EGG-EA-6473

DECEMBER 1983

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING EVENTS AT A TYPICAL WESTINGHOUSE 3-LOOP PLANT

D. E. Baxter
S. J. Bruske
C. B. Ransom

Idaho National Engineering Laboratory
Operated by the U.S. Department of Energy

This is an informal report intended for use as a prelimina.y or working document

Prepared for the
U. S. NUCLEAR REGULATORY COMMISSION
Under DOE Contract No. DE-AC07-76ID01570
FIN No. A6477

EG&G Idaho

EGG-EA-6473

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING EVENTS AT A TYPICAL WESTINGHOUSE 3-LOOP PLANT

D. E. Baxter
S. J. Bruske
C. B. Ransom

Published December 1983

EG&G Idaho, Inc.
Idaho Falls, ID 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Under DOE Contract No. DE-AC07-76ID01570
FIN No. A6477

ABSTRACT

Recently, concerns dealing with the possibility that certain accidents or transients could be made more severe by control system failures or malfunctions have been raised. These concerns have been documented under Unresolved Safety Issue (USI) A-47, Safety Implications of Control Systems. Specific concerns dealing with steam generator overfill and reactor coolant system overcooling are included in USI A-47.

This EG&G Idaho, Inc., report presents the study performed to evaluate the effects of postulated control system failures on steam generator overfill and reactor coolant system overcooling events at the H. B. Robinson Nuclear Power Plant.

FOREWORD

This report is supplied as part of the "Safety Implications of Control System Failures A-47" study being conducted for the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Division of Safety Technology by EG&G Idaho, Inc., NRC Licensing Support Section, Special Projects Group.

The U.S. Nuclear Regulatory Commission funded the work under the authorization B&R 20-19-50-51-5, FIN No. A6477.

SUMMARY

The purpose of this study is to determine which system or systems if any at commercial Pressurized Water Reactor (PWR) units could initiate, contribute to or aggravate any overfill or overcooling events. These events have been identified as significant concerns for plant safety by the Nuclear Regulatory Commission.

A study of the Nuclear Power Experiences[1] and Licensee Event Reports for the years of 1980 through 1982 for all 3-loop PWR units was performed to identify all events of these types which have occurred. Independent of this study a non-mechanistic Failure Mode and Effects Analysis was performed for each of these events. The results of these two studies produced a list of significant systems of concern. These systems were then processed through a detailed study to determine what mechanism was available to create the failure or operation of concern. These failures were then ranked and a probability of occurrence assigned to each. These rankings were then combined with engineering judgment and postulated worse case transient scenarios were developed.

These postulated transients are considered to be potentially more severe than those presented in the Final Safety Analysis Report.

Conclusive documentation that verifies these assumptions requires completion of computer modeling and analysis of these transients.

CONTENTS

ABSTRACT ii

FOREWORD iii

SUMMARY iv

1. INTRODUCTION 1

2. METHOD OF ANALYSIS 2

3. ASSUMPTIONS 5

4. SYSTEM DESCRIPTION 6

5. CONCLUSIONS 7

6. REFERENCES 9

APPENDIX A--SAFETY IMPLICATIONS OF CONTROL SYSTEMS (A-47) SIGNIFICANT SYSTEMS SELECTION CRITERIA 11

APPENDIX B--OVERFILL/OVERCOOLING FAILURE MODE AND EFFECTS ANALYSIS (FMEA) TABLES 17

APPENDIX C--OVERFILL AND/OR OVERCOOLING POTENTIALLY SIGNIFICANT SYSTEMS LIST AND DISCUSSIONS 45

APPENDIX D--DETAILED REVIEW TABLES FOR STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENTS 59

APPENDIX E--OVERFILL AND OVERCOOLING POSTULATED TRANSIENT SCENARIOS 105

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING EVENTS AT A TYPICAL WESTINGHOUSE 3-LOOP PLANT

1. INTRODUCTION

EG&G Idaho Inc., is technically supporting the Nuclear Regulatory Commission in their efforts to resolve the generic issue A-47, Safety Implications of Control Systems. The concern of the A-47 study is to determine if any accidents or transients can be initiated or made more severe than previously analyzed as a result of control system failures or malfunctions. Specific concerns dealing with steam generator overfill and reactor coolant system overcooling events are included in the A-47 study. This report addresses the steam generator overfill and reactor coolant system overcooling events. A later report will cover other events of concern.

This report addresses the analysis performed to evaluate the effects of control system (non safety grade) failure or malfunction and their potential for causing or contributing to a steam generator overfill or reactor coolant system overcooling event.

2. METHOD OF ANALYSIS

The evaluation of control system failures or malfunctions on steam generator overfill and/or reactor coolant system overcooling events at pressurized water reactors (PWR) was performed in two separate phases. Each of these phases utilized a slightly different methodology.

The first phase of this study was to identify all the control grade systems used for plant control at the pressurized water reactor sites, and then identify those systems which could be postulated to cause or contribute to a steam generator overfill or reactor coolant system overcooling event. A review of the H. B. Robinson Final Safety Analysis Report (FSAR) provided a list of 54 systems, both safety grade and control grade, which are capable of affecting reactor plant performance, safety and control. Safety grade systems were included to ensure that all plant operations and evolutions were completely analyzed. However, failures of safety grade systems, other than single failures were not taken into consideration for this report as it is not the intent of this report to identify multiple safety grade system failures, although there have been documented cases, but rather control grade system failures. The complete list of systems identified and analyzed is contained in Appendix B.

The second phase of this study was to develop a set of criteria which could be used to establish which system failures or operations would have a significant impact on the various events of concern. The listing of the criteria developed for the entire A-47 study is contained in Appendix A. For this report on steam generator overfill and reactor coolant system overcooling only Criteria 1 and 2 of Appendix A are applicable.

In order to determine which systems have a potential for affecting or causing a steam generator overfill or reactor coolant system overcooling event two separate approaches were utilized. These reviews were performed separate of each other to preclude as much commonality as practicable. The first approach entailed a detailed review of the Licensee Event Reports and the Nuclear Power Experiences[1] for a specific group of PWRs for the years 1980 through 1982. The review was focused around any and all events that were or could be classified as steam generator overfill or reactor coolant system overcooling events. This detailed review produced several instances which caused or contributed to a steam generator overfill and/or reactor coolant system overcooling event. In several cases water level was actually raised high enough to cause flooding of the main steam lines and several instances of cooldown rates exceeding 100°F/hr were documented.

The second approach utilized was to perform a Failure Mode and Effects Analysis (FMEA) for each of the events. The FMEA tables are contained in Appendix B. During the course of producing the FMEA all of the systems were subjected to a very broad and liberal interpretation of Criteria 1 and 2 of Appendix A. In utilizing these interpretations, systems which were postulated to be capable of causing or contributing to either of these events were designated as potentially significant systems and placed in a further detailed review status. The listing of those systems designated as potentially significant along with a brief discussion explaining the plant conditions and system failure mode of concern are contained in Appendix C.

Systems which were not selected as being potentially significant for these events were rejected from further review. These systems have been identified in Appendix B along with the reason or reasons for rejections.

The potentially significant systems were then subjected to a detailed review to determine if mechanistic failures could be postulated to cause the system failure of concern. These mechanistic failures were identified and ranked according to the effect of the failure and the relative likelihood of its occurrence. The detailed review tables are contained in Appendix D.

Transient scenarios were then developed utilizing these tables and engineering evaluations. The postulated scenarios are contained in Appendix E and are considered to be more severe than those presented in the H. B. Robinson Final Safety Analysis Report. Included in Appendix E is a listing of additional systems that have the potential to cause or aggravate the transient and may be used in additional transient studies based on the results of the computer simulation and analysis of what appears to be a worse case at this time.

The next phase of this task requires computer modeling and analysis of these worse case transients. These studies could produce additional transient scenarios of concern as previously mentioned. These additional transients will be documented in a future amendment to this report or will be presented in an additional report and, if required, will be computer modeled and analyzed.

3. ASSUMPTIONS

The assumptions utilized in each phase of this study are contained in their respective appendices.

4. SYSTEM DESCRIPTION

The systems which were evaluated in the FMEA tables were extracted from the systems as identified in the H. B. Robinson Final Safety Analysis Report (FSAR). The systems which were evaluated represent the major nonsafety grade control systems which are used for reactor plant control. Many systems have several subsystems or support systems associated with them which were not specifically listed in the FMEA. However, failures of these systems were factored into the analysis by considering a support or subsystem failure to result in a non-mechanistic failure of the major system.

5. CONCLUSIONS

Although defining the actual consequences of a steam generator overfill or reactor coolant system overcooling event is considered beyond the scope of this task, it could be postulated that a steam generator overfill to the point of water entering the main steam lines could cause main turbine damage and the possibility exists of main steam line damage due to the static loading of water. Additionally, main steam isolation valves and safety relief valve(s) could be damaged due to thermal stresses or water loadings. Similarly, overcooling concerns dealing with thermal shock and structural damage have been postulated.

The scenarios postulated in Appendix E identify concerns with control system failures as they relate to steam generator overfill and reactor coolant system overcooling transients. It must be recognized however, that due to the dynamic nature of nuclear power plants and their associated control systems, definitive conclusions concerning the effects of system failures cannot be made without verifying these postulated effects through computer simulation.

Recognizing these limitations, the postulated overfill scenario indicates a potential problem with regard to the steam generator overfill transient resulting from the design and operation of the steam generator feedwater system. No conclusions will be made concerning reactor coolant system overcooling until the scenarios are analyzed.

These postulated scenarios are consistent with the guidance provided in Standard Review Plan Section 7.1, Appendix B, Item 3.

Specifically, the steam generator feedwater system is considered a control system and is not subjected to the requirements established for safety related systems. The scenarios in Appendix E postulate single active failures which can cause or significantly contribute to a steam generator overfill.

Based on the concerns associated with a steam generator overfill event, the steam generator feedwater and control system apparently does not meet the intent of Standard Review Plan Section 7.7, III, 5.

Recommendations at this time include:

1. A thorough evaluation of the consequences of a steam generator overfill transient and defining of the safety significance.

If it is determined that these transients have safety implications, a cost versus benefit study should be performed to evaluate the following possible solutions.

1. Evaluation of the steam generator overfill transients by the licensees and proposed modifications to existing systems to preclude the effects of these transients.

2. Reclassification of the steam generator feedwater system as a "System Important to Safety" as defined in Standard Review Plan Section 7.1 Appendix A and upgrading the system to meet the applicable criteria.

6. REFERENCE

1. Nuclear Power Experiences PWR-2; Nuclear Power Experiences a division of S. M. Stoller Corporation, 1919 14th Street Suite 550, Boulder, Co. 80302-5386, Phone (303)449-7220.

APPENDIX A

SAFETY IMPLICATIONS OF CONTROL SYSTEMS (A-47) SIGNIFICANT SYSTEMS SELECTION CRITERIA

APPENDIX A

SAFETY IMPLICATIONS OF CONTROL SYSTEMS (A-47)
SIGNIFICANT SYSTEMS SELECTION CRITERIA

1. Any control grade system or component failure, either initiating or aggravating, which results in an undesired increase in steam generator water level beyond the bounds of the present FSAR analysis will be recommended for further review. For this study, the point of overfill is defined as that level which, if exceeded, could cause carryover into the main steam system.

   There is no limiting transient identified in the H. B. Robinson FSAR for the steam generator overfill event.

   There is no design basis accident identified in the H. B. Robinson FSAR for the steam generator overfill event.

2. Any control grade system or component failure, either initiating or aggravating, which results in an undesired reactor vessel water temperature decrease beyond the bounds of the present FSAR analysis will be recommended for further review.

   The bounding transient analysis in the H. B. Robinson FSAR for this overcooling event is the "Large steam line break outside of containment with offsite power available."

   The design basis accident for this overcooling event is also the "Large steam line break outside of containment with offsite power available," even though it meets all of the requirements of a bounding transient.

3. Any control grade system or component failure, either initiating or aggravating, which results in an undesired nuclear system pressure

increase, positive reactivity increase or increase in reactor coolant inventory beyond the bounds of the present Final Safety Analysis Report (FSAR) analysis will be recommended for further review.

The limiting transient for a nuclear pressure increase event in the H. B. Robinson FSAR analysis is the "Instantaneous loss of steam load (turbine trip) without automatic steam dump or reactor trip."

The design basis accident for the increase in nuclear system pressure event is the "Loss of reactor coolant flow due to reactor coolant pump shaft seizure (locked rotor).

The limiting transient for a positive reactivity increase is the "Uncontrolled Rod Control Cluster Assembly (RCCA) bank withdrawal from full power with minimum reactivity feedback (80 pcm/s withdrawal rate).

The design basis accident for the increase in positive reactivity event is a "Rod Control Cluster Assembly (RCCA) ejection near the end of life of the core.

The limiting transient for an increase in reactor coolant inventory is an "Inadvertent start of a Safety Injection (SI) pump with the plant in a cold shutdown condition.

There is no design basis accident identified for the increase reactor coolant inventory event.

4. Any control grade system or component failure, either initiating or aggravating, which results in an undesired reactor core coolant flow decrease or reactor vessel inventory decrease beyond the bounds of the present FSAR analysis results will be recommended for further review.

The limiting transient for a decrease in reactor coolant flow is a "Simultaneous loss of power to all reactor coolant pumps at full power."

The design basis accident for the decrease in reactor coolant flow is the "Instantaneous shaft seizure (locked rotor) of the reactor coolant pumps."

The limiting transient for the decrease in reactor coolant inventory is the "Steam Generator Tube Rupture at full power."

The design basis accident for this event is the "Double-Ended Cold Leg Guillotine (DECLG) pipe break."

5. Any control grade system or component failures which are projected to cause transients identified as incidents of moderate frequency (Anticipated Operational Occurrences) to occur at a rate significantly more frequent than once per year, or failures which are projected to cause transients identified as infrequent incidents to occur more than once during the lifetime of a plant, or failures which are projected to cause limiting faults (Design Basis Accidents) will be recommended for further review.

6. Any control grade system or component failures which would adversely affect any assumed or anticipated operator action during the course of a particular event or result in manual or automatic actuation of Engineered Safety Features, including the Reactor Protection System or result in exceeding any Technical Specification safety limit will be recommended for further review.

APPENDIX B

STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENTS FAILURE MODE AND EFFECTS ANALYSIS

APPENDIX B. SECTION I STEAM GENERATOR OVERFILL TRANSIENTS FAILURE MODE AND EFFECTS ANALYSIS

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
1. Reactor Coolant System and Pumps	Provides coolant flow to the reactor vessel for core cooling.	High flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
2. Pressurizer Overpressure Protection System	Provides reactor coolant system overpressure protection.	Inadvertent opening of a power operated or safety relief valve.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator	None
		Failure of a power operated or safety relief valve to open when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
3. High Head Safety Injection System	Provides reactor coolant inventory makeup during a small leak, while system pressure is high.	Inadvertent initiation when not required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Failure to initiate when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
4. Residual Heat Removal System	Provides a long term decay heat removal system and a low head high volume inventory makeup system for a large reactor coolant system break.	High flow or inadvertent initiation when not required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
5. Chemical and Volume Control System	Provides a means of maintaining reactor coolant chemistry and normal reactor coolant inventory makeup.	High makeup flow rate or low letdown flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam gnerator.	None
		Low makeup flow rate or high letdown flow rate.	These failures should not have the potential to cause or contribute to a steam gnerator overfill transient as it has no capability to add inventory to the steam generator.	None
6. Coolant Sampling System	Provides a means of sampling the reactor coolant system for chemical analysis.	High flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
7. Pressurizer Pressure Control System	Provides a means of controlling reactor coolant system pressure and provides pressurizer pressure indication.	Pressure is higher then indicated or is controlling high.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Pressure is lower than indicated or is controlling low.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
8. Accumulator Tank System	Provides coolant inventory makeup to the reactor coolant system in the event of a large coolant system pressure boundary breach.	Inadvertent coolant injection.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Failure to inject when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
9. Reactor Protection System	Provides protection to the reactor coolant system and core to prevent plant parameters from going outside of design conditions.	Inadvertent reactor trips.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Failure to trip the reactor when required.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient but should not because the system is safety grade and although failures of safety grade systems have occurred they are outside the scope of this task.	None
10. Control Rod Drive System	Provides a means of moving the control rods for gross reactivity control.	Uncontrolled rod withdrawal or rod ejection.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	I (App. C Item 1)
		Inadvertent rod insertion or a dropped rod.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the rod insertion would cause a cooling transient rather than heating.	None
11. Pressurizer Level Control System	Provides level indication and control signals for Chemical and Volume Control System (CVCS).	Level is higher than indicated or is controlling high.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Level is lower than indicated or is controlling low.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
12. Engineered Safety Feature Actuation System	Provides engineered safety feature (ESF) actuation of specific systems and components to mitigate the consequences of postulated accidents.	Inadvertent ESF initiation.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	I (App. C Item 2)
		Fails to initiate ESF when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system is safety grade and multiple failures of safety grade systems is beyond the scope of this task.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
13. Incore Instrumentation System	Provides core power distribution and core temperature indication.	Provides higher than actual condition indications.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Provides lower than actual condition indications.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
14. Excore Instrumentation System	Provides reactor power indication and protection trips for power levels from the source range to 120% of full rated power.	Provides higher than actual condition indications.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Provides lower than actual condition indications.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
15. Reactor Containment Structure and Containment Isolation System	Provides reactor core and reactor coolant isolation from the environment.	Fails to maintain the required isolation.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Inadvertent containment isolation when not required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
16. Feedwater and Condensate System	Provides the feedwater to the steam generators and collects and stores the condensate for return to the steam generators as feedwater.	Feedwater/condensate flow fails high.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 3)
		Feedwater/condensate flow fails low.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as lower flow rates would cause lower level.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
17. Reactor Coolant System Leak Detection System	Provides an indication of a reactor coolant system to atmosphere leak within the reactor containment.	Inadvertent leak indication.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Failure to indicate when a leak exists.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator	None
18. Process Computer	Monitors and records plant parameters.	Provides a higher than actual indication.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as it has no capability to add inventory to the steam generator.	None
		Provides a lower than actual indication.	These failures appear the have the potential to cause or contribute to a steam generator overfill transient.	i (App. C Item 4)
19. Steam Generator Water Level Control System	Provides level indication and feedwater control for each steam generator.	High feedwater flow rate.	These failure appear the have the potential to cause or contribute to a steam generator overfill transient.	i (App. C Item 5)
		Low feedwater flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as lower feedflow rates would cause lower levels.	None
20. Steam Line Overpressure Protection System	Provides main steam system overpressure protection.	Inadvertent operation of a power operated or safety relief valve.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	i (App. C Item 6)
		Failure to relieve pressure when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the increased pressure would tend to cause void collapse and level shrink.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
21. Main Steam System	Transfers steam from the steam generators to the turbine or the steam dump.	High steam flow rate or inadvertent main steam isolation valve opening.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 7)
		Low steam flow rate or inadvertent main steam isolation valve closure.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as loss of steam flow would increase pressure and collapse voids thereby causing level shrink.	None
22. Turbine Electro-hydraulic Control System (EHC)	Controls steam flow to the turbine.	Inadvertent opening of a turbine governor valve or failure to trip.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 8)
		Inadvertent closing of a turbine governor valve.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as loss of steam flow would increase pressure and collapse voids thereby causing level shrink.	None
23. Auxiliary Feedwater System	A safety grade system which provides steam generator inventory makeup when the main feedwater system is unavailable.	High feedwater flow rate or inadvertent operation.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 9)
		Low feedwater flow rate or loss of flow.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as lower feedflow rates would cause loss of level.	None
24. Steam Generator	Provides a mechanical barrier to separate the reactor coolant and secondary coolant systems while permitting thermal energy transfer between them and thus generating high quality steam.	Failure to keep the systems separate from each other.	These failures appear the have the potential to cause or contribute to a steam generator overfill transient but steam generator failure was not considered as an initiator or aggravator for this report. It will be covered in a later report.	None
		Failure to allow heat transfer.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as lower heat transfer rates would tend to cause void collapse and level shrink.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
25. Steam Generator Blowdown System	Provides a method of removing unwanted chemicals or contaminants from the steam generator water for chemistry control.	High flow rate or inadvertent flow.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as these would tend to reduce levels.	None
		Low flow rate.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 10)
26. Steam Generator Sampling System	Provides a method of removing liquid from the steam generator for chemical analysis.	High flow rate or inadvertent flow.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as this would lower level.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the sampling rate is insignificant for concern.	None
27. Turbine Generator Support Systems	Provides the required lubrication and cooling for generator operation.	Fails to provide the required lubrication or cooling.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 11)
28. Auxiliary Steam System	Provides low pressure steam for air ejectors, turbine gland seals and other auxiliary systems.	High steam flow or inadvertent flow.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 12)
		Low flow or loss of flow.	These failures should not have the potential to cause or contribute to a steam generator overfill transient.	None
29. Main Condenser and Evacuation Systems	Provides a low pressure collection point for the unused steam from power generation operations.	Failure to maintain a vacuum.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 13)
		Increase vacuum.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient but are insignificant for this study as the increase steam flow cause by the vacuum increase will be minor.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
30. Steam Dump System	Provides a method of removing steam from the steam generators when the turbine generator is unavailable or a load rejection has been initiated.	Inadvertent operation when not required or valves fail open.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient.	1 (App. C Item 14)
		Fails to operate when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the loss of steam flow causes a pressure increase transient which tends to collapse voids and shrink level.	None
31. Service Water System	A safety grade system which provides cooling water to components necessary for plant safety under all conditions.	High flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
32. Component Cooling Water System	A safety grade intermediate heat transfer system that separates the reactor coolant system and the service water system.	High flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
33. Condenser Circulating Water System	Provides a heat sink for the unused steam from power generation operations.	High flow rate.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient but are insignificant for this study as the increased vacuum would be minor and the subsequent steam flow increase would be minor.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
34. Primary and Demineralized Water Makeup System	Provides makeup water for the reactor coolant and secondary coolant system.	High flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
35. Station and Instrument Air Systems NOTE: Failures are evaluated within the individual systems.	Provides air for plant use.	High air header pressure. Low air header pressure.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient however, the system was rejected because normal operation or failure to supply components is covered during the individual component system review.	None
36. Communications Systems	Provides normal and emergency inter and intraplant communications.	Fails to operate when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
37. Fire Protection Systems NOTE: Failures are evaluated within individual systems.	Protects equipment and personnel in the event of a fire.	Inadvertent system operation.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient but are covered in the individual system reviews.	None
		Failure to operate when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
38. Nitrogen Supply System	Provides nitrogen gas for pressurizing the safety injection accumulators and a backup source to the instrument air compressors.	High nitrogen header pressure.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Low nitrogen header pressure.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
39. Diesel Generator and Support Systems NOTE: Failures are evaluated within individual systems.	Provides emergency AC power to selected equipment.	Fails to provide power when required.	Failures of this type have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
40. Heating, Ventilation and Air Conditioning Systems NOTE: Failures are evaluated within individual systems.	Provides the plant with the necessary heating ventilating and air conditioning.	Fails to provide sufficient H&V or air conditioning. Provides excessive H&V or air conditioning.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operations or failure to supply components is covered during the individual component system reviews.	None
41. 125 Volt DC Busses, 125 Volt Battery and Battery Chargers NOTE: Failures are evaluated within the individual systems.	Provides power to the 125 volt DC busses.	Fails to provide power when required.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
42. 120 Volt AC Instrument System NOTE: Failures are evaluated within the individual systems.	Provides 120 volts AC power to the general use instrumentation and control power.	Failure to provide the necessary power to the designated equipment.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
43. Lighting System	Provides normal and emergency lighting throughout the plant.	Fails to provide lighting.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
44. Station Normal Auxiliary Power NOTE: Failures are evaluated within the individual systems.	Provides the power for the unit auxiliaries through various transformers.	Fails to provide the required power.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
45. Station Emergency Auxiliary Power NOTE: Failures are evaluated within the individual systems.	Provides the power to the station auxiliaries in the event normal sources fail.	Fails to provide power when required.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
46. New Fuel Storage	Provides for the dry storage of new fuel until time for its loading.	Fails to store the new fuel safely and effectively.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
47. Spent Fuel Storage	Provides for the storage of spent fuel until time for shipment.	Fails to store the spent fuel safely and effectively.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
48. Spent Fuel Pool Cooling and Cleanup Systems	Provides for cooling and cleanup of the spent fuel pool water.	Fails to maintain water temperature or purity.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
49. Fuel Handling System	Provides for the handling of fuel assemblies during core loading and unloading.	Failure to provide movement when required.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Failure to prevent movement or inadvertent movement.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
50. Radioactive Waste Management Systems	Provides for the collecting treating, and storage of radioactive solids, liquids and gases.	Fails to provide safe storage disposal of radioactive materials.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
51. Radiation Monitoring System	Provides for site wide radiation level monitoring.	Indicates higher than actual levels.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Indicates lower than actual levels.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
52. Annunciator System	Provides alarm indication for out of tolerance parameters.	Inadvertent alarms. Fails to alarm when required.	These failures appear to have the potential to cause or contribute to a steam generator overfill transient, however, the system was rejected from this report as it will be covered under "other" transients.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
53. Backup Control System	Provides the capability of shutting down the reactor from locations outside the control room in the event the control room is evacuated.	Inadvertent reactor shutdowns from remote locations.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
		Inability to shutdown the reactor from remote locations.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None
54. Equipment and Floor Drainage System	Provides for the collecting and storage of potentially radioactive drains for transfer to liquid waste disposal system.	Fails to provide safe storage and transfer of drains.	These failures should not have the potential to cause or contribute to a steam generator overfill transient as the system has no capability to add inventory to the steam generator.	None

APPENDIX B. SECTION II REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENTS FAILURE MODE AND EFFECTS ANALYSIS

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
1. Reactor Coolant System and Pumps	Provides coolant flow to the reactor vessel for core cooling.	High flow rate.	These failures appear the have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 15)
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as low flow causes heatup.	None
2. Pressurizer Overpressure Protection System	Provides reactor coolant system overpressure protection.	Inadvertent opening of a power operated or safety relief valve.	These failures appear the have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 16)
		Failure of a power operated or safety relief valve to open when required.	These failures should not have the potential to cause or contribute to an overcooling transient as high pressure tends to increase heating.	None
3. High Head Safety Injection System	Provides reactor coolant inventory makeup during a small leak, while system pressure is high.	Inadvertent initiation when required.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 17)
		Failure to initiate when required.	These failures should not have the potential to cause or contribute to an overcooling transient as it would not result in a reactor shutdown and cooling.	None
4. Residual Heat Removal System	Provides a long term decay heat removal system and a low head high volume inventory makeup system for a large reactor coolant system pipe break.	High flow or inadvertent initiation when not required.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 18)
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as low flow would cause a heatup.	None
5. Chemical and Volume Control System	Provides a means of maintaining reactor coolant chemistry and normal reactor coolant inventory makeup.	High makeup flow rate or low letdown flow rate.	These failures appear to have the potential to cause or contribute to an overcooling transient but the contribution appears to be insignificant for this study.	None
		Low makeup flow rate or high letdown flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as the lower coolant volume would result in a heatup.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
6. Coolant Sampling System	Provides a means of sampling the reactor coolant system for chemical analysis.	High flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as the flow rates involved are insignificant compared to the volume of the reactor coolant system.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as the flow rates involved are insignificant compared to the volume of the reactor coolant system.	None
7. Pressurizer Pressure Control System	Provides a means of controlling reactor coolant system pressure and provides pressurizer pressure indication.	Pressure is higher than indicated or is controlling high.	These failures should not have the potential to cause or contribute to an overcooling transient as pressures tend to cause insignificant temperature changes.	None
		Pressure is lower than indicated or pressure is is controlling low.	These failures should not have the potential to cause or contribute to an overcooling transient as pressures tend to cause insignificant temperature changes.	None
8. Accumulator Tank System	Provides coolant inventory makeup to the reactor coolant system in the event of a large coolant system pressure boundary breach.	Inadvertent coolant injection.	These failures should not have the potential to cause or contribute to an overcooling transient as it is a low pressure system that cannot inject unless the system is already shutdown and cooling.	None
		Failure to inject when required.	These failures should not have the potential to cause or contribute to an overcooling transient as lack of injection could not create a cooldown event.	None
9. Reactor Protection System	Provides protection to the reactor coolant system and core to prevent plant parameters from going outside of design conditions.	Inadvertent reactor trips.	These failures appear to have the potential to cause or contribute to an overcooling transient even though the system is safety grade and redundant.	2 (App. C Item 19)
		Failure to trip the reactor when required.	These failures should not have the potential to cause or contribute to an overcooling transient as reactor operation would cause heatup.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
10. Control Rod Drive System	Provides a means of moving the control rods for gross reactivity control.	Uncontrolled rod withdrawal or rod rejection.	These failures should not have the potential to cause or contribute to an over-cooling transient as this would result in a power increase and a heatup vice cool-down.	None
		Inadvertent rod insertion or a dropped rod.	These failures appear to have the potential to cause or contribute to an over-cooling transient.	2 (App. C Item 20)
11. Pressurizer Level Control System	Provides level indication and control signals for the chemical and volume control system.	Level is higher than indicated or is controlling high.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant temperature.	None
		Level is lower than indicated or is controlling low.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant temperature.	None
12. Engineered Safety Feature Actuation System NOTE: Failures are evaluated within the individual systems.	Provides engineered safety feature (ESF) actuation of specific systems or components to mitigate the consequences of postulated accident.	Inadvertent ESF initiation.	These failures appear to have the potential to cause or contribute to an over-cooling transient, however, the system was rejected because normal operation or failure to supply components is covered in the individual component system reviews.	None
		Fails to initiate ESF when required.		
13. Incore Instrumentation System	Provides core power distribution and core temperature indications.	Provides higher than actual condition indications.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None
		Provides lower than actual condition indications.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
14. Excore Instrumentation System	Provides reactor power indication and protection trips for power levels from the source range to 120% of full rated power.	Provides higher than actual condition indications.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None
		Provides lower than actual condition indications.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None
15. Reactor Containment Structure and Containment Isolation System	Provides reactor core and reactor coolant isolation from the environment.	Fails to maintain the required isolation.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None
		Inadvertent containment isolation when not required.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant system temperature.	None
16. Feedwater and Condensate System	Provides the feedwater to the steam generators and collects and stores the condensate water for return to the steam generators as feedwater.	Feedwater/condensate flow fails high or condensate/feedwater heating fails low.	These failures appear to have the potential to cause or contribute to an over-cooling transient.	2 (App C Item 21)
		Feedwater/condensate flow fails low.	These failures should not have the potential to cause or contribute to an over-cooling transient as low flows tend to cause heatup events.	None
17. Reactor Coolant System Leak Detection System	Provides an indication of a reactor coolant to atmosphere leak within the reactor containment.	Inadvertent leak indication.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant temperature.	None
		Failure to indicate when a leak exists.	These failures should not have the potential to cause or contribute to an over-cooling transient as it has no capability to control or affect reactor coolant temperature.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
18. Process Computer	Monitors and records plant parameters.	Provides a lower than actual indication.	These failures should not have the potential to cause or contribute to an overcooling transient as it has no capability to control or affect reactor coolant temperature.	None
		Provides a higher than actual indication.	These failures appear to have the potential to cause or contribute to an overcooling transient but will be covered during the "other" event report.	None
19. Steam Generator Water Level Control	Provides level indication, and feedwater control for each steam generator.	High feedwater flow rate.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App C Item 22)
		Low feedwater flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as low flow rates would cause a heatup.	None
20. Steamline Overpressure Protection System	Provides main steam system overpressure protection.	Inadvertent operation of a power operated or safety relief valve.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 23)
		Failure to relieve pressure when required.	These failures should not have the potential to cause or contribute to an overcooling transient as the lesser flow rates should not cause an overcooling event.	None
21. Main Steam System	Transfers steam from the steam generators to the turbine or the steam dump.	High steam flow or inadvertent main steam isolation valve opening.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App C Item 24)
		Low steam flow or inadvertent main steam isolation valve closure.	These failures should not have the potential to cause or contribute to an overcooling transient as the low steam flow would result in a heatup.	None
22. Turbine Electrohydraulic Control System (EHC)	Controls steam flow to the turbine.	Inadvertent opening of a turbine governor valve or failure to trip.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 25)
		Inadvertent closing of a turbine governor valve.	These failures should not have the potential to cause or contribute to an overcooling transient as it would cause a steam flow reduction and subsequent heatup.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
23. Auxiliary Feedwater System	A safety grade system which provides steam generator inventory makeup when the main feedwater system is unavailable.	High feedwater flow rate or inadvertent operation.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 26)
		Low feedwater flow rate or loss of flow.	These failures should not have the potential to cause or contribute to an overcooling transient as the low feedflow would cause a heatup.	None
24. Steam Generator	Provides a mechanical barrier to seperate the reactor coolant and secondary coolant systems while permitting thermal energy transfer between them and thus producing high quality steam.	Failure to keep the systems separate from each other.	These failures should not have the potential to cause or contribute to an overcooling transient as it would require a tube repture and that event it being reported or in another report.	None
		Failure to allow heat transfer.	These failures should not have the potential to cause or contribute to an overcooling transient, as loss of heat transfer would result in a heatup.	None
25. Steam Generator Blowdown System	Provides a method of removing unwanted chemicals or contaminants from the steam generator water for chemistry control.	High flow rate or inadvertent flow.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 27)
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient, as the low flow would cause heatup events.	None
26. Steam Generator Sampling System	Provides a method of removing liquid from the steam generator for chemical analysis.	High flow rate or inadvertent flow.	These failures appear to have the potential to cause or contribute to an overcooling transient, but are insignificant, due to volume comparisons, for this study.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as low flow causes heatup events.	None
27. Turbine Generator Support Systems	Provides the required lubrication and cooling for generator operation.	Fails to provide the required lubrication and cooling.	These failures should not have the potential to cause or contribute to an overcooling transient as loss of the turbine would cause reactor heatup.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
28. Auxiliary Steam System	Provides low pressure steam for air ejectors, turbine gland seals and other auxiliary systems.	High steam flow or inadvertent flow.	These failures appear to have the potentail to cause or contribute to an overcooling transient.	2 (App. C Item 28)
		Low flow or loss of flow.	These failures should not have the potential to cause or contribute to an overcooling transient as low flow tends to cause heatup.	None
29. Main Condenser and Evacuation Systems	Provides a low pressure collection point for the unused steam from power generation operations.	Failure to maintain a vacuum.	These failures should not have the potential to cause or contribute to an overcooling transient as they would result in decrease steam flow which results in a heatup.	None
		Increase vacuum.	These failures appear to have the potential to cause or contribute to an overcooling transient, but are insignificant as the vacuum increase would result in minor steam flow increase.	None
30. Steam Dump System	Provides a method of removing steam from the steam generators when the turbine generator is unavailable or a load rejection has been initiated.	Inadvertent operation when not required or valves fail open.	These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (App. C Item 29)
		Fails to operate when required.	These failures should not have the potential to cause or contribute to an overcooling transient as low or loss of flow tends to cause heatups.	None
31. Service Water System	A safety grade system which provides cooling water to components necessary for plant safety under all conditions.	High flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as the system has no capability to affect reactor coolant temperature.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as the system has no capability to affect reactor coolant temperature.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
32. Component Cooling Water System	A safety grade, intermediate heat transfer system that separates the reactor coolant system and the service water system.	High flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient, as the system normally operates at rated flow and there is another system between this system and the reactor coolant system.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as low flows cause heatups.	None
33. Condenser Circulating Water System	Provides a heat sink for the unused steam from power generation operations.	High flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as increase flow would result in only minor vacuum and steam flow increases.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as this would result in steam flow decreases.	None
34. Primary and Demineralized Water Makeup System	Provides makeup water for the reactor coolant and secondary coolant systems.	High flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no capability to affect reactor coolant temperature.	None
		Low flow rate.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-49 Selection Criteria (Appendix C Item X)
35. Station and Instrument Air Systems NOTE: Failures are evaluated within individual systems.	Provides air for plant use.	High air header pressure. Low air header pressure.	These failures may have the potential to cause or contribute to an overcooling transient, however the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
36. Communications Systems	Provides normal and emergency inter- and intra-plant communications.	Fails to operate when required.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
37. Fire Protection System NOTE: Failures are evaluated within individual systems.	Protects equipment and personnel in the event of a fire.	Inadvertent system operation or failure to operate.	These failures appear to have the potential to cause or contribute to an overcooling transient, however the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
38. Nitrogen Supply System	Provides nitrogen gas for pressurizing the safety injection accumulators and is a backup source to the instrument air compressors.	High nitrogen header pressure.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
		Low nitrogen header pressure.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
39. Diesel Generator and Support Systems NOTE: Failures are evaluated within individual systems	Provides emergency ac power to selected equipment.	Fails to provide power when required.	These failures should not have the potential to cause or contribute to an overcooling transient, however the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-4/ Selection Criteria (Appendix C Item X)
40. Heating, Ventilation and Air Conditioning Systems NOTE: Failures are evaluated within individual systems.	Provides the plant with the necessary heating ventilating and air conditioning.	Fails to provide sufficient H&V or air conditioning. Provides excessive H&V air conditioning.	These failures appear to have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
41. 125 Volt DC Busses; 125 Volt Battery and Battery Chargers NOTE: Failures are evaluated within individual systems.	Provides power to the 125 volt DC busses.	Fails to provide power when required.	These failures appear to have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
42. 120 Volt AC Instrument System NOTE: Failures are evaluated within individual systems.	Provides 120 volt ac power to the general use instrumentation and control power.	Failure to provide the necessary power to the designated equipment.	These failures appear to have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
43. Lighting System	Provides normal and emergency lighting throughout the plant.	Fails to provide lighting.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
44. Station Normal Auxiliary Power NOTE: Failures are evaluated within individual systems.	Provides the power for the unit auxiliaries through various transformers.	Fails to provide the required power.	These failures should not have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
45. Station Emergency Auxiliary Power NOTE: Failures are evaluated within individual systems.	Provides safety grade power to the station auxiliaries in the event normal sources fail.	Fails to provide power when required.	These failures should not have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
46. New Fuel Storage	Provides for the dry storage of new fuel until time for its loading.	Fails to store the new fuel safely and effectively.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant system temperature.	None
47. Spent Fuel Storage	Provides for the storage of spent fuel until time for shipment.	Fails to store the spent fuel safely and effectively.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
48. Spent Fuel Pool Cooling and Cleanup Systems	Provides for cooling and cleanup of the spent fuel pool water.	Fails to maintain water temperature or purity.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
49. Fuel Handling System	Provides for the handling of fuel assemblies during core loading and unloading.	Failure to provide movement when required.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
		Failure to prevent movement or inadvertent movement.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
50. Radioactive Waste Management Systems	Provides for the collecting, treating, and storage of radioactive solids, liquids, and gases.	Fails to provide safe storage or disposal of radioactive materials.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
51. Radiation Monitoring System	Provides for site wide radiation level monitoring.	Indicates higher than actual levels.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
		Indicates lower than actual levels.	These failures should not have the potential to cause or contribute to an overcooling transient as this system has no direct capability to affect reactor coolant temperature.	None
52. Annunciator System	Provides alarm indication for out of tolerance parameters.	Inadvertent alarms.	These failures appear to have the potential to cause or contribute to an overcooling transient but will not be address during this phase of this task as it affects operator action which will be evaluated during the "other" events report.	None
		Fails to alarm when required.	These failures appear to have the potential to cause or contribute to an overcooling transient but will not be address during this phase of this task as it affects operator action which will be evaluated during the "other" events report.	None
53. Backup Control System NOTE: Failures are evaluated within individual system reviews.	Provides the capability of shutting down the reactor from locations outside the control room in the event the control room is evacuated.	Inadvertent reactor shutdowns from remote locations.	These failures appear to have the potential to cause or contribute to an overcooling transient, however, the system was rejected because normal operation or failure to supply components is covered during the individual component system reviews.	None
		Inability to shut down the reactor from remote locations.	These failures should not have the potential to cause or contribute to an overcooling transient as failure to shutdown would result in a heatup situation.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria (Appendix C Item X)
54. Equipment and Floor Drainage System	Provides for the collecting and storage of potentially radioactive drains for transfer to the liquid waste disposal system.	Fails to provide safe storage and transfer of drains.	These failures should not have the potential to cause or contribute to an over-cooling transient as this system has no direct capability to affect reactor coolant system temperature.	None

APPENDIX C

STEAM GENERATOR OVERFILL AND/OR REACTOR COOLANT SYSTEM OVERCOOLING POTENTIALLY SIGNIFICANT SYSTEMS LIST AND DISCUSSIONS

APPENDIX C

STEAM GENERATOR OVERFILL TRANSIENT SCENARIOS

1. Control Rod Drive System

    Failure Mode: Inadvertent rod withdrawal or rod ejection.

    Plant Conditions: High steam generator level; any power level.

    Discussion: If the steam generator water level is high and an inadvertent rod withdrawal or rod rejection occurs, the rapid heat input to the steam generator could cause the water level to swell enough to cause an overfill situation.

2. Engineered Safety Feature Actuation System:

    Failure Mode: Inadvertent actuations.

    Plant Conditions: Any steam generator level; any power level.

    Discussion: Inadvertent actuations could contribute or cause a steam generator overfill transient and are being evaluated within the individual systems.

3. Feedwater and Condensate System

    Failure Mode: Feedwater/condensate flow fails high.

    Plant Conditions: High steam generator level; any power level.

Discussion: If the feedwater or condensate systems fail in a higher than normal flow mode, the potential exists to cause or contribute to a steam generator overfill transient.

4. Process Computer:

Failure Mode: Gives a lower than actual indication.

Plant Conditions: High steam generator level; any power level.

Discussion: If the operator is using the computer output as an indication for maintaining steam generator level and steam generator level is higher than indicated, it appears to be possible to overfill the steam generator by trying to compensate for the erroneous indication.

5. Steam Generator Water Level Control System:

Failure Mode: Higher than required feedwater flow rate

Plant conditions: High steam generator level; any power level

Discussion: If the feedwater control valve fails open or fails to control properly, from either a control signal failure or a control valve failure, a steam generator overfill could result.

6. Steam Line Overpressure Protection System:

Failure Mode: Inadvertent operation of a power operated or safety relief valve.

Plant Conditions: High steam generator level; any power level.

Discussion: If the steam generator level is high and one or more power operated or safety relief valves open, the resultant pressure drop would cause an increase in void formation and a rise in steam generator level. The swell in steam generator level could be severe enough to cause an overfill condition.

7. Main Steam System:

Failure Mode: High steam flow rate or inadvertent main steam isolation valve opening.

Plant Conditions: High steam generator level; any power level.

Discussion: If the steam generator level is high and there is a sharp increase in steam flow, the resultant pressure drop would cause an increase in void formation and a rise in steam generator level. The level swell could be severe enough to cause an overfill condition.

8. Turbine Electrohydraulic Control System (EHC):

Failure Mode: Inadvertent opening of the turbine governor valve(s), improper control or failure to trip when required.

Plant Conditions: High steam generator level; any power level.

Discussion: While at a given power level and a high steam generator level, if the turbine governor valve(s) fail(s) open or fails to respond to control signal(s) or fails to trip the resultant pressure drop could cause an increase in steam generator level severe enough to cause an overfill condition if the steam generator level was high at the onset.

9. Auxiliary Feedwater System:

Failure Mode: High feedwater flow rate or inadvertent operation.

Plant Conditions: High steam generator level; any power level.

Discussion: Inadvertent operation of the auxiliary feedwater system could cause or contribute to a steam generator overfill transient.

10. Steam Generator Blowdown System:

Failure Mode(s): Low blowdown flow rate.

Plant Conditions: High steam generator level; any power level.

Discussion: If the steam generator level is high and the feedwater control system is in manual, it may be possible to cause or contribute to a steam generator overfill transient if the blowdown rate decreases below the feed and bleed rate.

11. Turbine Generator Support Systems:

Failure Mode: Turbine trip from loss of lubrication or cooling.

Plant Conditions: High steam generator level; high power level.

Discussion: With a high steam generator level and high power level, if the turbine trips while the feedwater control system is in MANUAL it may be possible to overfill the steam generator.

12. Auxiliary Steam System:

Failure Mode: High steam flow rate.

Plant Conditions: High steam generator level; any power level.

Discussion: A sudden flow rate increase, caused by a failure in the auxiliary steam header pressure regulator, would cause a decrease in steam to the turbine thereby tending to cause a drop in generator load. To counteract this tendency the EHC system would open the turbine governor valves, the main steam header pressure would decrease and thereby cause swell in the steam generator level and an overfill condition could result.

13. Main Condenser and Evacuation Systems:

Failure Mode: Failure to maintain a vacuum.

Plant Conditions: Any steam generator level; high power level.

Discussion: If the condenser vacuum drops the turbine trips and if the feedwater control system is in MANUAL it could be possible to overfill the steam generator.

14. Steam Dump System:

Failure Mode: Inadvertent steam dump valve operation or steam dump valve(s) fail(s) open.

Plant Conditions: High steam generator level; any power level.

Discussion: If the steam dump valve(s) fail(s) open, the resultant pressure drop would cause increased void formation and a swell in the steam generator level. With the steam generator at a high level, an overfill condition could result.

REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENT SCENARIOS

15. Reactor Coolant System and Pumps:

    Failure Mode: High flow rate

    Plant Conditions: Any power level

    Discussion: Inadvertent startup of an idle reactor coolant pump could cause excessive heat transfer from the reactor coolant, which could lead to an overcooling transient.

16. Pressurizer Overpressure Protection System:

    Failure Mode: Inadvertent opening of a relief or safety valve

    Plant Conditions: Any power level

    Discussion: Inadvertent opening of pressurizer power operated relief or safety valve could result in an overcooling transient as the discharged fluid is replaced by relatively cold makeup fluid.

17. Safety Injection System:

    Failure Mode: Inadvertent initiation

    Plant Conditions: Any power level

Discussion: Inadvertent initiation of the safety injection system would cause a decrease in reactor coolant temperature from the cooler injection water and could result in an overcooling transient.

18. Residual Heat Removal System:

Failure Mode: High flow or inadvertent initiation

Plant Conditions: Shutdown

Discussion: Inadvertent initiation or high flow rate could cause the reactor coolant temperature to be lowered at a rate in excess of the allowable rate. This overcooling transient could be in excess of the previously analyzed transient.

19. Reactor Protection System:

Failure Mode: Inadvertent reactor trip

Plant Conditions: Any power level

Discussion: Inadvertent trips could contribute to a cooldown event in excess of allowable cooldown rates.

20. Reactor Control Rod Drive System:

Failure Mode: Inadvertent insertion or rod drop

Plant Condition: Any power level

Discussion: Inadvertent insertion of the control rods or several dropped rods would cause a reactor trip and core power to decrease. This will cause the temperature of the primary coolant to decrease and result in an overcooling transient.

21. Feedwater and Condensate System:

Failure Mode: Feedwater/condensate flow fails high or feedwater/condensate heating fails low

Plant Conditions: Any power level

Discussion: Failures that could cause the feed or condensate system flow to increase above normal would cause excessive cool water to be placed in the system generators, which could cause an overcooling transient on the reactor coolant system.

Loss of feedwater/condensat steam heating could result in introduction of cooler feedwater to the steam generator and may result in an overcooling transient.

22. Steam Generator Water Level Control System:

Failure Mode: Higher than required feedwater flow rate

Plant Conditions: Any power level

Discussion: If the feedwater control valve fails open or fails to properly respond either from control signal failure or a control valve failure, an increased feedwater flow and an overcooling transient to the reactor coolant system could result.

23. Steam Line Overpressure Protection System:

Failure Mode:	Inadvertent operation of a power operated or safety relief valve
Plant Conditions:	Any power level
Discussion:	An inadvertent opening of a relief or safety valve would cause increased steam flow. This in turn would cause a cooling of the steam generator water; a reactor coolant overcooling transient could be initiated.

24. Main Steam System:

Failure Mode:	High steam flow rate or inadvertent main steam isolation valve opening
Plant Conditions:	Any power level
Discussion:	Increased steam flow will cause reactor coolant system temperature to decrease and may cause an overcooling transient.

25. Turbine Electrohydraulic Control system (EHC):

Failure Mode:	Inadvertent opening of the turbine governor valve(s), failure to properly respond or failure to trip when required
Plant Conditions:	Any power level
Discussion:	Failure of the EHC to trip the turbine when required or to increase the turbine governor valve opening or for the govenor valves to fail to

respond could cause an overcooling transient to the reactor coolant system.

26. Auxiliary Feedwater System:

Failure Mode: High feedwater flow rate or inadvertent operation

Plant Conditions: Any power level

Discussion: Inadvertent initiation of auxiliary feedwater would cause a cooling of the steam generator water which could cause an overcooling transient on the reactor system.

27. Steam Generator Blowdown System:

Failure Mode: High blowdown flow rate

Plant Conditions. Any power level

Discussion: An excessive blowdown flow would cause an increased feedwater flow which would cool the steam generator water and thus the reactor coolant faster than the core is adding heat. This could cause or contribute to an overcooling transient.

28. Auxiliary Steam System:

Failure Mode: High steam flow rate.

Plant Conditions: Any power level.

Discussion: An increased steam flow through the auxiliary steam system could cause an overcooling transient to the reactor coolant system.

29. Steam Dump System:

Failure Mode:	Inadvertent steam dump operation or steam dump valve(s) fail(s) open
Plant Conditions:	Any power level
Discussion:	Inadvertent operation of the steam dump system could create an overcooling transient to the reactor coolant system.

APPENDIX D

DETAILED REVIEW TABLES FOR STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSEM OVERCOOLING TRANSIENTS

APPENDIX D

DETAILED REVIEW TABLES FOR STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENTS

1. INTRODUCTION

This report section addresses the mechanistic analysis of the transients identified in the Failure Mode and Effects Analysis (FMEA) for steam generator overfill and reactor coolant system overcooling transients from Appendix B. It determines the mechanistic means by which failures of the identified systems occur. Control logic, instrumentation, electrical power and pneumatic and hydraulic interfaces for each system identified by the FMEA as requiring further review have been analyzed.

The results of these analysis were tabulated and assigned system impact and probability of occurrence values based on the criteria for ranking control system failures. Fault effect designations are A, B or C depending on whether the failure results in adverse effects in two or more systems of concern, one system of concern, or a negligible effect on any of the systems of concern respectively. The values assigned to the failure probability category (ie) 1, 2, or 3 were assigned dependent upon the failure rate probabilities identified in Table D-1 of Appendix D.

The following presents the calculations performed to support the probability category assignment on the IE&C Analysis Tables. The concept analyzed was, given some transient has already occurred, then what is the probability that an additional fault would occur to potentially make the transient more severe. This concept requires the calculation of the unavailability and the following equations were used to calculate the basic event unavailability as appropriate.

Nonrepairable Events

$$\bar{a} = 1 - e^{-\lambda t}$$

$$\lesssim \lambda t \text{ (for } \lambda t \leq 0.1)$$

Repairable Events

$$\bar{a} = \frac{\lambda\tau}{1 + \lambda\tau} [1 - e^{-(\lambda + 1/\tau)t}]$$

$$\leq \frac{\lambda\tau}{1 + \lambda\tau} \text{ (for } t \geq 2\tau)$$

$$\lesssim \lambda\tau \text{ (for } \lambda\tau \leq 0.1 \text{ and } t \geq 2\,\tau)$$

The symbols are as follows: $\bar{a}$ is unavailability, $\bar{A}$ is the total cutsets or combinations of unavailabilities, λ is the failure rate, t is the mission time (usually taken as the time to mitigate the transient), and τ is the fault duration. The fault duration is defined as one-half the time to detect the fault plus the repair time.

A component may be in operation or in standby. For example, a single valve (no bypass around the valve) mav be normally open in an operational system. If this valve should remain open given a transient has already occurred, then the component is nonrepairable over the transient mission time and the unavailability is given by the equation for nonrepairable events. Associated with this valve may be some control logic. For the valve to close, two contacts must open. The logic is tested once per month per the Technical Specification at which time a faulty contact would be discovered. One contact could open but the valve will not close until the second contact opens and since the contacts are redundant, the failed contact can be repaired once it has been detected. The contact unavailability is then given by the equation for a repairable event.

The repairable unavailability equation is also used for a standby system to determine the probability of failure at demand. Once a standby system is demanded and becomes operational, the nonrepairable unavailability equation is generally used (except where there is redundancy) to determine the probability of failure to operate over the mission time.

The probability categories assigned were 1 for failures considered "likely" with a calculated unavailability between 1 and 1×10^{-6} failures considered "unlikely" with a calculated unavailability between 10^{-6} and 10^{-8} were assigned a 2, and failures which are considered "extremely unlikely" with a calculated unavailability of less than 1×10^{-8} were assigned a 3. A transient category of 1 is a steam generator overfill transient and 2 is a reactor coolant system overcooling transient.

2. ASSUMPTIONS

The following assumptions were utilized in performing the mechanistic failure mode analysis:

1. Current drawings, Final Safety Analysis Report (FSAR), Technical Specifications, and other pertinent H. B. Robinson documents were used to the extent of their availability. Where these documents were not available, best engineering assumptions based on experience, knowledge of other PWR plants and engineering judgments were used as a generic substitute in making the evaluation.

2. Only the systems identified in the general postulated scenarios developed from the FMEA and the mode of failure for each system as described in those scenarios were evaluated for mechanistic failure modes.

3. There would be no corrective action taken by the operator during the first ten minutes following the postulated failure.

4. The potential for human error as an initiating event was not considered in these analyses.

5. Unacceptable transient frequency, adverse effects on operator actions, challenges to the ESF, and Technical Specifications safety limit violations will be evaluated against LERs, NPEs,[1] NTOLs and other studies, on those systems, identified by the computer transient analyses to be significant, and which were not included in this mechanistic analysis.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS

SYSTEM Control Rod Drive System

FAILURE MODE Inadvertent rod withdrawal

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
One or more rod cluster control assemblies are inadvertently withdrawn from the core due to one of the following system failures:						
a. A failure of one or more of the control rod actuators which results in a withdrawal signal to the drive mechanisms	1×10^{-6}/hr (short or open in a relay coil)	None	None	B	2	1
b. Failure in a manual rod control switch which results in a withdrawal signal to the control rod actuators.	1×10^{-8}/hr/switch (short across switch contacts)	None	None	B	3	1
c. Failure in the sequential rod control unit and/or the associated permissive circuits which results in a withdrawal signal to the control rod actuators.	1×10^{-6} (short or open in relay coil)	None	None	B	2	1
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following the computer model simulations.	TBD[c]	TBD	TBD	1,2

* There are other input circuits feeding the sequential rod control unit whose failure could result in an erroneous demand for rod withdrawal. However, due to the circuit design and the protective interlocks, multiple failures have to occur to result in any inadvertent rod withdrawal.

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Feedwater and Condensate System

FAILURE MODE Feedwater and/or consensate high flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
1. The feedwater regulating valve is open further than called for by the Steam Generator Water Level Control System because of:						
a. Failure of the valve operating mechanism.	1×10^{-3}/d (failure to operate)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
b. Valve mechanical failure causes it to stick open.	1×10^{-3}/d (failure to operate)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
c. Control air pressure to the feedwater regulating valve fails high.	1×10^{-5}/hr/switch (premature open)	All systems utilizing control air from the same regulator would experience high pressure. This will be further addressed when common mode failures are evaluated.	Reactor coolant system temperature will decrease and pressure will decrease.	A	1	1,2
d. Failure of the solenoid operated vent or control valve so that the control air is not vented from the regulating valve actuator.	1×10^{-3}/d	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
e. Blockage of the vent path used to vent control air from the regulating valve actuator.	3×10^{-4}/d (failure to remain open-plugged)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Feedwater and Condensate System

FAILURE MODE Feedwater and/or consensate high flowrate (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
2. The main feedwater regulating valve Bypass valve is open further than necessary while controlling feedwater flow because of:						
a. Failure of the valve operating mechanism.	1×10^{-3}/d (failure to operate)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
b. Valve mechanical failure causes it to stick open.	1×10^{-3}/d (failure to operate)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
c. Control air pressure to the feedwater regulating valve fails high.	1×10^{-5}/hr/switch (premature open)	All Systems utilizing control air from the same regulator would experience high pressure. This will be further addressed when common mode failures are evaluated.	Reactor coolant system temperature will decrease and pressure will decrease.	A	1	1,2
d. Failure of the solenoid operated vent or control valve so that the control air is not vented from the regulating valve actuator.	1×10^{-3}/d	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2
e. Blockage of the vent path used to vent control air from the regulating valve actuator.	3×10^{-4}/d (failure to remain open-plugged)	None	Reactor coolant system temperature will decrease and pressure will decrease.	B	1	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Feedwater and Condensate System

FAILURE MODE Feedwater and/or consensate high flowrate (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
3. A main feedwater pump starts or fails to shut off during a plant shutdown due to:						
a. Breaker failure.	2 x 10^{-7}/hr/motor (motor starter all modes)	None	None	B	2	1,2
b. Control switch failure.	1 x 10^{-8}/hr/switch (short across contacts)	None	None	B	3	1,2
c. Control interlock failure.	3 x 10^{-5}/hr (instrumentation shift in calibration)	None	None	B	1	1,2
A condensate pump starts or fails to shut off during a plant shutdown due to:						
a. Breaker failure.	2 x 10^{-7}/hr/motor (motor starter, all modes)	None	None	B	2	1,2
b. Control switch failure.	1 x 10^{-8}/hr/switch (short across contacts)	None	None	B	3	1,2
c. Control interlock failure.	3 x 10^{-5}/hr (instrumentation shift in calibration)	None	None	B	1	1,2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following the computer model simulations	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Generator Water Level Control System

FAILURE MODE High Feedwater Flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The Steam Generator Water Level Control System erroneously sends an open signal to the feedwater regulating valve because of:						
a. Failure of a steam flow instrument channel producing a false high steam flow signal to the controller.	2×10^{-6}/hr (taken 3 times)	None	If other instrument failures occur while these channels are failed, it could result in an MSIV closure, steam dump valve opening and/or reactor trip.	B	1	1,2
b. Failure of a feedwater flow instrument channel producing a false low feedwater flow signal to the controller.	2×10^{-6}/hr (taken 3 times)	None	None	B	1	1,2
c. Failure in the steam generator level channel resulting in a false low steam generator level signal to the controller.	1×10^{-6}/hr (taken 3 times)	None	None	B	2	1,2
d. Failure of the level controller circuitry.	3×10^{-5}/hr (shift in calibration)	None	None	B	1	1,2
e. Failure of power to the level controller due to a fuse, breaker, or ABT malfunction.	1×10^{-5}/hr (premature breaker transfer)	None	None	B	1	1,2
f. Controller manual control element malfunctions (short circuits, opens, shorts to ground, or switch failure).	1×10^{-7}/hr (failure of contacts given no switch operation)	None	None	B	2	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Generator Water Level Control System

FAILURE MODE High Feedwater Flowrate (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
• There appears to be a possible common mode failure between this system and other systems through failures within the electrical power, control and service air, heating, ventilation and air conditioning and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Line Overpressure Protection

FAILURE MODE Inadvertent operation of a power operated or safety relief valve

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure in Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
A power operated relief valve opens due to one of the following malfunctions:						
a. Manual control switch failure results in an open signal to the valve.	3×10^{-8}/hr/switch (short across contacts)	None	None	B	2	1,2
b. Automatic pressure relief circuit failure results in the valve opening when the pressure is below the set point.	9×10^{-5}/hr (shift in calibration)	None	None	B	1	1,2
c. Power operated valve fails open due to valve mechanical failure.	1×10^{-5}/hr/valve (premature open)	None	None	B	1	1,2
d. Pressure instrument supplying the automatic system fails high.	3×10^{-6}/hr (instrument failure to operate)	None	None	B	1	1,2
A main steam safety valve opens due to one of the following reasons:						
a. The lift setpoint drifted to a lower value.	1×10^{-5}/hr/valve (premature open)	None	None	B	1	1,2
b. The valve experiences a mechanical failure.	1×10^{-5}/hr/valve (premature open)	None	None	B	1	1,2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and instrument and control air systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Main Steam System

FAILURE MODE High steam flowrate or inadvertent main steam isolation valve opening

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
A main steam system piping failure occurs which causes a high steam flowrate.	1×10^{-10}/hr/section	None	Major effects on many systems.	A	3	1,2
Under conditions where it is intended to remain closed, a main steam isolation valve fails open due to:						
a. Control switch failure resulting in an open signal to the MSIV.	1×10^{-8}/hr/switch (short across contacts)	None	None	B	2	1,2
b. Control solenoid valve failure that results in opening of the MSIV.	3×10^{-8}/hr (rupture)	None	None	B	2	1,2
c. Failure in the solenoid control circuitry that results in an open signal to the MSIV.	1×10^{-6}/hr/device (solid state device failure)	None	None	B	2	1,2
Under conditions where it is intended to remain closed, an MSIV bypass valve opens due to:						
a. Control switch failure resulting in an open signal to the MSIV bypass valve.	1×10^{-8}/hr/switch (short across contacts)	None	None	B	2	1,2
b. Mechanical valve failure.	3×10^{-8}/hr (rupture)	None	None	B	2	1,2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air, and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Turbine Electro-Hydraulic Control System (EHC)

FAILURE MODE Inadvertent opening of the govenor and/or intercept valves

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient Category[b]
The turbine govenor and/or intercept valves open excessively, causing an increase in the steam flowrate due to:						
a. Failure of the turbine speed sensor system causing a low speed signal to the electro-hydraulic controller.	3×10^{-5}/hr (shift in calibration)	None	None	B	1	1,2
b. Failure of the turbine impulse pressure instrument resulting in a low pressure signal to the electro-hydraulic controller.	3×10^{-5}/hr (shift in calibration)	None	None	B	1	1,2
c. Failure of the electro-hydraulic control system's electronic controller which results in a erroneous output signal.	1×10^{-6}/hr (solid state device fails to function)	None	None	B	1	1,2
d. Switch failure (short to power or mechanical failure) in the control panel causing an erroneous load increase signal to the controller.	1×10^{-8}/hr	None	None	B	3	1,2
e. Mechanical failure of the governor/intercept valve causes it to go fully open.	1×10^{-3}/d/valve (failure to operate open or close)	None	None	B	1	1,2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Auxilliary Feedwater System

FAILURE MODE High feedwater flowrate or inadvertent operation

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The auxiliary feedwater flowrate is higher than necessary due to:						
a. A control switch failure resulting in startup of a standby auxiliary feedwater pump.	1×10^{-8}/hr/switch (short across contacts)	None	None	B	2	1,2
b. A control switch failure resulting in the pump discharge valve opening.	1×10^{-8}/hr/switch (short across	None	None contacts)	B	2	1,2
c. The turbine driven auxiliary feedwater pump speed increases due to a circuitry failure in the speed controller.	1×10^{-6}/hr (fails to function)	None	None	B	2	1,2
d. The turbine driven auxiliary feedwater pump's speed is too high due to the speed governor suffering a mechanical failure.	1×10^{-3}/hr (failure to operate)	None	None	B	1	1,2
e. When given a control signal to reduce speed, the turbine driven pump speed remains constant due to a stuck governor valve.	1×10^{-3}/hr (failure to operate)	None	None	B	1	1,2
Auxiliary feedwater flow is initiated inadvertently due to:						
a. A manual control switch failure resulting in a start signal (short to power, mechanical failure, ground).	1×10^{-8}/hr (short across contacts)	None	None	B	3	1,2
b. A spurious safety injection or blackout signal causes the motor driven auxiliary feedwater pumps to start.	6×10^{-5}/hr (shift in calibration)	None	None	B	1	1,2
c. A failure in the auxiliary feedwater pump start up control circuitry results in a pump start signal.	2×10^{-7}/hr (motor starter all modes)	None	None	B	2	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Auxiliary Feedwater System

FAILURE MODE High feedwater flowrate or inadvertent operation (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air, and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Generator Blowdown System

FAILURE MODE Low blowdown flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The steam generator blowdown flowrate is reduced due to one of the following failures:						
a. Failure of the flow signal to the flow controller.	3×10^{-5}/hr (shift in calibration)	None	None	B	1	1
b. Failure of the flow controller resulting in an output signal to the flow control valve to decrease flow.	1×10^{-6}/hr (solid state device fails to function)	None	None	B	1	1
c. Failure of control air to the controller.	4×10^{-6}/hr/unit (compressor failure)	None	None	B	1	1
d. Blockage of the air line to the control valve.	8×10^{-7}/hr (air filter failure)	None	None	B	2	1
e. Rupture or sheared air line to the control valve.	1×10^{-9}/hr	None	None	B	3	1
f. Flow control valve mechanical failure shut. (Either one of the two series valves in each blowdown line closing would stop blowdown flow for that S.G.).	6×10^{-7}/hr/S.G. (failure to remain open)	None	None	B	2	1
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air, heating and ventilation, and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Turbine Generator Support System

FAILURE MODE Turbine trip due to a failure in support systems

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The turbine trips due to a failure in one of the following input channels to the turbine generator trip circuit.						
a. Turbine overspeed.	3×10^{-5}/hr (shift in calibration)	None	Open steam dump valves and atmospheric relief valves; reactor trip.	A	1	1,2
b. Thrust bearing failure.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and the steam dump and atmospheric relief valves open.	A	1	1,2
c. Turbine bearing low oil pressure.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip; steam dump and atmospheric relief valves open.	A	1	1,2
d. Low condenser vacuum.	3×10^{-5}/hr (shift in calibration)	The steam dump system becomes inoperable if same instrument channel is used.	Reactor trip; atmospheric relief valves open.	A	1	1,2
e. Manual trip mechanism.	1×10^{-8}/hr	None	Reactor trip; steam dump and atmospheric relief valves open.	A	3	1,2
f. 2 out of 3 low steam generator water level channels taken 3 times.	2.7×10^{-9}/hr [shift in calibration $(3 \times 10^{-5}/hr)^2$ times 3]	None	Auxiliary feed-water pumps start. steam generator water level control gets erroneous level signal-opens regulating valve.	A	3	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Turbine Generator Support System

FAILURE MODE Turbine trip due to a failure in support systems (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient Category[b]
g. Reactor trip signal (two seperate channels).	2×10^{-6}/hr (solid state device failure)	Reactor Trips	Reactor trip and associated interlock actions.	A	1	1,2
h. Switch failure for manual trip at the control board.	1×10^{-8}/hr (short across contacts)	None	Reactor trip and associated interlock actions.	A	3	1,2
i. Main feedwater pump breakers open (2 out of 2 trip signals).	1×10^{-12}/hr (2/2 solid state devices fail)	None	Reactor trip and associated interlock actions.	A	3	1,2
j. Circulating water pump breakers open (3 out of 3 trip signals).	1×10^{-18}/hr (3/3 solid state devices fail)	None	Reactor trip and associated interlock actions.	A	3	1,2
k. Electro-hydraulic governor DC power monitor.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
l. Loss of generator field.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
m. Negative sequence on generator.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
n. Unit differential current.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
o. OCB 52-8 monitoring circuit failure.	1×10^{-6}/hr (coil open or short)	None	Reactor trip and associated interlock actions.	A	2	1,2
p. OCB 52-9 monitoring circuit failure.	1×10^{-6}/hr (coil open or short)	None	Reactor trip and associated interlock actions.	A	2	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Turbine Generator Support System

FAILURE MODE Turbine trip due to a failure in support systems (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
q. Unit auxiliary transformer-faulty pressure.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
r. Unit auxiliary transformer differential current.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
s. Exhaust hood temperature high.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
t. Main transformer-faulty pressure.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
u. Generator ground monitoring circuit failure.	1×10^{-6}/hr (coil open or short)	None	Reactor trip and associated interlock actions.	A	2	1,2
v. Voltage controlled overcurrent relay.	1×10^{-6}/hr (coil open or short)	None	Reactor trip and associated interlock actions.	A	2	1,2
w. Generator differential current.	3×10^{-5}/hr (shift in calibration)	None	Reactor trip and associated interlock actions.	A	1	1,2
The turbine trip due to a failure in the turbine generator trip logic circuit.	1×10^{-6}/hr (solid state device fails)	None	Reactor trip and associated interlock actions.	A	2	1,2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air, heating and ventilation, and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Auxiliary Steam System

FAILURE MODE High steam flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The extraction steam flowrate becomes abnormally high due to one of the following failures in the system:						
a. An extraction steam valve fails open.	3×10^{-7}/hr/valve (failure of valve to remain open)	None	High and low pressure heaters will lose full heating capability.	B	2	1
b. An extraction steam valve suffers a rupture.	1×10^{-8}/hr/valve (rupture)	None	High and low pressure heaters will lose full heating capability.	B	3	1
c. An auxiliary steam pipe rupture.	1×10^{-10}/hr (per section)	None	High and low pressure heaters will lose full heating capability.	B	3	1

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Dump System

FAILURE MODE High steam flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient Category[b]
One or more steam dump valve/s open/s or increases the amount that it/they are open due to one of the following failures:						
a. Manual control switch failure.	1×10^{-8}/hr (short across contacts)	None	None	B	3	1,2
b. The turbine load signal to the average temperature programmer fails low causing a low T_{ref} output.	1×10^{-6}/hr (solid state device fails)	None	None	B	2	1,2
c. The average temperature programmer circuitry fails causing an erroneously low T_{ref} output.	1×10^{-6}/hr (solid state device fails)	None	None	B	2	1,2
d. One or more of the temperature signals to the average temperature unit fails high causing an erroneously high T_{AVG} signal to the steam dump controller.	1×10^{-6}/hr (instrumentation-fails to operate)	None	None	B	2	1,2
e. Averaging unit failure resulting in an erroneously high T_{AVG} signal to the steam dump controller.	1×10^{-6}/hr (solid state device fails)	None	None	B	2	1,2
f. Steam dump controller fails resulting in an open signal to the valves.	1×10^{-6}/hr (solid state device fails)	None	None	B	2	1,2
g. The steam dump cutout permissive circuit fails resulting in a spurious signal to the valves.	1×10^{-6}/hr (solid state device fails)	None	None	B	2	1,2
h. The steam dump positioner fails and sends an open signal to the valves.	1×10^{-6}/hr (instrumentation-fails to operate)	None	None	B	2	1,2
i. Control solenoid valve fails allowing the steam dump valve to be fully opened.	1×10^{-8}/hr (rupture)	None	None	B	3	1,2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Steam Dump System

FAILURE MODE High steam flowrate (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Reactor Coolant System

FAILURE MODE High coolant flowrate

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient Category[b]
An idle reactor coolant pump inadvertently starts due to one of the following failures:						
a. Switch contacts fail open or closed without any switch operation.	3×10^{-7}/hr per switch	None	None	B		2
b. Short occurs in pump control circuit wiring.	1×10^{-8}/hr per pump	None	None	B		2
c. Inadvertent closure of the circuit breaker due to a breaker failure.	2×10^{-7}/hr	None	None	B		2
Note: The plant Technical Specifications do not permit N-1 loop operation at power. Therefore, all three reactor coolant pumps should be running during power operation and an inadvertent start should not be possible.						
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

SYSTEM Pressurizer Overpressure Protection System

FAILURE MODE Premature opening of a relief or safety valve

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
A pressurizer power operated relief valve opens prematurely due to one of the following failures:						
a. With the PORV selector switch in "Auto", theassociated pressurizer instrument fails.	3×10^{-5}/hr per PORV	None	Reactor coolant system has a loss of coolant.	B	1	2
b. With the PORV selector switch in "Auto", the pressure switch fails and actuates prematurely.	3×10^{-5}/hr per PORV contacts)	None	Reactor coolant system has a loss of coolant.	B	1	2
c. The PORV selector switch fails resulting in a manual open signal to the logic circuitry.	3×10^{-7}/hr per PORV	None	Reactor coolant system has a loss of coolant.	B	1	2
d. A control circuit logic gate suffers a failure resulting in an open signal to the PORV.	2×10^{-6}/hr per PORV	None	Reactor coolant system has a loss of coolant.	B	1	2
A pressurizer safety valve opens premature due to one of the following failures:						
a. Premature open due to setpoint drift.	1×10^{-5}/hr per safety valve	None	Reactor coolant system has a loss of coolant.	B	1	2
b. Mechanical valve failure--rupture.	1×10^{-8}/hr per safety valve	None	Reactor coolant system has a loss of coolant.	B	1	2
A pressurizer PORV or safety valve does not close after it has opened due to a valve failure.	2×10^{-2}/d per valve	None	Reactor coolant system has a loss of coolant.	B	1	2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Pressurizer Overpressure Protection System

FAILURE MODE Premature opening of a relief or safety valve (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Safety Injection System

FAILURE MODE Inadvertent initiation

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The Safety Injection System is inadvertently initiated due to one of the following failures:						
a. Failure of 2 out of 3 pressurizer pressure instruments or a shift in calibration.	2.7×10^{-9}/hr	None	The safety injection signal would cause a reactor trip and if pressure is low enough would inject borated water.	A	3	2
b. Failure of 2 out of 3 containment pressure instruments resulting in a shift in calibration or erroueous high indication.	2.7×10^{-9}/hr	None	The safety injection signal would cause a reactor trip and if pressure is low enough would inject borated water.	A	3	2
c. Failure of 2 out of 3 steam line differential pressure instruments resulting in a shift in calibration or erroneous high indication.	2.7×10^{-9}/hr per steam line	None	The safety injection signal would cause a reactor trip and if the primary pressure is low enough borated water would be injected.	A	3	2
d. Manual pushbutton failure by shorting to power.	1×10^{-8}/hr per each of 2 buttons	None	The safety injection signal would cause a reactor trip and if the primary pressure is low enough borated water would be injected.	A	3	2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Safety Injection System

FAILURE MODE Inadvertent initiation (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
e. Failure in the following instrument channels to result in high steam line flow (1 ou. of 2 instrument) in 2 out of 3 steam lines along with either 2 out of 3 low T_{AVG} or 2 out of 3 low steam line pressure.	3×10^{-5}/hr/per inst. channel-- 5.8×10^{-17}/hr	The main steam line isolation valves would close.	The safety injection signal would cause a reactor trip and if the primary pressure is low enough borated water would be injected.	A	1	2
f. Failure in a logic gate in the safety injection system actuation circuitry.	1×10^{-6}/hr per steam line	None	The safety injection signal would cause a reactor trip and if the primary pressure is low enough borated water would be injected.	A	2	2
g. Failure of control relay in safety injection pump circuitry.	7×10^{-9}/hr per steam line	None	If primary pressure is below the shut-off head of the SI pumps, then borated water will be injected into the PCS.	B	3	2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Residual Heat Removal System

FAILURE MODE High RHR flowrate or inadvertent initiation of RHR flow

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
The RHR flow control valve fails open during the cooling mode due to one of the following failures:						
a. Valve suffers a mechanical failure and opens further than necessary for the existing conditions.	1×10^{-8}/hr	None	None	B	3	2
b. Control solenoid valve fails resulting in the flow control valve opening.	1×10^{-8}/hr	None	None	B	3	2
c. Control circuitry failure results in a open signal to the flow control valve.	1×10^{-8}/hr (short to ground)	None	None	B	3	2
d. Switch failure results in a open signal to the flow control valve.	1×10^{-8}/hr (short across contact)	None	None	B	3	2
The standby RHR pump is inadvertently started due to one of the following failures: (SI initiation covered seperately)						
a. Failure of a relay in the motor control circuit.	1×10^{-6}/hr/relay	None	None	B	2	2
b. Manual start switch fails resulting in a start signal to the pump motor.	1×10^{-8}/hr/switch	None	None	B	2	2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Reactor Control Rod Drive System

FAILURE MODE Inadvertent insertion or rod drop

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
Control rods are inadvertently inserted into the core due to one of the following failures:						
a. A failure of one or more of the control rod actuators which results in an insertion signal to the drive mechanisms.	1×10^{-6}/hr (short or open relay coil)	None	Decrease in primary temperatures, automatic control would try to correct.	B	2	2
b. Failure in manual rod control switch which results in an insertion signal to the control rod actuators.	1×10^{-8}/hr/switch (short across contacts)	None	Decrease in primary temperatures, automatic control would try to correct.	B	3	[illegible]
c. Failure in the sequential rod control unit and/or the permissive circuits resulting in an insertion signal to actuators.	1×10^{-6}/hr (short or open relay coil)	None	Decrease in primary temperatures, automatic control would try to correct.	B	2	2
Control rods are inadvertently dropped into the core due to one of the following failures:						
a. Loss of power from the solid state power cabinet due to a blown fuse, tripped breaker, or open wire.	1×10^{-5}/hr (breaker premature transfer)	None	Initiate a turbine load cutback by EHC system and inhibit rod withdrawal.	B	1	2
b. Electrical failure of stationary or moveable gripper coils in a control rod drive mechanism.	1×10^{-6}/hr/CRDM (coil short or open)	None	Initiate a turbine load cutback by EHC system and inhibit rod withdrawal.	B	1	2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Reactor Control Rod Drive System

FAILURE MODE Inadvertent insertion or rod drop (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure in Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
c. Mechanism failure of control rod drive mechanism latch assembly.	1×10^{-6}/hr/CRDM (clutch premature disengagement)	None	Initiate a turbine load cutback by EHC system and inhibit rod withdrawal.	B	1	2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Feedwater and Condensate System

FAILURE MODE Failure of the feedwater/condensate heating

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused by This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
Steam flow is lost to the high and low pressure heaters due to one of the following failures:						
a. The extraction steam regulating valve/s closes due to mechanical failure/s.	3×10^{-7}/hr/valve (failure to remain open)	None	Decrease in feedwater temperatures will cause decrease in cold leg temperature which will add positive reactivity to the reactor.	B	2	2
b. One or more of the non-return valves close due to a failure in the control system.	3×10^{-7}/hr/valve (air operated valve fails to remain open)	None	Decrease in feedwater temperatures will cause decrease in cold leg temperature which will add positive reactivity to the reactor.	B	2	2
c. Failure of the heater drain tank pump/s results in tank overfill thereby restricting steam flow to the heaters.	1×10^{-5}/hr/motor (motor fails to run)	None	Decrease in feedwater temperatures will cause decrease in cold leg temperature which will add positive reactivity to the reactor.	B	1	2
d. Failure of the heater drain tank control system which results in overfilling the tank.	3×10^{-5}/hr (Instrument system shift in calibration)	None	Decrease in feedwater temperatures will cause decrease in cold leg temperature which will add positive reactivity to the reactor.	B	1	2

APPENDIX D. ROBINSON A-47 IE&C ANALYSIS (continued)

SYSTEM Feedwater and Condensate System

FAILURE MODE Failure of the feedwater/condensate heating (continued)

Event Initiator Producing the Failure Mode	Failure Rate[a]	Failures in Other System Caused By This Event Initiator	Effect of Failure In Other System(s)	Fault Effect Designation	Probability Category	Transient[b] Category
Feedwater or condensate flow bypasses the low pressure heaters due to the following failure:						
a. One or more of the three-way bypass valves fails in the bypass position.	3×10^{-7}/hr/valve (failure to remain open on air operated valves)	None	Decrease in feedwater temperature, will cause decrease in cold leg temperature which will add positive reactivity to the reactor.	B	[illegible]	2
There appears to be a possible common mode failure mechanism between this system and other systems through failures in the electrical power, instrument and control air and fire protection systems.	None assigned for this report	Not determined for this report; will be evaluated following computer model simulations.	TBD[c]	TBD	TBD	1,2

a. From Appendix D, Table D-1.

b. 1--steam generator overfill transient, 2--reactor coolant system overcooling transient.

c. TBD--To be determined.

TABLE D-1. STATISTICAL ANALYSIS TABLE

Component and Failure Mode	Failure Rate	Error Factor	Remarks
1. Pumps:			From proposed NREP data base--Reference 1.
a. Motor:			Pump and motor; excludes control circuits.
Failure to start on demand	1E-3/d	10	
Failure to run, given start	1E-5/hr	10	
b. Turbine:			Pump, turbine, steam and throttle valves, and governor.
Failure to start on demand	1E-2/d	10	
Failure to run, given start	1E-5/hr	3	
c. Diesel:			Pump, diesel, lube oil system, fuel oil, suction and exhaust air, and starting system.
Failure to start	1E-3/d	3	
Failure to operate	1E-4/hr	30	
2. Valves:			Catastrophic leakage valves assigned by engineering judgement; catastrophic leakage assumes the valve to be in a closed state, then the valve fails. From Reference 1 except as noted.
a. Motor operated:			
Failure to remain open	1E-7/hr	3	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
2. Valves (continued)			
Failure to open/close	1E-3/d	10	
Rupture	1E-8/hr	10	From WASH-1400--Reference 2.
b. Solenoid operated:			
Failure to operate (open or close)	1E-3/d	3	
Rupture	1E-8/hr	10	Based on WASH-1400--Reference 2.
c. Air/fluid operated valves:			
Failure to operate (open or close)	1E-3/d	10	
Failure to remain open	3E-7/hr	100	From IEEE-500--Reference 3.
Rupture	1E-6/hr	10	From WASH-1400--Reference 2.
d. Check valves:			
Failure to open	1E-4/d 1E-7/hr	3 10	
Failure to close	1E-3/d 1E-6/hr	3 10	
Internal leakage (catastrophic)	1E-8/hr	100	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
2. Valves (continued)			
d. Check valves (continued):			
Rupture	1E-8/hr	10	From WASH-1400--Reference 2.
e. Manual valves:			
Failure to operate (open or close)	1E-4/d	3	Failure to operate is dominated by human error; rate is based on one actuation per month.
	1E-7/hr	10	
Rupture	1E-8/hr	10	Based on WASH-1400--Reference 2.
f. Code safety valves:			
Fail to open	1E-5/d	3	
Premature open	1E-5/hr	3	From WASH-1400--Reference 2.
Fail to reclose (given valve open)	1E-2/d	10	
g. Relief valves:			
Failure to open	1E-4/d	10	
Premature open	1E-5/hr	3	From WASH-1400--Reference 2.
Failure to close, given open	2E-2/d	3	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
2. Valves (continued)			
h. Test valves, flow meters, orifices:			
Fail to remain open (plug)	3E-4/d	3	
Rupture	1E-8/hr	10	
i. Stop check valves:			
Failure to open	1E-4/d	3	
3. Switches:			Where torque/limit switches are used as parts of pumps/valves, switch failure rate included in pump/valve failure rate. From Reference 1
a. Limit:			
Failure to operate	1E-4/d	3	
b. Torque:			
Failure to operate	1E-4/d	3	
c. Pressure:			
Failure to operate	1E-5/d	3	
d. Manual:			
Fail to transfer	1E-4/d	10	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
4. Switch Contacts:			From WASH-1400--Reference 2.
Failure of NO contacts to close, given switch operation	3E-7/hr	3	
Failure of NC contacts by opening, given no switch operation	1E-7/hr	3	
Short across NO/NC contact	1E-8/hr	10	
5. Circuit Breakers:			Includes all components of the circuit breaker mounted on drawout frame. From Reference 1.
Failure to transfer (open or close)	1E-3/d	10	
Premature transfer	1E-5/hr	10	For sizes 4kV and smaller.
6. Fuse:			
Failure to open	1E-5/d	3	From WASH-1400
Premature open	1E-6/hr	10	From proposed NREP data base--Reference 1
7. Bus:			From proposed NREP data base--Reference 1.
Failure	1E-8/hr	3	All modes
8. Transformer:			From proposed NREP data base--Reference 1.
Failure (open ckt or short)	1E-6/hr	3	All modes

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
9. Emergency Diesel (complete plant):			Engine frame and associated moving parts, generator coupling, governor, static exciter, output breaker, lube oil system, fuel oil, suction and exhaust air, starting system; excludes starting air compressor and accumulator, fuel storage, load sequencers, and synchronizers. From Reference 1.
Failure to start	3E-2/d	3	
Failure to run (emergency conditions, given start)	1E-3/hr	10	
10. Relays:			
Fail to energize	1E-4/d	3	From WASH-1400--Reference 2.
Failure to transfer (open or close)	1E-4/d	10	From Reference 1.
Short across NO/NC contact	1E-8/hr	10	From WASH-1400--Reference 2.
Coil (open or short)	1E-6/hr	10	From Reference 1.
11. Battery Power System (wet cell):			Assumes out-of-spec cell replacement. From Reference 1.
Fails to provide proper output	1E-6/hr	3	
12. Battery Charger:			From proposed NREP data base--Reference 1.
Failure to operate	1E-6/hr	3	
13. DC-Motor-Generator:			From proposed NREP data base--Reference 1.
Failure to operate	1E-6/hr	10	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
14. Wires:			Consistent with IEEE-500 data for 1000 circuit feet. From Reference 1 except as noted.
Open circuit	1E-6/hr	10	
Short to ground	1E-7/hr	10	
Short to power (control circuit)	1E-8/hr	10	
Short to power (power circuit--line to line)	1E-6/hr	3	From IEEE-500--Reference 3.
15. Solid State Devices High Power Applications:			For more detailed information, see MIL-HDBK-217C. From Reference 1.
Fails to function	1E-6/hr	10	
16. Solid State Devices Low Power Application			See MIL-HDBK-217C. From Reference 1.
Fails to function	1E-6/hr	10	
17. Terminal Boards:			Values given are per terminal. From Reference 1.
Open connection	1E-7/hr	10	
Short to adjacent circuit	1E-7/hr	10	
18. Damper:			From Reference 1.
Failure to operate	1E-3/d	10	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
19. Motor:			From WASH-1400--Reference 2. Electric motor.
Failure to start	3E-4/d	3	
Failure to run	1E-5/hr	3	
20. Motor Starter:			
All modes	2E-7/hr	10	Spurious operation, fails to open/close, fails to interrupt on opening. From IEEE-500--Reference 3.
21. Pipe (per section):			Per 12-ft section. From WASH-1400-Reference 2.
Rupture			
<3-in. rupture	1E-9/hr	30	
>3-in. rupture	1E-10/hr	30	
22. Heat Exchanger:			From proposed NREP data base--Reference 1.
Tube leak	1E-9/hr	10	Per tube.
Shell leak	1E-6/hr	10	
Plugged	1E-6/hr	10	From IREP/Browns Ferry--Reference 4.
23. Strainer/Filter (liquid):			For clear fluids; contaminated fluids or fluids with a heavy chemical burden should be considered on a plant-specific basis. Reference 1.
Plugged	1E-5/hr	10	

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
24. Clutch:			From WASH-1400--Reference 2.
Mechanical failure to operate	3E-4/d	10	
Electrical failure to operate	3E-4/d	3	
Premature disengagement	1E-6/hr	10	
25. Instrumentation General--(includes: transmitters, amplifiers, and output devices):			From proposed NREP data base--Reference 1.
Failure to operate	1E-6/hr	10	
Shift in calibration	3E-5/hr	10	
26. Compressors:			
All modes	4.17E-6/hr	30	From IEEE-500--Reference 3.
27. Chiller:			
Fails to operate	8E-6/hr	10	From Reference 5.
28. Fans (Cooling Tower):			
All modes	1.24E-6/hr	10	From Reference 3.

TABLE D-1. (continued)

Component and Failure Mode	Failure Rate	Error Factor	Remarks
29. Fans (HVAC)			
All modes	2.22E-6/hr	3	From Reference 3.
30. CIS Valves			Values derived from Reference 6. A PWR plant was chosen with the largest number of CIS valve leakage failures. Failure rates are based on number of failures, calendar hours from date of initial criticality for the time period of January 1, 1976 to December 31, 1978, and valve population which was obtained from the specific plant's inservice testing program.
a. Air operated			
Leakage	4.2E-6/hr	10	
b. Check Valve			
Leakage	3.8E-5/hr	10	
31. Filters (air):			
Failure	8.0E-7/hr	30	From Reference 8.
32. Power			
Loss of offsite power (LOSP)	1.0E-5/hr		From Reference 7.
Loss of Unit Auxiliary Transformer (UAT)	3.0E-3/hr		Failure rate is the square root of the LOSP failure rate.
Loss of Reserve Auxiliary Transformer (RAT)	3.0E-3/hr		Failure rate is the square root of the LOSP failure rate
33. Flanges			
Rupture/Leak	3.0E-7/hr	30	From Reference 2.

TABLE REFERENCES

1. A. J. Oswald et al., Generic Data Base for Data Models Chapter of the National Reliability Evaluation Program (NREP) Guide, EGG-EA-5887, June 1982.

2. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commerical Nuclear Power Plants, WASH-1400 (NUREG 75/014), October 1975.

3. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations, IEEE Std 500-1977, June 1977.

4. S. E. Mays et al., Interim Reliability Evaluation Program: Analysis of the Browns Ferry, Unit 1 Nuclear Plant, Appendix C--Sequence Quantification, NUREG/CR-2902, EGG-2199, July 1982.

5. R. H. Nicholls and O. Gokcek, Reliability Data for the CRBRP Shutdown Heat Removal System, CRBRP-GEFR-00554, August 1981.

6. R. J. Nicholls and O. Gokcek, A Reliability Assessment of the Clinch River Breeder Reactor Plant SHutdown Heat Removal System, CRBRP-GEFR-00552, January 1982.

7. A. S. McClymont and B. W. Poehlman, ATSW: A reapprasial; Part 3: Frequency of Anticipated Transients, EPRI NP-2330, 1982.

8. R. P. Dawkins and J. A. Derdiger, Component Failure and Repair Data: Casification--Combined-Cycle Power-Generation Units, EPRI-AP-2205, DE82 902081, February 1982.

APPENDIX E

STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING POSTULATED TRANSIENT SCENARIOS

APPENDIX E

STEAM GENERATOR OVERFILL AND REACTOR COOLANT SYSTEM OVERCOOLING POSTULATED TRANSIENT SCENARIOS

1. INTRODUCTION

This phase of the steam generator overfill and reactor coolant system overcooling report was performed to identify transient and accident scenarios which have the potential to produce results which would be more limiting than those presented in the H. B. Robinson Final Safety Analysis Report.

2. ASSUMPTIONS

1. A single safety grade component failure may be assumed.

2. Multiple control grade failures may be assumed.

3. A single occurrence which results in multiple failures is considered to be a single failure.

3. SEQUENCE OF EVENTS FOR STEAM GENERATOR OVERFILL ACCIDENT

3.1 H. B. Robinson Licensing (FSAR) Accident Analysis

The H. B. Robinson FSAR does not recognize or analyze any accidents associated with a steam generator overfill event.

4. POSTULATED ACCIDENT

Through the course of this study there have been no failures of control grade systems or components identified that could create a steam generator overfill design basis accident.

5. SEQUENCE OF EVENTS FOR STEAM GENERATOR OVERFILL TRANSIENT

5.1 H. B. Robinson Licensing (FSAR) Transient Analysis

The H. B. Robinson FSAR does not recognize or analyze any transients associated with the steam generator overfill event.

6. POSTULATED TRANSIENT

The following initial conditions will be assumed. Hot zero power, feedwater system in manual on the bypass valves with auxiliary feedwater still operating, the feedwater regulating valve fails full open. As an aggravating failure, when the steam generator level reaches the high level trip, the feedwater pump breaker fails to trip.

The initiating event is failure of one steam generator feed flow regulating valve full open. This failure is assumed to result in an increase in feed flow rate to 100% or greater for the affected steam generator.

The result of this initiating event is assumed to be a steam generator water level increase of approximately 3.0 inches/sec or greater. With an aggravating failure of the feedpump breaker failing to open upon demand it is postulated that water will enter the main steam line in approximately 32 s.

Based on these assumptions it can be postulated that in approximately 32 seconds water will reach the main steam line nozzle and begin to enter the steam line. (Assumed initial level of 39% of narrow range indication.)

6.1 Sequence of Events

Initial conditions: hot zero power, reactor feedwater system in manual, normal steam generator vessel water level (39% of indicated narrow range).

Event	Time (second)
Hot zero operation (0-5% power)	0
Feedflow regulating valve for one steam generator fails full open and feedflow goes to 100% or greater	10
High level trip setpoint reached, feedwater pump breaker trip fails to actuate	15
Water reaches main steam line nozzle.	42

6.2 Discussion

In applying the normal assumptions used for licensing reviews this is considered to be a valid scenario of concern. An initiating event was assumed and an additional active failure was assumed.

Since these feedwater pump trip circuits are not considered safety related or designed to safety grade standards it could further be assumed that on a generic basis a single event such as a seismic event could cause failure of two or more trip circuits.

Additional failures which were identified as potential initiators or aggravators were considered to be bounded by the postulated transient scenario. See Table E-1 for a complete listing of additional failures that may be used as aggravating failures in later postulated scenarios based on computer model simulation results.

TABLE E-1. STEAM GENERATOR OVERFILL POSTULATED AGGRAVATING FAILURES

System	Ranking	Postulated Effects
Control rod drive system (rod withdrawal) *(C.M.F. 1,4)	B3	Rod withdrawal--increase in reactor power
Main steam system (main steam isolation valve opens) *(C.M.F. 1,2)	B2	Could cause level swell and slightly faster level rise
Steam line overpressure protection system (relief or safety opens) *(C.M.F. 1,2)	B1	Could cause level swell and slightly faster level rise
Turbine EHC system (power increase) *(C.M.F. 1,2,4)	B1	Could cause level swell and slightly faster level rise
Steam dump system (inadvertent open) *(C.M.F. 1,4)	B2	Could cause level swell and slightly faster level rise
Steam generator water level control system *(C.M.F. 1,2,3,4)	B1	Could cause faster level rise or could cause additional failures in other steam generator levels.
Feedwater and condensate system (high flowrate) *(C.M.F. 1,2,4)	B1	Could cause faster level rise due to failure of valves to respond to signals.

* Common Mode Failure (C.M.F) 1--Electrical (loss of power), 2--Control and Service Air (low or loss of air pressure), 3--Heating, Ventilation and Air Conditioning (loss of HVAC), 4--Fire Protection (actuation).

6.3 Conclusions

Although defining the actual consequences of a steam generator overfill transient is considered beyond the scope of this task, it could be postulated that main turbine damage could be caused by this scenario and the possibility of main steam line damage due to the static loading of water is also possible. Additionally, thermal stresses and the possibility that safety systems which are connected to the main steam system could be disabled or damaged by water loading are concerns. For example, main steam isolation valves or safety relief valve(s) could be damaged due to thermal stresses and/or water loadings.

Operator action might be postulated to terminate the transient or limit the consequences by manually isolating the feedwater system from the steam generator. However, based on the time frame involved (less than 1 minute) operator action is not considered.

6.4 Additional Analysis Required

The consequences of this postulated scenario cannot be predicted at this time. In a later phase of this study computer simulations will be performed to determine the control system response and to calculate nuclear and thermal hydraulic responses to this scenario. Additional aggravating failures can be postulated at that time to verify suspected minimal effects. Systems which are suspected of being susceptible to common mode failures will be modeled and the effects of the failures will be analyzed. Common mode failures will be analyzed for a loss of power, low or loss of air pressure, overheating and fire protection actuation. Insight gained from the computer simulation will be used to postulate other potentially significant scenarios and to determine which systems have a negligible effect. System failures which produce scenarios more severe than previously analyzed will then be evaluated to determine if the specific scenarios are applicable on a generic basis.

7. SEQUENCE OF EVENTS FOR REACTOR COOLANT SYSTEM OVERCOOLING ACCIDENT

7.1 H. B. Robinson Licensing (FSAR) Accident Analysis

The identified design basis accident for the overcooling event in the H. B. Robinson FSAR is the main steam line break outside containment with offsite power available.

8. POSTULATED MORE SEVERE ACCIDENT

The design basis accident for an overcooling event also meets all of the requirements necessary to classify it as a transient. Therefore, the postulated more severe transient scenario will also qualify as the more severe accident scenario and is documented in Section 10 of this Appendix.

9. SEQUENCE OF EVENTS FOR REACTOR COOLANT SYSTEM OVERCOOLING TRANSIENT

9.1 H. B. Robinson Licensing (FSAR) Transient Analysis

Events that result directly in a reactor vessel water temperature decrease are those that either increase the flow of cold water to the reactor vessel or increase the rate of heat removal from the reactor coolant system through the steam generator. The event that results in the most severe transient in this category is the main steam line break outside of containment with offsite power available.

A rupture of a steam pipe is assumed to include any accident which results in an uncontrolled steam release from a steam generator. The release can occur due to a break in a pipe line or due to a valve malfunction. The steam release arising from a rupture of a main steam pipe would result in an initial increase in steam flow, with a decrease during the accident as the steam pressure falls. The energy removal from the RCS would cause a reduction of coolant temperature and pressure. With a negative moderator temperature coefficient, the cooldown would result in a reduction of core shutdown margin. If the most reactive control rod assembly is assumed stuck in its fully withdrawn position, there is a possibility that the core will become critical and return to power even with the remaining control rods inserted. A return to power following a steam pipe rupture is a potential problem only because of the high hot channel factors which may exist when the most reactive rod is assumed stuck in its fully withdrawn position. Assuming the most pessimistic combination of circumstances which could lead to power generation following a steam line break, the core is ultimately shut down by the boric acid in the SI System.

The analysis of a steam pipe rupture is performed to demonstrate that:

1. With a stuck rod cluster control assembly (RCCA), with or without offsite power, and with minimum engineered safety features, the core remains in place and essentially intact so as not to impair effective cooling of the core and no consequential damage to the primary system occurs.

2. With no stuck rod and all equipment operating at design capacity, insignificant cladding rupture occurs.

Although DNB following a steam pipe rupture is not necessarily unacceptable, the following analysis shows that, in fact, no DNB occurs for any rupture, assuming the most reactive rod stuck in its fully withdrawn position.

The following functions provide the necessary protection against a steam pipe rupture:

1. SI System actuation from any of the following:*

   a. Two out of three pressurizer low pressure signals,

   b. Two out of three high differential pressure signals between any steam line and the main steam header,

   c. High steam flow in two out of three lines (one out of two per line) in coincidence with either low RCS average temperature (two out of three) or low steam line pressure (two out of three), and

   d. Two out of three high containment pressure signals.

2. The overpower reactor trips (nuclear flux and ΔT) and the reactor trip occurring in conjunction with receipt of the SI signal.

3. Redundant isolation of the main feedwater lines. Sustained high feedwater flow would cause additional cooldown; thus, in addition to the normal control action which will close the main feedwater valves, any SI signal will rapidly close all feedwater control valves, trip the main feedwater pumps, and close the feedwater pump discharge valves.

4. Trip of the fast acting steam line stop valves (designed to close in less than 5 s with no flow) on:

   a. High steam flow in two out of three main steam lines (one out of two per line) in coincidence with either low RCS average temperature (two out of three) or low steam line pressure (two out of three).

   b. Two, 2/3 high-high containment pressure signals.

Each steam line has a fast closing stop valve with downstream check valve. These six valves prevent blowdown of more than one steam generator for any break location even if one valve fails to close. For example, for a break upstream of the stop valve in one line, closure of either the check valve in that line or the stop valves in the other lines will prevent blowdown of the other steam generators. In particular, the arrangement precludes blowdown of more than one steam generator inside the containment and thus prevents structural damage to the containment.

Steam flow is measured by monitoring the dynamic head in the nozzles inside the steam pipes. The nozzles, which are considerably smaller in diameter than the mainsteam pipes (16.5 in. ID vs. a pipe diameter of 23.8 in. ID), are located inside the containment near the steam generators, and also serve to limit the maximum steam flow for any break further downstream. In particular, the nozzles limit the flow for all breaks outside the containment.

9.2. Sequence of Events

Initial conditions: hot zero power

Event	Time (Seconds)
0% operation (Hot Zero Power)	0
Main steam line circumferentially severes.	10
Core returns to power.	24
Boron reaches the core to terminate the power increase.	48

Steam line break transients were performed with PTS-PWR/MOD002 to establish reactor conditions at the times of expected minimum DNB ratios (peak heat fluxes). These conditions (pressure, inlet temperature, core average density, etc.) were input to the XTG code. This two group, three-dimensional, reactor simulation code established the hot channel factors around the stuck rod, and predicted the corresponding minimum DNB ratio.

The PTS-PWR/MOD002 segment of this analysis was initiated from hot zero power conditions, assuming the most reactive rod to be withdrawn from the core. A shutdown reactivity of 1.77% was assumed. Initial temperatures and pressure were such that the primary and secondary systems were in equilibrium.

As a worst case, the steam line break is assumed to occur at hot zero power conditions. At that time, the steam generator secondary side water inventory is at a maximum, prolonging the duration and increasing the magnitude of the primary system cooldown. For conservatism, the most reactive control rod is assumed to be stuck out of the core when evaluating the shutdown capability of the control rods.

The analysis utilizes two codes:

1. PTS-PWR/MOD002, which determines the system transient response, and

2. XTG, which performs the space-dependent calculations and predicts the DNB ratio using the thermal-hydraulic conditions as predicted by PTS-PWR/MOOD002.

The worst steam line break was found to be a large break outside the containment with outside power available. The core returns to power at 14 s. Boron reaches the core at 38.0 s, terminating the power increase. Heat flux peaks soon afterward at 45% of rated value of 184,000 BTU/hr ft^2.

Input conditions for the XTG portion of the analysis were taken at the time of peak heat flux (42 s). Based on these conditions, the XTG analysis predicted an MDNBR of 1.33, based on an overall hot channel factor of 13.7.

This transient is a cooldown event for which the enveloping core parameter values occur at the end of the cycle (EOC). The only change in EOC coefficients is the moderator pressure coefficient, which changes from-0.05 pcm/psi to +0.0 pcm/psi; this tends to reduce the possibility of the core returning to criticality. Therefore, this event has not been reanalyzed with a positive MTC.

10. POSTULATED MORE SEVERE TRANSIENT

The same initial conditions will be assumed.

Hot zero power.

The initiating event for this transient will be circumferential break of a main steam line outside of containment. This is further aggravated by failure of the MSIV for the affected loop to close on demand. The assumption that the most reactive control rod cluster remains stuck in the full withdrawn position will be deleted as it appears to be non-conservative for an overcooling transient. It will require additional time for the core to return to power, if it does, and violation of the 10 CFR 50 Appendix G curve will be more severe in intensity and duration.

10.1 Sequence of Events

Initial Conditions: 0% design power.

Event	Time (Seconds)
Hot zero operation	0
Main steam line circumferentially ruptures outside of containment.	10
Main steam isolation valves for non-affected loops close.	16
High concentration boron reaches the core and shutdowns or maintains the reactor shutdown.	48

10.2 Discussion

In utilizing normal licensing review assumptions this scenario is considered valid and appears to be of concern. An initiating event was assumed and then was aggravated by failure of a safety related system. During the course of this study there have been several system failures identified that have the potential to contribute to an overcooling event. These failures, when considered singularly, appear to be of no consequence to this type of transient. However, when they are considered in conjunction with other failures, a serious overcooling transient could result. The actual consequences attributable to this transient in forms of excessive thermal shock to primary components or possible damage due to thermal limits being exceeded are beyond the scope of this task.

Additional system or component failures which have a potential to aggravate or contribute to an overcooling transient but were considered to be bounded by the postulated scenario are summarized Table E-2.

10.3 Conclusions

The ability to factually state that any of these failures either singularly or in combinations will actually cause an overcooling transient more severe than previously analyzed or create a thermal shock possibility is beyond our capabilities for this portion of this task and will require computer analysis to affect final determinations.

10.4 Additional Analysis Required

The consequences of this postulated scenario cannot be predicted at this time. In a later phase of this study computer simulations will be performed to determine the control system response and to calculate nuclear and thermal hydraulic responses to this scenario. Additional aggravating failures can be postulated at that time to verify suspected minimal effects. Systems which are suspected of being susceptible to common mode failures will be modeled and the effects of the failures will be analyzed. Common mode failures will be analyzed for a loss of power, low or loss of air pressure, overheating and fire protection actuation. Insight gained from the computer simulation will be used to postulate other potentially significant scenarios and to determine which systems have a negligible effect. System failures which produce scenarios more severe than previously analyzed will then be evaluated to determine if the specific scenarios are applicable on a generic basis.

TABLE E-2. REACTOR COOLANT SYSTEM OVERCOOLING POSTULATED AGGRAVATING FAILURES

Failure System/Component	Failure Mode	Ranking	Postulated Effect
Feedwater and Consensate System *(C.M.F. 1,2,4)	Failure to shutdown automatically	B-1	Continued flow of relatively cold water to the steam generator causing continued excessive cooldown rate.
Primary Overpressure Protection System *(C.M.F. 1,2)	Inadvertent opening of a relief or safety valve	B-1	Causes steam flow from the pressurizer and additional cooldown of the primary water.
Electro-Hydraulic Control System (EHC) *(C.M.F. 1,4)	Inadvertent opening of turbine governor or bypass valve(s)	B-1	This would cause increased steam flow and subsequent cool-down as heat is being extracted at a rate faster than it is being added.
Residual Heat Removal System (RHR) *(C.M.F. 1,4)	Excessive heat removal rate due to high flow rate	B-3	During shutdown the potential exists to create an over-cooling transient if RHR flow fails high.
Residual Heat Removal Service Water System *(C.M.F. 1,4)	Excessive heat removal rate due to increase flow rates	B-3	Inadvertent startup of idle pumps or flow control valve failures could cause the RHR system to be cooled beyond allowable limits and therefore the primary system could be overcooled.

* Common Mode Failure (C.M.F) 1--Electrical (loss of power), 2--Control and Service Air (loss of air), 3--Heating, Ventilation and Air Conditioning (loss of HVAC), 4--Fire Protection (actuation).

NRC FORM 335 (11 81)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)	EGG-EA-6473
4. TITLE AND SUBTITLE	Report Concerning the Effects of Control System Failures on Steam Generator Overfill and Reactor Coolant System Overcooling Events at a Typical Westinghouse 3-Loop Plant
2. (Leave blank)	
3. RECIPIENT'S ACCESSION NO.	
7. AUTHOR(S)	D. E. Baxter, S. J. Bruske, C. B. Ransom
5. DATE REPORT COMPLETED	MONTH: December; YEAR: 1983
9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)	EG&G Idaho, Inc. Idaho Falls, ID 83415
DATE REPORT ISSUED	MONTH: December; YEAR: 1983
6. (Leave blank)	
8. (Leave blank)	
12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)	Division of Safety Technology Office of Nuclear Reactor Regulation U.S. Nuclear Regulatory Commission Washington, DC 20555
10. PROJECT/TASK/WORK UNIT NO.	
11. FIN NO.	A6477
13. TYPE OF REPORT	
PERIOD COVERED (Inclusive dates)	
15. SUPPLEMENTARY NOTES	
14. (Leave blank)	

16. ABSTRACT (200 words or less)

This is a completed interim report on the effects of control system failures on steam generator overfill and reactor coolant system overcooling events at H. B. Robinson. It includes the Failure Mode and Effects Analysis, Potentially Significant Systems List, Detailed Review Tables, and the Postulated Worse Case Transients for these events.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT	
19. SECURITY CLASS (This report)	Unclassified
21. NO. OF PAGES	
20. SECURITY CLASS (This page)	Unclassified
22. PRICE	$

NRC FORM 335 (11 81)