be available from IREP, systems interaction studies, and other ongoing reliability and risk assessment studies for use on Task A-47. The completion schedules of these activities may not be compatible with Task A-47. Uncertainty as to whether the information obtained from these activities can be used for a generic study.

Table 1 A-47 USI Funding

	FY 1982		FY 1983		FY 1984		Total	
	Manpower	Cost	Manpower	Cost	Manpower	Cost	Manpower	Cost
EG&G Activities Resolution of TAP A-47 Review on BWR Type Design FIN# A6477	1.0 Staff Years	99K	3.3 Staff Years	409K	0.2 Staff Years	42K	4.5 Staff Years	550K
EG&G or ORNL Activities (to be decided) Resolution of Task A-47 on one W PWR design	0.1 Staff Years	11K	4.0 Staff Years	456K	0.4 Staff Years	83K	4.5 Staff Years	550K
RES (ORNL) Activities to include resolution of TAP A-47 on 2 PWR type designs FIN# B0467	4.4 Staff Years	636K	4.2 Staff Years	636K	5.5 Staff Years	1035K	13.1 Staff Years	2207K

Table 2 Related Activity Funding

	FY 82 Cost	FY 83 Cost	FY 84 Cost
RES (Sandia) Activities FIN No. A-1324	$350,000	$400,000	$400,000

Figure 1

Flow Diagram for
Resolution of USI A-47

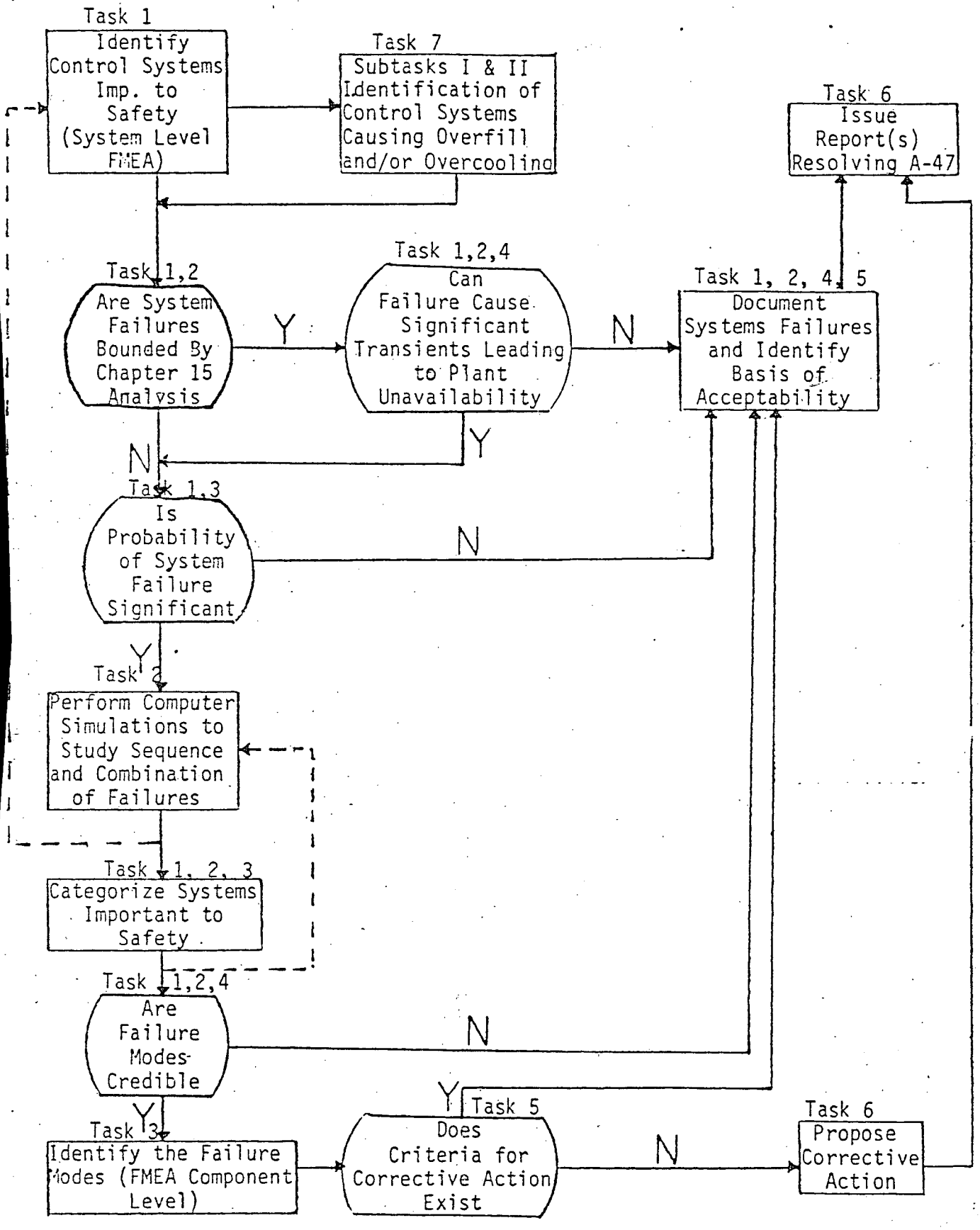
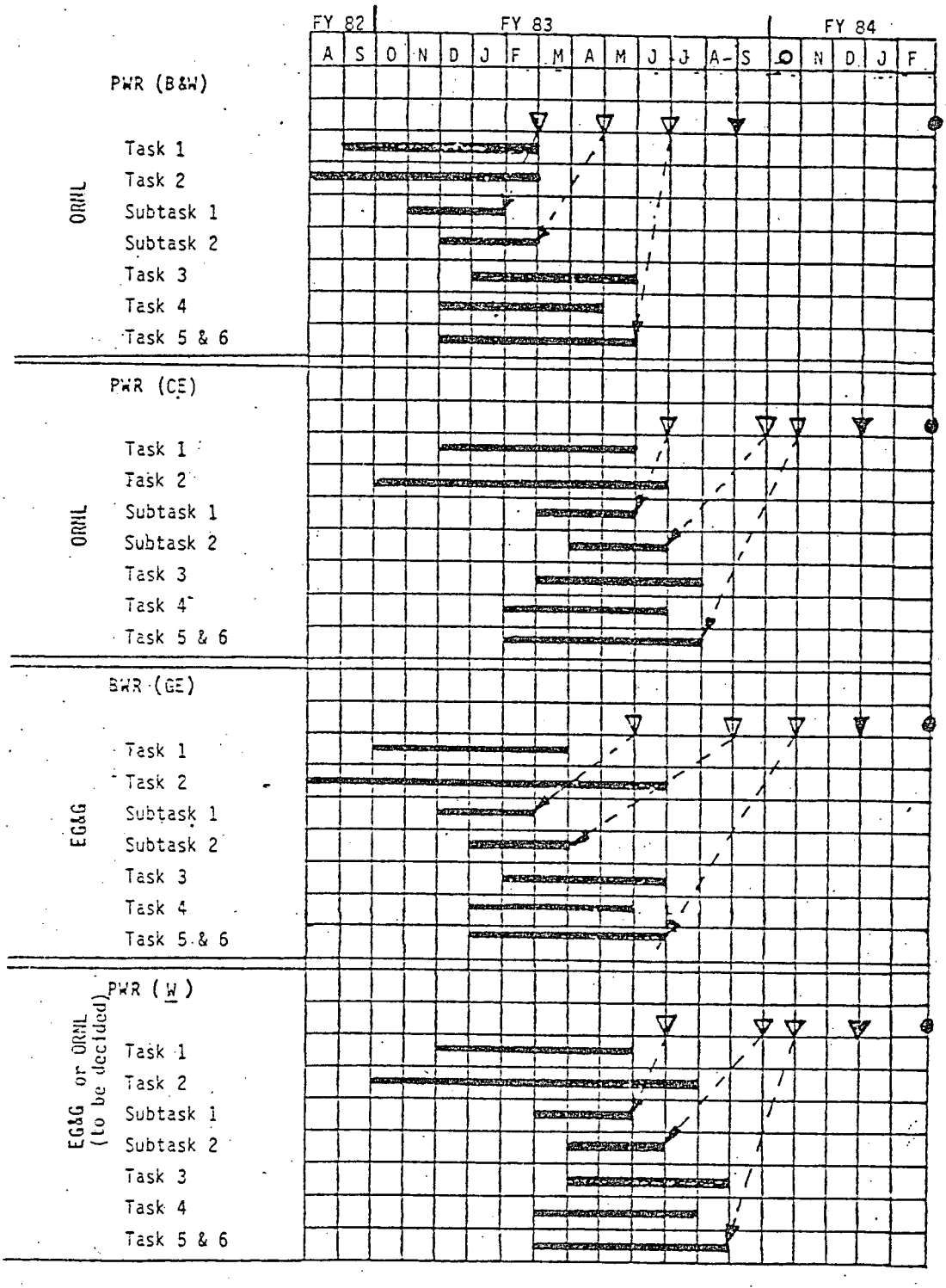


Figure 2

Proposed Schedule for Task A-47

"SAFETY IMPLICATIONS OF CONTROL SYSTEMS"



NOTE:

▽ Draft Report Submitted by Labs
▼ Final Report Submitted by Labs
◉ Draft Report Submitted by NRR