TP

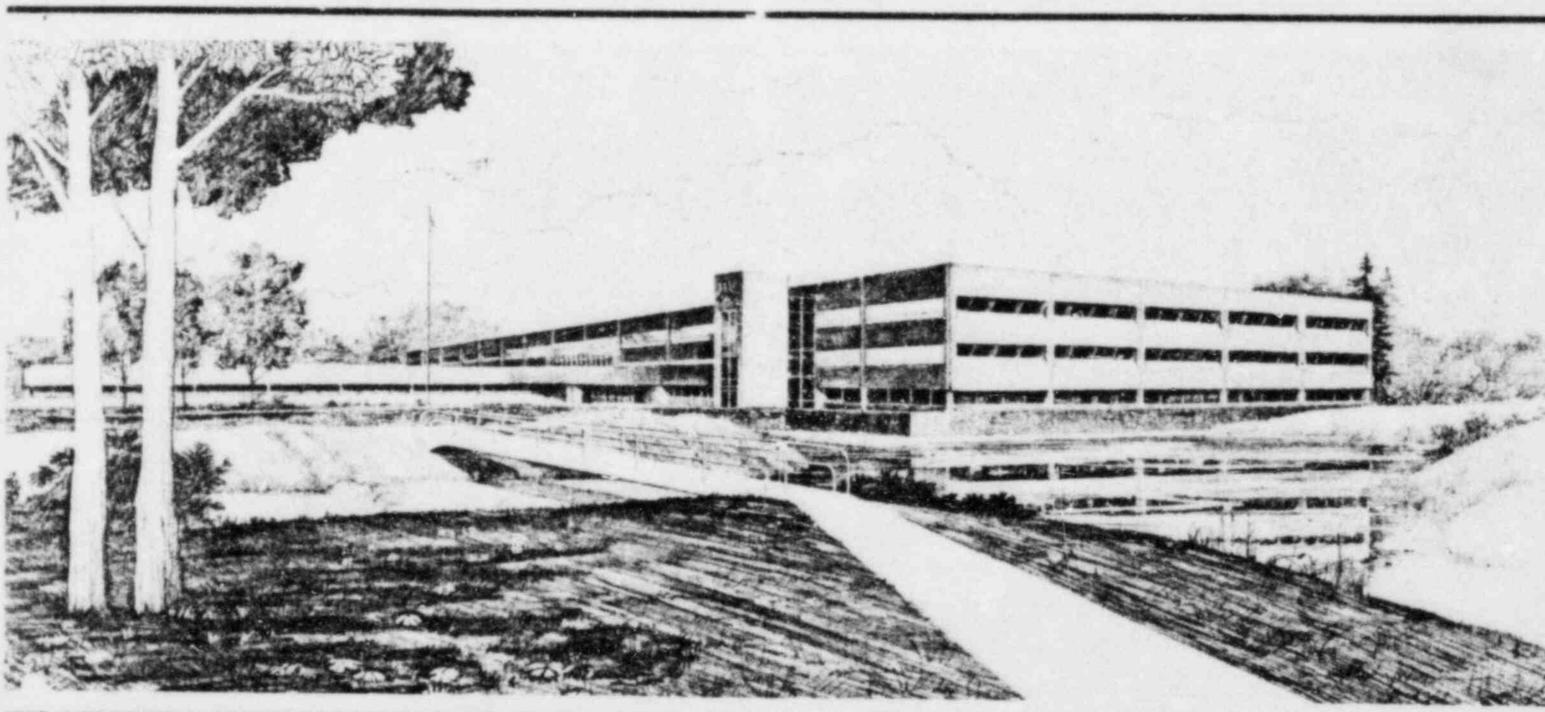
EGG-EA-6353

OCTOBER 1983

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON OVERFILL/OVERCOOLING EVENTS AT BROWNS FERRY

D. E. Baxter
S. J. Bruske
D. J. Morken

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



This is an informal report intended for use as a preliminary 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-6353

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON OVERFILL AND OVERCOOLING EVENTS AT BROWNS FERRY

D. E. Baxter
S. J. Bruske
D. J. Morken

Published October 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 overfill and overcooling events 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 overfill and overcooling events at the Browns Ferry 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.

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

CONTENTS

SUMMARY

The purpose of this study is to determine which system or systems if any at commercial Boiling Water Reactor (BWR) 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 BWR 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 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.

REPORT CONCERNING THE EFFECTS OF CONTROL SYSTEM FAILURES ON OVERFILL AND OVERCOOLING EVENTS AT BROWNS FERRY

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 reactor vessel overfill and overcooling events are included in the A-47 study. This report addresses only the overfill and overcooling events. Later reports 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 an overfill or overcooling event.

2. METHOD OF ANALYSIS

The evaluation of control system failures or malfunctions on reactor vessel overfill and/or overcooling events at boiling water reactors (BWR) 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 boiling water reactor sites, and then identify those systems which could be postulated to cause or contribute to an overfill or overcooling event. A review of the Browns Ferry Final Safety Analysis Report (FSAR) provided a list of 56 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 was 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 overfill and overcooling only Criteria 1 and 2 of Appendix A are applicable.

In order to determine which systems have a potential for affecting or causing an overfill or overcooling event two separate approaches were utilized. These two methodologies were performed separate of each other to preclude as much commonalty 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 BWRs for the years 1980 through 1982. The review was focused around any and all events that were

or could be classified as overfill or overcooling events. This detailed review produced several instances which caused or contributed to an overfill and/or 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. A composite listing of several of these events as documented in the Nuclear Power Experiences[1] is contained in Appendix G.

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 rejection.

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 and the statistical calculations are contained in Appendix E.

Transient scenarios were then developed utilizing these tables and engineering evaluations. The postulated scenarios are contained in Appendix F and are considered to be more severe than those presented in the Browns Ferry Final Safety Analysis Report. Included in Appendix F 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 Browns Ferry 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 an overfill or overcooling event are considered beyond the scope of this task, it could be postulated that an 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, 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 the high pressure coolant injection (HPCI) turbine might be disabled, 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 F identify concerns with control system failures as they relate to overfill and 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 scenarios indicate potential problems with regard to overfill and overcooling transients resulting from the design and operation of the reactor feedwater and control system.

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

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

Based on the concerns associated with overfill and overcooling events, the reactor 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 overfill and overcooling transients and defining of the safety significance of each.

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. Reevaluation of the overcooling and overfill transients by the licensees and proposed modifications to existing safety systems to preclude the effects of these transients.

2. Provide additional systems designated as "Interlock Systems Important to Safety" to preclude the postulated effects of these transients.

3. Reclassification of the reactor 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. REFERENCES

1. Nuclear Power Experiences BWR-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 c[illegible]t failure, either initiating or aggravating, which results in an undesired increase in reactor coolant inventory to the point where water enters the main steam line will be recommended for further review.

   The Browns Ferry bounding transient analysis presented in the FSAR for increase in reactor coolant inventory is a "Feedwater Controller Failure-Maximum Demand, 115% Feedflow". The addition of feedwater is terminated 5 seconds after transient initiation by the reactor vessel high water level trip.

   The design basis accident for this event is a main steam line break outside of containment. This accident is terminated by closure of the main steam isolation valves.

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 limiting transient for this event in the Browns Ferry FSAR analysis is the "Loss of Feedwater Heater(s) equivalent to a 100°F Decrease in Temperature." This represents the maximum temperature decrease obtainable through tripping or bypassing of heaters caused by a single event.

   There is no design basis accident identified for the decrease in reactor coolant temperature event.

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 a reactor core coolant flow increase beyond the bounds of the present Final Safety Analysis Report (FSAR) analysis results will be recommended for further review.

The limiting transient for a nuclear pressure increase event in the Browns Ferry FSAR analysis is the "Loss of Condenser Vacuum". This represents the instantaneous loss of vacuum and closure of the turbine stop valves and bypass valves, therefore, all stored energy must be dissipated through the relief valves.

There is no design basis accident identified for the pressure increase event.

The limiting transient for a positive reactivity increase event in the Browns Ferry FSAR analysis is a "Continuous Rod Withdrawal During Reactor Startup." This represents the most severe transient. The reactor is just critical at room temperature and a high worth, out of sequence, rod is continuously withdrawn.

The design basis accident for a positive reactivity increase event is a rod drop (ejection) and is terminated with a reactor trip.

The limiting transient for a reactor core coolant flow increase event in the Browns Ferry FSAR analysis is "Recirculation Flow Controller Failure--Increasing Flow." This represents the fastest rate at which flow can be increased with the reactor power level at the most optimum level to maximize the severity of the transient.

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

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

The limiting transient for a reactor vessel inventory decrease event presented in the Browns Ferry FSAR is "Loss of Feedwater Flow from High Power." This represents the maximum anticipated rate of inventory decrease due to the high steam flow rate.

The design basis accident for the decrease in inventory event is a loss of coolant accident caused by a circumferential break of the recirculation system crosstie with the crosstie valve(s) open.

The limiting transient for a reactor core coolant flow decrease event in the Browns Ferry FSAR analysis is a "Recirculation Pump Seizure." This represents the fastest flow decrease possible through any single failure or operator action.

There is no design basis accident identified for a decrease reactor core coolant flow event.

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

OVERFILL/OVERCOOLING TRANSIENTS FAILURE MODE AND EFFECTS ANALYSIS

APPENDIX B. OVERFILL/OVERCOOLING TRANSIENTS FAILURE MODE AND EFFECTS ANALYSIS

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Reactor Recirculation System	Controls flow through the reactor vessel and thereby controls reactor power.	High flow rate or inadvertent startup of a recirculation loop.	These failures should not have the potential to cause or contribute to an overfill transient as the increase in flowrate would cause void collapse and level shrink. These failures appear to have the potential to cause or contribute to an overcooling transient.	2 (Appendix C, item 1)
		Low flow rate.	These failures appear to have the potential to cause or contribute to an overfill transient but should not cause an overcooling transient as the low flow rate would result in a heatup situation rather than cooldown.	1 (Appendix C, item 1)
Nuclear System Pressure Relief System	Provides the required overpressure protection for the nuclear supply system.	Inadvertent opening of a relief or safety valve.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 2)
		Failure to open when required to relieve pressure.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as failure to open would cause void depression (level shrink) and a power increase which would cause heatup rather than cooldown of the water.	None
Main Steam Line Isolation Valves	Provides isolation of the reactor vessel from the remainder of the steam supply system.	Inadvertent individual valve closure.	These failures should not have the potential to cause or contribute to an overfill transient and should not result in an overcooling transient as the sudden reduction in steam flow would result in a power increase and a heatup situation and overfill is not a problem as the MSIV would already be closed.	None
		Inadvertent individual valve opening or failure to close upon demand.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system valves are arranged 2 in series and failure of one valve to close or inadvertent opening of one valve should not cause or contribute to the transient of concern. The entire system is safety grade and would require failure of both valves which is beyond the scope of this task.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Reactor Core Isolation and Standby Cooling Systems	Provides makeup water to the reactor vessel from various sources whenever the vessel is isolated.	Failure to stop makeup flow on high level or inadvertent start-up when not required.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 3)
		Failure to provide the required makeup flow to the vessel.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the lack of makeup flow would cause no level increase and no cooling.	None
Residual Heat Removal System	Provides for heat removal from the primary system during normal shutdown and accident conditions.	Failure to supply the required heat removal.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as failure to remove heat does not result in a cooling transient and the heat addition rate is not sufficient to cause a significant void formation and subsequent level rise.	None
		Failure to control the heat removal rate.	These failures should not have the potential to cause or contribute to an overfill transient as the increased cooling would cause void collapse and level shrink. The excess cooling could cause or contribute to an overcooling transient.	2 (Appendix C, item 4)
Reactor Water Cleanup System	Provides filtration and ion exchange to maintain the reactor water purity. Also serves as a letdown path during startup.	Failure to provide letdown flow when necessary.	These failures appear to have the potential to cause or contribute to an overfill transient but should not cause or contribute to an overcooling transient as the volume of the system in comparison to the primary system is insignificant.	1 (Appendix C, item 5)
		Failure to stop letdown flow when required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the flow out would tend to lower level and the lower level would tend to aid a heatup vice cooldown situation.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Primary Containment System and Reactor Vessel Isolation Control System	Provides automatic isolation of the primary system and reactor vessel to prevent a release to the environs.	Failure to affect isolation when required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is designed to contain the primary coolant after a design basis accident but does not directly provide coolant or cooling to the core.	None
		Inadvertent isolation when not required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is designed to contain the primary coolant after a design basis accident but does not directly provide coolant or cooling the the core.	None
Secondary Containment System	Provides backup isolation to the primary containment to prevent releases to the environs.	Failure to affect isolation when required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is designed to contain any releases from the primary containment but does not directly provide coolant or cooling to the core.	None
		Inadvertent isolation when not required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is designed to contain any release from the primary containment but does not directly provide coolant or cooling to the core.	None
Reactor Protection System	Provides protection to the reactor system and fuel from damage due to out of tolerance conditions.	Failure to provide the required trips and isolations.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is safety grade, redundant and would require multiple failures to fail to provide any required trips or isolation that may have an affect on these transients and multiple safety grade failures is beyond the scope of this task.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
		Inadvertent trips and isolations.	These failures appear to have the potential to cause or contribute to an overcooling transient even though system is safety grade because the system is failing in the safest mode.	2 (Appendix C, item 8)
Core Standby Cooling Control and Instrumentation System	Provides protection from excess fuel clad temperatures in the event of a breach in the nuclear process barrier that results in a loss of reactor coolant.	Failure to initiate cooling of the core when required.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as failure to initiate would result in a loss of level and heatup situation.	None
		Failure to terminate cooling of the core upon reaching high vessel water levels or inadvertent initiation of cooling systems when not required.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 6)
Neutron Monitoring System	Monitors the neutron flux level of the core over the range of shutdown to full power.	Indicates higher than actual levels.	These failures should not have the potential to cause or contribute to an overfill overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
		Indicates lower than actual levels.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
Refueling Interlocks System	Restricts the movements of refueling equipment and control rods during refueling to prevent a criticality.	Failure to restrict movements when necessary.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Failure to allow movements when necessary.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Reactor Manual Control and Control Rod Drive Systems	Provides the means to manipulate the control rods for gross reactivity control.	Inadvertent rod withdrawal, or ejection.	These failures appear to have the potential to cause or contribute to an overfill transient but not an overcooling transient as the power increase would add heat to the vessel vice cause cooling.	1 (Appendix C, Item 7)
		Inadvertent rod(s) insertion while at power.	These failures appear to have the potential to cause or contribute to an overcooling transient but not an overfill as the power decrease would tend to cause void collapse and level shrink vice swell.	2 (Appendix C, item 7)
Reactor Vessel Instrumentation	Monitors and transmits information concerning the conditions within and of the reactor vessel.	Transmits or indicates higher than actual conditions.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but will be covered in a later phase of this study because it affects operator actions.	None
		Transmits or indicates lower than actual conditions.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but will be covered in a later phase of this study because it affects operator actions.	None
Feedwater Control System	Provides the necessary signals to maintain the required feedflow to maintain proper reactor vessel level.	High flow rate.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 9)
		Low flow rate.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as low feed flow will cause a loss of level and a heatup problem vice cooldown.	None
Pressure Regulator and Turbine Generator Control System	Provides the necessary control to maintain the turbine load and reactor pressure at prescribed levels.	Inadvertent opening of turbine governor or bypass valves.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 10)
		Inadvertent closing of turbine governor or bypass valves.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the sudden pressure increase results in void collapse, level shrink, power increase and a heatup vice cooldown transient.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Process Radiation Monitoring System	Monitors various lines for radioactive materials released to the environs by process liquids and gases or through process system failures.	Indicates higher than actual levels of radiation.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Indicates lower than actual levels of radiation.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Area Radiation Monitoring System	Monitors for radiation at various locations within the reactor building, turbine building and radwaste building.	Indicates higher than actual levels.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Indicates lower than actual levels.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Site Environmental Radiation Monitoring System	Monitors for natural and other radiation levels outside the plant.	Indicates higher than actual levels.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Indicates lower than actual levels.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Health Physics Lab Radiation Monitoring System	Monitors for abnormal radiation levels within the health physics lab.	Indicates higher than actual level.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Indicates lower than actual level.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Process Computer System	Monitors and logs process variables and provides certain analytical computations.	Provides higher than actual outputs.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
		Provides lower than actual outputs.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
Backup Control System	Provides the capability to shut down the reactor and operate required emergency systems from locations outside the control room in the event the control room must be evacuated.	Inability to shut down the reactor or stop makeup flows from remote locations.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 11)
		Inadvertent shutdown of the reactor or startup of emergency makeup systems from remote locations.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 11)
Diesel Generator Systems	Provides the necessary services to ensure the diesel generators are capable of coming on line and supplying electrical power.	Failures that result in a loss of service which prevents the diesel from coming on line and supplying electrical power.	Failures of this type should not have the potential to cause or contribute to an overfill or overcooling transient as the systems are safety grade, redundant and would require multiple failures to prevent all of the diesels from coming on line and supplying the required power.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Normal Auxiliary Power System*	Provides the power source for the unit auxiliaries through various transformers.	Failure to provide the required power to the unit auxiliaries.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but are evaluated within the individual systems supplied by this power source.	None
Standby AC Power Supply System*	Provides an emergency supply of electrical power to emergency and safety equipment.	Failure to provide the necessary power to the designated equipment.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is safety grade, redundant and would require multiple failures to prevent the supplying of power to the equipment. Failures of the equipment supplied by this system are evaluated within those systems.	None
250 V DC Power Supply System*	Provides the power source for the engineered safety features of one unit and the safe shutdown loads of the other two units.	Failure to provide the necessary power to the designated equipment.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system is safety grade, redundant and would require multiple failures to prevent the supplying of power to the equipment. Failures of the equipment supplied by this system are evaluated within those systems.	None
120 V AC Power Supply System*	Provides power to equipment through; a) 120 V instrument and control power, b) plant preferred and nonpreferred 120 V system and c) unit preferred 120 V AC system.	Failure to provide the necessary power to the designated equipment.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but are evaluated within the individual systems supplied by this power source.	None
Auxiliary DC Power Supply System*	Provides 48 V power to the plant communications and annunciators systems during all modes of operations.	Failure to provide the required power to the designated equipment.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but are evaluated within the individual systems supplied by this power source.	None
Liquid Radwaste System	Provides for the collection, storage and disposal of the liquid radwaste generated at the unit.	Failure to provide the required collection, storage or disposal of liquid radwaste.	These failures appear to have the potential to contribute to an overfill transient but are insignificant for this study and these failures should not have the potential to cause or contribute to an overcooling transient as the system has no direct capabilities to supply cooling to the reactor vessel.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Solid Radwaste System	Provides for the collection, storage and disposal of the solid radwaste generated at the unit.	Failure to provide the required collection, storage or disposal of solid radwaste.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Gaseous Radwaste System	Provides for the collection, storage and disposal of the gaseous radwaste generated at the unit.	Failure to provide the required collection, storage or disposal of the gaseous radwaste.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
New Fuel Storage System	Provides for the dry storage of new fuel until ready for core loading.	Failure to store the fuel safely and effectively.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Spent Fuel Storage System	Provides for the storage of spent fuel until ready for shipment.	Failure to store the spent fuel safely and effectively.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Fuel Pool Cooling and Cleanup System	Provides for water cleanup and cooling of the spent fuel pool.	Failure to maintain water temperature or purity requirements.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Reactor Building Closed Cooling Water System	Provides cooling water to designated auxiliary plant equipment during both normal and emergency conditions.	Loss of cooling water to designated equipment.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and loss of equipment cooling will not be transmitted to the reactor vessel.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
		Excessive cooling water to designated equipment.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and excessive cooling of the equipment will not be transmitted to the reactor vessel in enough magnitude to be significant.	None
Raw Cooling Water System	Provides cooling water to the RBCCW system and the turbine associated equipment.	Loss of cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
		Excessive cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel.	None
Raw Service Water System	Provides cooling water to miscellaneous plant equipment and yard watering supply.	Loss of cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Excessive cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Residual Heat Removal (RHR) Service Water System	Provides cooling water to the RHR system and the emergency equipment cooling water system.	Loss of cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the loss of flow would cause a heatup transient vice cooldown and unless there is a failure of the heat exchanger this system cannot provide coolant to the reactor vessel.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
		Excessive cooling water flows.	These failures appear to have the potential to cause or contribute to an overcooling transient but should not cause or contribute to an overfill transient unless there has been an additional failure of a heat exchanger tube which is determined to be insignificant for this transient as the volume of flow would require excessive time to be of a problem for overfill.	2 (Appendix C, item 12)
Emergency Equipment Cooling Water System	Provides cooling water flows to essential equipment during accident situations.	Loss of cooling water flows.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the loss of flow would create a heatup transient and unless there was failure of a heat exchanger this system does not have a capability to provide coolant to the reactor vessel.	None
		Excessive cooling water flows.	These failures appear to have the potential to cause or contribute to an overcooling transient but should not cause or contribute to an overfill transient unless there has been an additional failure of a heat exchanger and multiple failures of safety grade systems is beyond the scope of this task.	2 (Appendix C, item 13)
Fire Protection System*	Provides the plant with the required fire protection and fire combatants.	Failure to provide the necessary fire protection.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and any failures within other systems caused by these failures are evaluated within the individual systems.	None
		Inadvertent actuation.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and any failures within other systems caused by these failures are evaluated within the individual system.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Heating, Ventilation and Air Conditioning Systems*	Provides the plant with the necessary heating, ventilating and air conditioning.	Failure to provide sufficient H&V or air conditioning.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and any failures within other systems caused by these failures are evaluated within the individual system.	None
		Provides excessive H&V or air conditioning.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel and any failures within other systems caused by these failures are evaluated within the individual system.	None
Demineralized Water System	Provides the necessary demineralized water for plant makeup and other uses.	Failure to provide the necessary quantities of demineralized water.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as this would cause a coolant shortage and subsequent heatup vice cooldown.	None
		Failures resulting in an excessive amount of demineralized water being supplied.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but are considered insignificant as it would require failures of several systems to cause the excess coolant to get to the reactor vessel.	None
Control and Service Air Systems*	Supplies air to all pneumatically operated instruments, controls and final operators such as control valves.	Control or service air pressure fails low.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient but evaluation of system failures caused by these failures is covered in the individual systems affected by these failures.	None
		Control or service air pressure fails high.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Potable Water and Sanitary Systems	Supplies drinking water and water to the restrooms.	Loss of flow.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		High flow.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Equipment and Floor Drainage System	Collects and removes noncontaminated liquid wastes from the plant.	Drain piping clogged or valve(s) fail closed.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Drain piping break or valve(s) fail open.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Process Sampling Systems	Samples process liquids and gases to determine plant performance.	Sample system valve(s) fail open.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
		Sample system valve(s) fail closed.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Plant Communications	Provides interplant and intraplant communications.	System failure.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Lighting System	Provides lighting for plant operation.	Power supply or component failure.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Auxiliary Boiler System	Supplies building heat and steam for systems testing prior to or during startup.	High steam pressure.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct capabilities to provide coolant or cooling to the reactor vessel without an inadvertent erroneous valve manipulation by the operator. Operator error as an initiating event, is beyond the scope of this task and will not be addressed.	None
		Low steam pressure.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the system has no direct or indirect capabilities to provide coolant or cooling to the reactor vessel.	None
Turbine Generator System	Utilizes steam produced in the reactor to produce electric power.	Transient power increase.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 14)
		Transient power decrease.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the sudden drop in steam flow will collapse voids and cause a power increase which results in a heatup situation.	None
Main Steam System	Delivers steam from the reactor system to the Main, RFP, HPCI, and RCIC turbines as well as auxiliary steam loads.	Steam flow failures high.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 15)
		Steam flow failures low.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the sudden drop in steam flow will result in a void collapse, power increase and a heatup situation.	None

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Main Condenser System	Provides a heat sink for the steam leaving the turbine generator during power operations.	Loss of condenser vacuum.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the loss of vacuum will result in a turbine trip and void collapse which would cause level shrink and a heatup transient.	None
		Increase of condenser vacuum.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as any increase in vacuum above normal would be minimal and any steam flow changes would be insignificant for this study.	None
Turbine Bypass System	Provides a bypass around the turbine directly to the condenser for excess steam flow.	Bypass valve(s) fail open.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 16)
		Bypass valve(s) fail closed.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the sudden drop in steam flow will result in void collapse and a power increase which shrinks level and heats up the system.	None
Condenser Circulating Water System	Provides a heat sink for condensing exhaust steam from power generation operations.	Circulating water flow fails low.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as loss of flow would cause a loss of vacuum and resultant trips.	None
		Circulating water flow fails high.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the increase flow could only increase vacuum a minimal amount which results in an insignificant change for this study.	None
Condensate and Reactor-feedwater System	Provides feedwater to the reactor; condensate storage and transfer.	Feedwater/condensate flow fails high.	These failures appear to have the potential to cause or contribute to an overfill or overcooling transient.	1 and/or 2 (Appendix C, item 17)
		Feedwater/condensate flow fails low.	These failures should not have the potential to cause or contribute to an overfill or overcooling transient as the loss of flow would result in a loss of level and a heatup vice cooldown situation.	None

APPENDIX B. (continued)

System	System Function	System Failure Mode	Effect of Failure	Applicable A-47 Selection Criteria Appendix A (Scenario Discussion)
Standby Liquid Control System	Provides a backup method to make the reactor subcritical.	Fails to actuate when required.	These failures should not have the potential to cause or contribute to an overfill transient.	None
		Inadvertent actuation.	These failures appear to have the potential to cause or contribute to an overfill transient, however, the capacity of the system is insufficient to be of significant concern for this study.	None

* Failures are evaluated within individual systems.

APPENDIX C

OVERFILL AND/OR OVERCOOLING POTENTIALLY SIGNIFICANT SYSTEMS LIST AND DISCUSSIONS

APPENDIX C

OVERFILL AND/OR OVERCOOLING POTENTIALLY SIGNIFICANT SYSTEMS LIST AND DISCUSSIONS

1. Reactor Recirculation System

Overfill, Overcooling

Overfill

Failure Mode: Low flow rate; loss of flow.

Plant Conditions: High power level; high reactor vessel level.

Discussion: A loss of one or both recirculation pumps or rapid speed reduction of operating recirculation pump(s) would create a level swell due to decrease heat removal capability which causes voids to increase. Since the level was high at the beginning of the transient it is possible to exceed the high level limits.

Overcooling

Failure Mode: Inadvertent startup of a cold recirculation loop or recirculation control failure--increasing flow.

Plant Conditions: Any power level.

Discussion Inadvertent startup of a cold recirculation loop or a control failure that increases flow reduces the void content of the coolant flowing through the core leading to an overcooling transient of short duration.

2. Nuclear System Pressure Relief System

Overfill, Overcooling

Overfill

Failure Mode: Inadvertent opening of a safety or relief valve.

Plant Conditions: Any power level; high reactor vessel level (due to manual control of the feedwater control system).

Discussion: One or more of the relief or safety valves failing open causes a rapid loss of pressure, voids will be increased and with the high initial reactor vessel level an overfill transient may occur.

Overcooling

Failure Mode: Inadvertent valve opening or failure to close upon demand.

Plant Conditions: Any power level.

Discussion: An inadvertent opening or failure to close causes a removal of the heat content of the reactor coolant in the vessel and could lead to or contribute to an overcooling transient.

3. Reactor Core Isolation and Standby Cooling Systems

Overfill, Overcooling

Failure Mode: Inadvertent actuation; failure to stop makeup on high level.

Plant conditions: Any power level, any reactor vessel level.

Overfill

Discussion: Inadvertent actuation of HPCI or RCIC pumps could cause an overfill transient to occur. Failure to stop HPCI or RCIC pumps at the high level switch setpoint could cause reactor vessel level to exceed the high level limits.

Overcooling

Discussion: Inadvertent actuation of HPCI or RCIC pumps or a failure to stop makeup when required, causes cool water to be sent through the core which could lead to or aggravate an overcooling transient.

4. Residual Heat Removal System (RHRS)

Overcooling

Failure Mode: Failure to control the rate of heat removal.

Plant Conditions: Shutdown.

Discussion: Failure of the RHRS to control the rate of heat removal may result in exceeding the allowable reactor coolant system cooldown rate or limit.

5. Reactor Water Cleanup System

Overfill

Failure Mode: Failure to provide letdown flow when required.

Plant conditions: Low power level; high reactor vessel level.

Discussion: This transient typically should only be a problem when the reactor is being started up from shutdown conditions. Failure to allow letdown flow during startup could create a high level situation as the reactor comes to power. An excess coolant problem, that could be handled by the letdown system, during power operation could better be compensated for by decreasing feedwater flow and steaming off the excess coolant.

6. Core Standby Cooling Control and Instrumentation System

Overfill, Overcooling

Overfill

Failure Mode: Failure to terminate core cooling upon reaching the high level switches; inadvertent initiation of cooling systems when not required.

Plant Conditions: Any power level; any reactor vessel level.

Discussion: Failure to shutdown core cooling systems upon reaching high level limits or inadvertent startup of core cooling systems when not required will cause or contribute to the reactor vessel level exceeding the high level limit.

Overcooling

Failure Mode: Inadvertent initiation of the cooling systems when not required or failure to terminate core cooling when required.

Plant Conditions: Any power level.

Discussion: Either of the above failures could cause or contribute to an overcooling transient by decreasing the temperature of the coolant that flows through the core.

7. Reactor Manual Control and Control Rod Drive Systems

Overfill, Overcooling

Overfill

Failure Mode: Inadvertent rod withdrawal; control rod ejection.

Plant Conditions: Any power level; high reactor vessel level.

Discussion: The sudden power spike will cause increased void formation and the resultant level swell could exceed the high level limits.

Overcooling

Failure Mode: One or more rods insert while at power.

Plant Conditions: High power level.

Discussion: One or more rods inserting while at power causes heat to be removed at a rate faster than it is being added to the coolant and could lead to an overcooling transient.

8. Reactor Protection System

Overcooling

Failure Mode: Inadvertent reactor trip.

Plant Conditions: Any power level.

Discussion: Inadvertent reactor trip with subsequent failure of the turbine to trip would result in cooldown of the system to the point of main steam isolation valve closure on low pressure. This cooldown may be in excess of allowable limits.

9. Feedwater Control System

Overfill, Overcooling

Overfill

Failure Mode(s): High automatic feed flow rate failure without subsequent high level trip; high feed flow in manual control without a high level trip.

Plant Conditions: Any power level; any reactor vessel level.

Discussion: This system has a known failure mode that causes it to fail at 115% of normal 100% feed flow rate. This failure if incurred coincident with failure of the high vessel level switches will cause the vessel level to exceed the high level limits. An operator running the feed system in manual control could cause the vessel level to exceed the high level limits.

Overcooling

Failure Mode: Feedwater flow rate fails high.

Plant Conditions: Any power level.

Discussion: The addition of excessive feedwater has the potential to cause or contribute to an overcooling transient as cold feedwater is added at a faster rate than the core heat addition rate.

10. Pressure Regulator and Turbine Generator Control System

<u>Overfill, Overcooling</u>

Failure Mode(s): Inadvertent opening of turbine governor or bypass valves.

Plant Conditions: Any power level; high reactor vessel level.

<u>Overfill</u>

Discussion: When the turbine governor valve or bypass valve opens steam flow increases, reactor pressure drops, the voids increase in size and the reactor vessel level increases due to swell. This could be sufficient to cause the vessel level to exceed the high level limits.

<u>Overcooling</u>

Discussion: This failure could cause or contribute to an overcooling transient since the failure causes the removal of heat from the coolant in the reactor vessel at a rate faster than the heat addition rate.

11. Backup Control System

<u>Overfill, Overcooling</u>

Failure Mode: Inadvertent startup of HPCI, RCIC from a remote location or failure to shutdown on a high level.

Plant Conditions: Any power level; any reactor vessel level.

Overfill

Discussion: Any problem that could cause an inadvertent startup of a RCIC or HPCI pump has the potential to cause or contribute to an overfill transient due to the ability to raise the vessel level when not required.

Overcooling

Discussion: Any problem that could cause an inadvertent startup of a RCIC or HPCI pump has the potential to cause or contribute to an overcooling transient due to the ability to cool the water in the reactor vessel at a faster rate than the core heat addition rate.

12. Residual Heat Removal Service Water System (RHRSW)

Overcooling

Failure Mode: Excessive cooling water flow.

Plant Conditions: Shutdown.

Discussion: Failure of the RHRSW which could cause an excessive cooling water flow, could contribute to an overcooling transient by decreasing the RHR temperature, resulting in an excessive cooldown rate to the reactor coolant system.

13. Emergency Equipment Cooling Water System (EECWS)

Overcooling

Failure Mode: Excessive cooling water flow.

Plant Conditions: Shutdown.

Discussion: Failure of the EECWS which could cause an excessive cooling water flow, could contribute to an overcooling transient by decreasing the RHR temperature, resulting in an excessive cooldown rate to the reactor coolant system.

14. Turbine Generator System

Overfill, Overcooling

Failure Mode: Transient power increase.

Plant Conditions: Any power level; high reactor vessel level.

Overfill

Discussion: A sudden power demand will cause increased void formation and reactor vessel level swell which could exceed high level limits.

Overcooling

Discussion: A sudden demand will cause additional heat removal from the reactor coolant and could contribute to or cause an overcooling transient since heat removal could be at a higher rate than the core heat being added to the coolant.

15. Main Steam System

Overfill, Overcooling

Failure Mode: Steam flow fails high or steam flow to auxiliary loads fails low.

Plant Conditions: Any power level; high reactor vessel level.

Overfill

Discussion: An increased steam flow will cause increased void formation and level swell which could exceed high level limits.

Overcooling

Discussion: An increased steam flow will cause increased heat removal from the reactor coolant and could contribute to or cause an overcooling transient. A decreased auxiliary steam flow to the feedwater heaters could cause or contribute to an overcooling transient.

16. Turbine Bypass System

Overfill, Overcooling

Failure Mode: Bypass valve(s) fail open.

Plant Conditions: Any power level; high reactor vessel level.

Overfill

Discussion: An increased power demand on the reactor will cause increased void formation and level swell which could exceed high level limits.

Overcooling

Discussion: An increased power demand on the reactor will cause increased heat removal from the reactor coolant and could cause or contribute to an overcooling transient.

17. Reactor Condensate and Feedwater Systems

Overfill, Overcooling

Failure Mode: High condensate/feedwater flow.

Plant Conditions: Any power level; any reactor vessel level.

Overfill

Discussion: A failure in the condensate or feedwater system that causes an inadvertent feed flow increase has the potential to increase the reactor vessel level beyond the high level limits.

Overcooling

Discussion: A failure in the condensate or feedwater systems which causes an inadvertent increase of feedwater flow has the ability to cause or contribute to an overcooling transient as cold feedwater may be added at a higher rate than the core heat addition rate. If shutdown, an inadvertent increase of feedwater flow may cause an excessive cooldown rate, and result in an overcooling transient.

APPENDIX D

DETAILED REVIEW TABLES FOR OVERFILL AND OVERCOOLING TRANSIENTS

APPENDIX D

DETAILED REVIEW TABLES FOR OVERFILL AND OVERCOOLING TRANSIENTS

1. INTRODUCTION

This report section addresses the mechanistic analysis of the transients identified in the Failure Mode and Effects Analysis (FMEA) for overfill and 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 calculations performed in Appendix E. They were assigned a 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 an overfill transient and 2 is an 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 Browns Ferry documents were used to the extent of their availability. Where these documents were not available, best engineering assumptions based on experience, knowledge of other BWR 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
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Recirculation System
Failure Mode: Low Flow Rate or Loss of Flow

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Recirculation pump fails to continue to run due to mechanical/electrical pump/motor failure.	1×10^{-5}/hr	None	None	B	1	1
Recirculation pumps fail to continue to run due to mechanical/electrical pump/motor failures. (two or more pumps)	1×10^{-5}/hr for each pump	None	None	B	3	1
Generator field breaker fails open or trips inadvertently on recirculation motor-generator set.	1×10^{-5}/hr	None	None	B	1	1
Loss of unit auxiliary and startup transformers causing a trip of both recirculation motor-generator sets.	1×10^{-5}/hr for each circuit breaker	Turbine generator Feedwater Control and service air Condenser circulating water Raw cooling water Reactor building closed cooling water	Turbine trip Loss of condensate and booster pumps Loss of compressors Loss of heat sink Loss of heat sink Loss of heat sink	A	3	1
Loss of cooling water to MG sets from boosted cooling water.	1×10^{-5}/hr pump fails to run in cooling water system 1×10^{-7}/hr MOV inadvertently closes	None	None	B	3	1
Failure of master controller to minimum speed demand due to electronic failure(s).	1×10^{-6}/hr	None	None	B	1	1
Failure of suction or discharge valve to remain open due to either electrical or mechanical failures.	1×10^{-7}/hr	None	None	B	2	2
Failure of one or more jet pumps in one or both loops.	6×10^{-6}/hr for flanges on each jet pump pair	None	None	B	1	2

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Recirculation System (continued)
Failure Mode: Low Flow Rate or Loss of Flow (continued)

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Recirculation pump motor-generator scoop tube fails causing the recirculation pumps to decrease speed.	3×10^{-7}/hr	None	None	B	2	2
Recirculation pump motor-generator failure due to electrical/mechanical failure of motor or generator.	1×10^{-6}/hr	None	None	B	2	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Heating, Ventilation and Air Conditioning Systems, Fire Protection System and Electrical Power System.	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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Recirculation System
Failure Mode: High Flow Rate

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Electronic failure within master controller that causes recirculation pumps to accelerate to maximum speed.	1×10^{-6}/hr	None	None	B	1	2
Recirculation pump motor-generator scoop tube failure that causes recirculation pumps to increase speed.	3×10^{-7}/hr	None	None	B	2	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Heating and Air Conditioning Systems, Fire Protection Systems and Electrical Power Systems.	None assigned for this report	Not determined for this report, will be evalated following computer model simulations	TBD[c]	TBD	TBD	2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Nuclear System Pressure Relief System
Failure Mode: Inadvertent Opening of Pressure Relief Valve

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
One or more pressure relief valves open due to:						
(a) Wiring to valve actuator shorted to power.	1×10^{-8}/hr per valve	None	None	B	2	1,2
(b) Premature opening of valve(s) due to setpoint drift.	1×10^{-5}/hr per valve	None	None	B	1	1,2
(c) Inadvertent opening due to solenoid valve failure allowing air pressure to open valve.	1×10^{-3}/d	None	None	B	1	1,2
(d) Inadvertent opening due to relief valve failure.	1×10^{-8}/hr	None	None	B	2	
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air, Fire Protection and Electrical Power 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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Core Isolation Cooling System
Failure Mode: Inadvertent Startup

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
RCIC starts from 1 out of 2 taken twice low water level switches failing low.[c]	3×10^{-5}/hr for each sensor	HPCI RHR CSS Diesel generators ADS	Starts HPCI Starts RHR Starts core spray Starts diesels ADS permissive	B	3	1,2
RCIC starts from logic wiring to Relays 13A-K2 and K3 shorting to power. Initiating turbine steam supply valve FCV 71-8 opening.	1×10^{-8}/hr	None	None	B	2	1,2
RCIC starts from contacts 2-2T on manual control switch HS71-8A failing closed.	1×10^{-8}/hr	None	None	B	2	1,2
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air, Fire Protection and Electrical Systems.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[d]	TBD	TBD	1,2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. Safety grade switches.

d. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Core Isolation Cooling System
Failure Mode: System Fails to Shutdown

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Circuit breaker to the 250 V dc MOV BD 1C[c] fails open causing loss of control power used to close valve.	1×10^{-5}/hr	Loss of power to: a. 3 ADS valves b. 2 relief valves (valves close)	Relief valve system has eight other valves on a separate power supply.	A	1	1,2
Breaker 1B2 on MOV BD 1C fails open causing loss of control power used to close valve.	1×10^{-5}/hr	None	None	B	1	1,2
1 out of 2 twice reactor vessel high water level sensors LIS 203A, 203C, 208A 208C[c] fail open.	3×10^{-5}/hr (calibration shift)	None	None	B	3	1,2
Loss of control logic due to fuse 13A-F9 or F-10 failing open.	2×10^{-6}/hr	None	None	B	1	1,2
Loss of control air to turbine trip valve FCV 71-9. Valve fails open.	1×10^{-9}/hr (per 12 ft section)	None	None	B	2	1,2
*There appears to be a possible common mode failure between this system and other systems through failures within Control Air, Fire Protection, Heating, Ventilation and Air Conditioning and Electrical Power System.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[d]	TBD	TBD	1,2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. Safety grade switchboard, power supply and switches.

d. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Water Cleanup System
Failure Mode: Failure to Provide LetDown Flow When Required

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Blowdown valve PCV 69-15 closes due to pressure sensor PS 69-15A or B failure.	3×10^{-5}/hr	None	None	B	1	1
Hand controller HC 69-15 fails in "valve closed" mode.	3×10^{-5}/hr	None	None	B	2	1
Loss of control air will cause PCV 69-15 to close.	1 x 10-9/hr/12 ft	None	None	B	2	1
Solenoid valve controlling air to blowdown valve fails causing blowdown valve to close.	1×10^{-3}/d	None	None	B	1	1
*There appears to be a possible common mode failure between this system and other systems through failures within Control Air and Electrical Power Systems.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[c]	TBD	TBD	1

a. From Appendix C, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Core Standby Cooling Control and Instrument System
Failure Mode: HPCI System Fails to Shutdown Automatically

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Mechanical or hydraulic failure of the turbine trip valve FCV 73-18 to close.	1×10^{-3}/demand	None	None	B	1	1,2
1 out of 2 taken twice. Reactor high water level switches LIS 203B, 203D, 208B, 208D[c] fail open.	3×10^{-5}/hr for each	None	None	B	3	1,2
Wiring from the reactor high water level switches to the control relay logic fails open or shorts to ground.	1×10^{-6}/hr	None	None	B	1	1,2
1 out of 2 taken twice reactor water level sensors LIS 73-58A, 58B, 58C, 58D[c] fail low after reactor water level has increased above low level HPCI initiation.	3×10^{-5}/hr for each	None	None	B	3	1,2
Manual control switch for HPCI pump fails in the start condition preventing the pump from shutting down.	1×10^{-8}/hr	None	None	B	2	1,2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. Safety grade switches.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Core Standby Cooling Control and Instrument System
Failure Mode: HPCI Inadvertent Startup

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
1 out of 2 taken twice reactor low water level sensors, LIS 3-58 A, B, C, D[c] fail low.	Calibration shift 3×10^{-5}/hr for each	RCIC RHR CSS Diesel generators ADS	Starts RCIC Starts RHR Starts core spray Starts diesel generators ADS permissive	A	3	1,2
1 out of 2 taken twice containment high pressure sensors PS 54-58A, B, C, D[c] fail closed.	Calibration shift 3×10^{-5}/hr for each	RHR	Starts RHR	A	3	1,2
Wiring from reactor low water level sensors or containment high pressure sensors fail shorted to hot bus.	1×10^{-8}/hr for each	None	None	B	2	1,2
Switch contacts on manual switches HS 73-16C or XS 76-16 fail N.O. to N.C.	1×10^{-8}/hr for each	None	None	B	2	1,2
Mechanical or pneumatic failure open of turbine control valve causing inadvertent start of HPCI turbine.	1×10^{-8}/d	None	None	A	2	1,2
There appears to be a possible common mode failure between this system and other systems through failures within the Control Air, Fire Protection and Electrical Power systems.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[d]	TBD	TBD	1,2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. Safety grade switches.

d. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Manual Control and Control Rod Drive System
Failure Mode: Inadvertent Rod Withdrawal or Ejection

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Inadvertent rod withdrawal caused by:						
a. Switch SI-XX-XX(typ. of 183) contacts failing shorted; control timer contacts fail closed; relay K1, K2, K14, K15, K16or K32 contacts fail shorted, and switch 53 contacts fail shorted.	1×10^{-8}/hr for switches 1×10^{-8}/hr for relays 1×10^{-5} for timer	None	None	B	3	1
b. Hydraulic control valve S-40A and S-40B rupture or or inadvertently open.	1×10^{-8}/hr per valve	None	None	B	3	1
c. Relay KXA18-03, KXA22-03 contacts fail open; RSGS lamp dimmer fails dim, rod out indication lamp fails to indicate, rod worth minimizer fails, and rod sequence control systems fail.	1×10^{-8}/hr for relays 1×10^{-6}/hr for dimmer and lamps 1×10^{-6}/hr for systems	None	None	B	3	1
Single rod ejection caused by:						
a. Rod uncoupled, rod drive unit is driven to full withdrawn position and the stuck rod releases, ejecting to full out position.	1×10^{-6}/hr for spud failure, 1×10^{-6}/hr for stuck rod	None	None	B	3	1
b. Rod coupling (spud) failure; rod uncouples, both hydraulic control valves S40A, S40B rupture or fail to open position, and hydraulic pressure increases due to failure of valve 3-20 and stabilizer valves.	1×10^{-6}/hr for spud failure 1×10^{-8}/hr for valves	None	None	B	3	1
c. Uncoupled rod or mechanical failure of rod drive, reactor manual control system output logic fails, and hydraulic pressure increases due to failure in hydraulic supply.	1×10^{-6}/hr for coupling and logic, 1×10^{-8}/hr for valves	None	None	B	3	1

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

NOTE: All BWR reactor plants have an installed rod ejection restraining structure to help protect against possible rod ejection.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Condensate and Feedwater Control
Failure Mode: High Feedwater Flow Rate

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Startup bypass feedwater flow too high when bypass line level controller input signal LC3-53, X53-53, LM3-60 or PT3-61 fails high during startup or shutdown or	1×10^{-6}/hr	None	None	B	1	1,2
Level detector LT3-60 signal to bypass control fails low during startup or shutdown.	1×10^{-6}/hr	None	None	B	1	1,2
Feedwater pump running too fast and reactor at low pressure:						
a. Malfunction of the feedwater turbine governor.	1×10^{-6}/hr	None	None	B	1	1,2
b. Malfunction of the throttle valve or feedwater controller.	1×10^{-5}/hr	None	None	B	1	1,2
c. Reactor level controller fails in high demand setting.	1×10^{-6}/hr	None	None	B	1	1,2
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air and Electrical Distribution 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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Turbine Generator Control System
Failure Mode: Inadvertent Opening of Turbine Governor or Bypass Valve

Event Initiator Proucing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
EHC control valve output logic fails high causing control valves to open.	1×10^{-6}/hr	None	None	B	1	1,2
Control valves fail in the open position due to electro or pneumatic failure.	1×10^{-8}/hr	None	None	B	2	1,2
Handswitch HS-47 162 fails to the "Open Valves" condition.	1×10^{-8}/hr	None	None	B	2	1,2
EHC bypass valve output logic fails high causing valves to open.	1×10^{-6}/hr	None	None	B	1	1,2
Bypass valve(s) fails to the open position due to electro or pneumatic failure.	1×10^{-8}/hr	None	None	B	2	1,2
*There appears to be a possible common mode failure between this system and other systems through failures within Control Air and Electrical Distribution 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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Main Steam
Failure Mode: High Steam Flow

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
One or more pressure relief or safety valves open from setpoint drift.	1×10^{-5}/hr for each valve	None	None	B	1	1,2
ADS valves fail open due to failure of ADS control logic.	1×10^{-5}/hr	None	None	B	1	1,2
One or more pressure relief valves open from control switch failure.	1×10^{-8}/hr	None	None	B	2	1,2
One or more pressure relief valves fail open due to pilot operator valve failure.	1×10^{-5}/hr	None	None	B	1	1,2
*There appears to be a possible common mode failure between this system and other systems through failures within the Electrical Distribution system.	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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Main Steam
Failure Mode: Low Steam Flow to Auxiliary Loads

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Loss of steam supply to feedwater heater when one or more motor operated extraction steam supply valves closes (wiring shorted to power).	1×10^{-8}/hr per valve	None	None	B	2	2
One or more feedwater heater level controller output fails high causing extraction steam supply valves to close.	3×10^{-5}/hr per controller	None	None	B	1	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Electrical Distribution system.	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 E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Emergency Equipment Cooling Water System
Failure Mode: EECWS Provides Excessive Cooling Water Flow to RHR System

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Manual switch on EECWS pump C3 or D3 shorts causing pump(s) to start and MOV49 or MOV48 to open causing a flow path to the RHR service water system.	1×10^{-8}/hr per pump start, 1×10^{-8}/hr per MOV 1×10^{-8}/hr per RHRSWS manual switches	RHR service water system	Increased or inadvertent water flow from EECWS to RHR	B	3	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air and Electrical Distribution systems.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[c]	TBD	TBD	2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determinied.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Residual Heat Removal System
Failure Mode: Failure to Control Rate of Heat Removal

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
RHR system inadvertently actuated in Low Pressure Coolant Injection (LPCI) mode:						
a. Loss of offsite power and reactor pressure appears to be ≤ 450 psig causing LPCI injection valves to open.	5×10^{-2}/yr (8×10^{-6}/hr) for loss of power 1×10^{-8}/hr for switch	None	None	B	3	2
b. LPCI one-out-of-two taken twice logic fails.	1×10^{-6}/hr	None	None	B	3	2
c. High drywell pressure and reactor low pressure permissives fail.	1×10^{-8}/hr per switch	None	None	B	3	2
d. Reactor vessel low level switches LIS3-58A, LIS3-58B, LIS3-58C, LIS3-58D (one-out-of-two taken twice) fail.	3×10^{-5}/hr per switch (calibration shift)	HPCI, RHR, CSC, Diesel generators, arms the ADS	Systems are actuated by level switches	A	3	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air and Electrical Distribution system.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[c]	TBD	TBD	2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Residual Heat Removal Service Water System (RHRSW)
Failure Mode: Excessive Cooling Water Flow

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Event Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
RHRSW Pump A1 or A2 or B1 or B2 or C1 or C2 or D1 or D2 manual switch shorts causing one or more pumps to start in addition to RHRSW pumps that have been previously initiated.	1×10^{-8}/hr per pump starter failure	None	None	B	2	2
Flow control valve FCV 23-40, FCV 24-52, FCV 23-34 or FCV23-46 from RHR heat exchangers fail open due to valve failure, switch failure or controller failure.	1×10^{-7}/hr per control valve 1×10^{-8}/hr per per switch failure 1×10^{-7}/hr per controller failure	None	None	B	2	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Control Air and Electrical Distribution systems.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[c]	TBD	TBD	2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX D
BROWNS FERRY A-47 IE&C ANALYSES

System: Reactor Control Rod Drive System
Failure Mode: One or More Rods Insert While at Power

Event Initiator Producing Failure Mode	Failure Rate[a]	Failures in Other Systems Caused by Events Initiator	Effect of Failure in Other Systems(s)	Fault Effect Designations	Probability Category	Transient Category[b]
Insertion of rod(s) while at power:						
Insert drive valve SD-40A and insert exhaust valve SD-40D fail open. (Typical of 185 units)	1×10^{-8}/hr per valve	None	None	B	3	2
Rod selection relay K32 contacts fail closed and K16 relay contacts fail closed.	1×10^{-8}/hr per relay contact	None	None	B	3	2
Relay K32 and Switch S2 and rod worth minimizer permisive fails closed. (Typical of 185 units)	1×10^{-8}/hr per relay contact	None	None	B	3	2
*There appears to be a possible common mode failure between this system and other systems through failures within the Electrical Distribution system.	None assigned for this report	Not determined for this report, will be evaluated following computer model simulations	TBD[c]	TBD	TBD	2

a. From Appendix E, Table 1.

b. 1--overfill transient, 2--overcooling transient.

c. TBD = To Be Determined.

APPENDIX E

STATISTICAL ANALYSIS TABLES

APPENDIX E

STATISTICAL ANALYSIS TABLES

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) may 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 following calculations also identify any assumptions that had to be made regarding the mission time or the test interval if there was not a Technical Specification to cover component testing.

The following probability categories were assigned to the calculated unavailabilities:

From: 1 to 1×10^{-6} = Category 1

1×10^{-6} to 1×10^{-8} = Category 2

less than 1×10^{-8} = Category 3

It should be noted that these unavailabilities appear extremely low, however, they are calculations indicating the probability that a failure occurs during a given 1 hour period. The categories assigned to the different unavailabilities were arbitrarily assigned so that single active failures would be a Category 1 and multiple failures would be a Category 3.

RECIRCULATION PUMP FAILURE

1. Failure of Pumps to Continue to Run--given start case considered is failure of pump/motor unit, excluding control circuits (two conditions considered: Failure of 1 pump, failure of 2 pumps).

   Detection of failure is considered to be immediate but pump is not repairable.

   $\bar{a} = \lambda t$

   t = mission time = 1 hour

   $\bar{a} = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$ for 1 pump PC = 1

   $\bar{a} = (1 \times 10^{-5})(1 \times 10^{-5}) = 1 \times 10^{-10}$ for 2 pumps PC = 3

2. Trip of One Recirculation Pump--

   Generator field breaker fails open or inadvertently trips. Mode of failure is breaker-premature transfer (from Table G-1). Assumptions: nonrepairable event; mission time is 1 hour.

   $a = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$

   PC = 1

3. Trip of both recirculation MG sets. (Loss of auxiliary and startup transformers).

   Failure in transformers could be attributed to failure within the transformer (internal) or failure of the automatic breakers associated with the transformer.

The mode considered was failure of the automatic transfer breakers (from Table G-1, premature transfer = 1×10^{-5}/hr). It is assumed that the trip would be detected immediately but that only one transformer is required for operation.

Mission time = 1 hour

$\bar{a}$ = 1×10^{-5} per transformer

$\bar{A}$ = $(1 \times 10^{-5})(1 \times 10^{-5}) = 1 \times 10^{-10}$ for both transformers

PC = 3

4. <u>Same occurrence as 3 above</u>.

Loss of boosted cooling water and isolation valve MOV 24-738. Boosted raw water cooling system is supplied by raw water system. Combination of failure in boosted system plus closure of MOV 24-738 is required to fail both MG sets. Assumed same conditions as 2 and 3 above. System is operational, and required for cooling MG sets.

MOV--failure to remain open = 1×10^{-7}/hr

System--failure of pump to continue to run = 1×10^{-5}/hr

$\bar{a}_{1\,\text{pump}} = \lambda t = (1 \times 10^{-5}/\text{hr})(1\ \text{hr}) = 1 \times 10^{-5}$

$\bar{a}_{2\,\text{valve}} = \lambda t = (1 \times 10^{-7}/\text{hr})(1\ \text{hr}) = 1 \times 10^{-7}$

$\bar{A}$ = $(1 \times 10^{-5})(1 \times 10^{-7}) = 1 \times 10^{-12}$

PC = 3

5. Failure of master controller, to minimum speed demand.

Master controller causes run-back of both recirculation pumps to minimum speed. Failures in other auxiliary portions, that affect controller operation, could also fail, but failure considered is failure of the master controller. This failure ultimately would cause run-back of the recirculation pumps. It is assumed that run-back of recirculation pumps is immediately detected.

$$\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$$

PC = 1

6. Failure of suction or discharge valve to remain open.

$$\bar{a} = (4 \times 10^{-7}/hr)(1\ hr) = 4 \times 10^{-7}$$

PC = 2

7. Failure of one or more jet pumps.

Failure is assumed to be a flange failure of a jet pump pair.

$$\bar{a} = (20)(6 \times 10^{-6}/hr)(1\ hr) = 1.2 \times 10^{-4}$$

PC = 1

8. Recirculation pump motor/generator scoop tube failure, resulting in decreased speed of the recirculation pumps.

$$\bar{a} = (3 \times 10^{-7}/hr)(1\ hr) = 3 \times 10^{-7}$$

PC = 2

9. Recirculation pump motor/generator failure, due to failure of either the motor or the generator.

$$\bar{a} = (2)(1 \times 10^{-6}/hr)(1\ hr) = 2 \times 10^{-6}$$

PC = 1

NUCLEAR SYSTEM PRESSURE RELIEF SYSTEM

One or More Pressure Relief Valves Open

1. Wiring to Valve Actuator--shorted to power (control circuit).

   Considered failure of a single valve sufficient in severity to result in transient.

   Nonrepairable; mission time = 1 hour

   $\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for one valve

   PC = 2

2. Premature Opening of Valve--due to setpoint drift, detected immediately, 1 hour mission time

   $\bar{a} = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$

   PC = 1

3. Inadvertent opening--due to solenoid valve failure, detected immediately, 1 hour mission time.

   $\bar{a} = (1 \times 10^{-3}/d)(1\ demand) = 1 \times 10^{-3}$
   PC = 1

4. Inadvertent opening--due to mechanical failure of relief valve, detected immediately, 1 hour mission time.

   $\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$
   PC = 2

REACTOR CORE ISOLATION COOLING SYSTEM

RCIC Inadvertent Start

1. 1 out of 2 taken twice reactor water low level sensors fail low--Technical Specifications require that this instrumentation receive an instrument check one/day, however, a low level is alarmed. Combinations of faults are 58A and 58C, 58A and 58D, 58B and 58C, 58B and 58D. The failure mode is calibration shift and failure rate per sensor of 3×10^{-5}/hr. Given that a transient has already occurred and that RCIC initiation would make the transient worse, then the $\bar{A}$ is:

   $\bar{a} = \lambda t = (3 \times 10^{-5}/\text{hr})(1\ \text{hr}) = 3 \times 10^{-5}$ for one sensor

   $\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for both sensors

   $\bar{A} = 3 \times 10^{-9}$ for all fault combinations

   PC = 3

2. Logic Wiring to Relays--fault would be detected immediately. Given that a transient has already occurred and that RCIC initiation would make the transient worse, then the $\bar{A}$ is:

   $\bar{a} = (1 \times 10^{-8}/\text{hr})(1\ \text{hr}) = 1 \times 10^{-8}$

   PC = 2

3. Contacts Fail Closed--same as 2 above.

RCIC Fails to Shutdown Automatically

Basic assumption is that RCIC has successfully started and is now required to shutdown. Under this condition, RCIC is an operating system.

1. Loss of power bus--power bus could fail during time when RCIC is required and not be detected until RCIC shutdown is required. Assumed that RCIC is required to operate for 1 hour and no repair.

$$\bar{a} = \lambda t = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$$

$$PC = 1$$

2. <u>Loss of Breaker</u>--same as 1 above.

3. <u>Loss of High Level Switches</u>--1 of 2 twice must fail.

   Switches:

$$\bar{a} = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5} \text{ per switch}$$

$$\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10} \text{ for loss of both switches}$$

$$\bar{A} = 3 \times 10^{-9} \text{ for all combinations}$$

$$PC = 3$$

   Calibration shift used as most likely failure mode for high water level sensors. Instrument check once/day; however, there is a high level alarm.

4. <u>Fuses Fail Open</u>--there are 2 fuses. Conditions the same as 1 above.

$$\bar{a} = (1 \times 10^{-6}/hr)(2\ fuses)(1\ hr) = 2 \times 10^{-6}$$

$$PC = 1$$

5. Loss of control air, failure rate is for pipe rupture. Assumed 1200 feet of piping, no repair, and that control air could fail during the time that RCIC is required to operate.

$$\bar{A} = (1 \times 10^{-9}/\text{hr - 12 ft section})(100 - 12 \text{ ft sections})(1 \text{ hr})$$
$$= 1 \times 10^{-7}$$

PC = 2

However, there may be a solenoid valve in control air that could inadvertently closed which would have an $\bar{A}$ ranging from 10^{-6} to 10^{-8} depending on type of wire fault.

REACTOR WATER CLEANUP SYSTEM

Failure to Provide Letdown Flow When Required

1. Blow Down Valve Closes Due to PS-15A Indicating Low--it appears that the letdown valve is only used during startup, not during a high reactor water level transient. If the valve fails to open, startup procedures will be discontinued. Thus, the valve must have closed and remained closed for some period of time. Given that some transient has already occurred and the letdown valve should remain closed:

   $$\bar{a} = \lambda t = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5}$$

   PC = 1

2. Hand Controller HC 69-15 fails in valve closed mode.

   Same as 1 above, PC = 1.

3. Loss of Control Air--assuming 1200 ft. of piping, no repair, and a mission time of 1 hour.

   $$\bar{a} = (1 \times 10^{-9}/hr - 12\ ft\ section)(100 - 12\ ft\ section)(1\ hr)$$
   $$= 1 \times 10^{-7}$$

   PC = 2

   There may be a valve that could inadvertently close which would have an $\bar{A}$ of 2×10^{-5} to 2×10^{-7} depending on type of wire fault. For all cases it appears PC = 2.

4. Loss of Control Air, from solenoid valve failure causing closure of PCV 69-15.

   Using the same assumptions as under 1 above:

$\bar{a} = (3 \times 10^{-7}/hr)(1\ hr) = 3 \times 10^{-7}$

PC = 2

REACTOR RECIRCULATION SYSTEM HIGH FLOW

1. Failure of Master Controller to maximum pump speed.

   Master controller causes spontaneous acceleration of both recirculation pumps to maximum speed. Failures in other auxiliary portions, that affect controller operation could also fail, but the failure considered is a failure of the master controller. It is assumed that acceleration of the recirculation pump is immediately detected.

   $\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$
   PC = 1

2. Recirculation Pump Motor-Generator Scoop Tube Failure, resulting in increased pump speed.

   $\bar{a} = (3 \times 10^{-7}/hr)(1\ hr) = 3 \times 10^{-7}$
   PC = 2

CORE STANDBY COOLING CONTROL AND INSTRUMENTATION SYSTEM

HPCI Inadvertent Start

1. Reactor Low Water Level Sensors Fail--1 out of 2 taken twice reactor water low level sensors fail low--Technical Specifications require that this instrumentation receive an instrument check one/day, however, a low level is alarmed. Combinations of faults are 58A and 58C, 58A and 58D, 58B and 58C, 58B and 58D. The failure mode is calibration shift and failure rate per sensor of 3×10^{-5}/hr. Given that a transient has already occurred and that HPIC initiation would make the transient worse, then the $\bar{A}$ is:

   $\bar{a} = \lambda t = (3 \times 10^{-5}/\text{hr})(1 \text{ hr}) = 3 \times 10^{-5}$ for one sensor

   $\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for both sensors

   $\bar{A} = 3 \times 10^{-9}$ for all fault combinations

   PC = 3

2. Containment High Pressure Switches Fail--per the Technical Specifications, a functional test is performed once/month, calibration once/3 months, and no instrument check. Calibration shift would be detected during the functional test; however, there is a high pressure alarm.

   $\bar{a} = \lambda t = (3 \times 10^{-5}/\text{hr})(1 \text{ hr}) = 3 \times 10^{-5}$ for 1 sensor

   $\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for loss of 2 sensors

   $\bar{A} = 3 \times 10^{-9}$ for all combinations

   PC = 3

3. Reactor Low Level or Containment Pressure Wiring--wire faults for either level or pressure would be detected immediately. Given that a transient has already occurred and that inadvertent HPCI initiation would make the transient worse.

$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$

PC = 2

4. Either of Two Switch Contacts Fail--detected immediately. Given that a transient has already occurred and that inadvertent HPCI initiation would make the transient worse, then:

$\bar{a} = \lambda t = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ (for one switch)

$\bar{a} = 2 \times 10^{-8}$ (for 2 switches)

PC = 2

5. Turbine Control Valve Fails Open--causing spontaneous startup of HPCI turbine.

$\bar{a} = (1 \times 10^{-8}/d)(1\ demand) = 1 \times 10^{-8}$
PC = 2

HPCI Fails to Shutdown Automatically

1. Turbine Trip Valve Fails to Close--

$\bar{a} = (1 \times 10^{-3}/d)(1\ demand) = 1 \times 10^{-3}$

PC = 1

2. <u>Reactor Water High Level Switches</u>--1 of 2 twice must fail.

Switches:

$\bar{a} = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5}$ per switch

$\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for loss of both switches

$\bar{A} = 3 \times 10^{-9}$ for all combinations

PC = 3

Calibration shift used as most likely failure mode for high water level sensors. Instrument check once/day; however, there is a high level alarm.

3. <u>Reactor Water High Level Wiring Fault</u>--

$\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$

PC = 1

4. <u>Reactor Low Water Level Sensors Fail</u>--There is a low water level alarm. Calibration shift is assumed.

$\bar{a} = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5}$ per sensor

$\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for 1 combination

$\bar{A} = 3 \times 10^{-9}$ for all combinations

PC = 3

5. Manual Control Switch Fails in start mode thereby preventing the pump from shutting down.

$\bar{a} = (1 \times 10^{-8}/\text{hr})(1 \text{ hr}) = 1 \times 10^{-8}$
PC = 2

REACTOR MANUAL CONTROL AND CONTROL ROD DRIVE SYSTEMS

Inadvertent Rod Withdrawal

1. Switch SI contacts short and timer contacts short and relay (K1 + K2 + K4 + K15 + K16 + K32) contacts short and switch S3 contacts short.

   The relay contacts have the longest fault duration, these could short prior to startup. However, due to the number of faults that must occur the fault duration would have to be on the order of 10^{50} hours before the probability category would equal 10^{-4}.

2. Hydraulic Control Valves Rupture, (S-40A and S-40B) Open, or Fail Open.

   Wire/logic faults that would cause these valves to open would probably be more likely at 1×10^{-6}/hr per valve during low power operations than rupture at 1×10^{-8} /hr per valve. At normal power operations, inadvertent rod withdrawal should not be a concern due to Technical Specification requirements on reactivity limits. Premature transfer of a circuit breaker probably does not apply. Safe direction would be fully inserted on loss of power so it would appear that these valves do not fail open. Control valve faults would only be a problem during startup or shutdown and this is still questionable since the Rod Worth Minimizer and Rod Sequence Control Systems must be operational.

   Assuming that a transient has already occurred, then the $\bar{A}$ is:

   $\bar{a} = (1 \times 10^{-6}/\text{hr})(1 \text{ hr}) = 1 \times 10^{-6}$ per valve

   $\bar{A} = 1 \times 10^{-12}$ for both valves

   PC = 3

3. Below 20% power, the RSCS is required per Technical Specifications to be operable. Below 20% power the RWM should be operable or a second operator must verify that the console operator is following the control rod program. If the above Technical Specification requirements cannot be met, shutdown is required immediately.

<u>Single Rod Ejection</u>

1. For each control rod during startup check:

$$\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6} \text{ for one failure}$$

$$\bar{A} = (1 \times 10^{-6})(1 \times 10^{-6}) = 1 \times 10^{-12} \text{ for both failures}$$

The above assumes 1 hour for check of each control rod which is overly conservative but easier to work with. There are 185 control rods.

$$\bar{A} = (1 \times 10^{-12})(185) = 2 \times 10^{-10}$$

$$PC = 3$$

2,3. The rod ejection restraining structure should limit the rod travel to 3/4-1". Given that a transient has already occurred and that the single rod ejection is an additional fault, that 1×10^{-8}/hr applies to all valves (valves can only rupture or have a wiring short to power) and that there are two stabilizer valves.

$$\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6} \text{ for speed failure}$$

$$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8} \text{ for valves 540A, 540B, 3-20 and stabilizer valves}$$

$$\bar{A} = \underset{\text{speed}}{(1 \times 10^{-6})}\underset{\text{540A}}{(1 \times 10^{-8})}\underset{\text{540B}}{(1 \times 10^{-8})}\underset{\text{3-20}}{(1 \times 10^{-8})}\underset{\text{STAB-1}}{(1 \times 10^{-8})}\underset{\text{STAB-2}}{(1 \times 10^{-8})} = \text{negligible}$$

PC = 3

In the second case, the logic would be common to all control rods.

$$\bar{a} = \underset{\text{logic}}{(1 \times 10^{-6})}\underset{\text{coupling}}{(1 \times 10^{-6})}\underset{\text{CR}}{(185)}\underset{\text{540A}}{(1 \times 10^{-8})}\underset{\text{CR}}{(185)}\underset{\text{540B}}{(1 \times 10^{-8})}\underset{\text{CR}}{(185)}$$

$\bar{a}$ = negligible

PC = 3

CONDENSATE AND FEEDWATER CONTROL SYSTEM

<u>High Feedwater Flow Rate</u>

1. <u>Startup Bypass Feedwater Flow</u>--too high

   a. Line level controller input signal fails high for consideration of fault only during startup and shutdown, assuming that the transient has occurred.

   Then:

   $$\bar{A} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$$

   $$PC = 1$$

   b. Detector signal, fails low same as a.

2. <u>One Feedwater Pump</u>--running too fast, detection is assumed to be immediate:

   a. $\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$

   $PC = 1$

   b. Same as a.

3. <u>All Feedwater Pumps Running Fast</u>--

   Reactor level controller fails in high demand setting. Assuming that analysis sheet is correct as stated, one common reactor level controller, failing in high demand can cause inadvertent speed-up of all feedwater pumps.

$\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$

PC = 1

$\bar{a} = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5}$ 1 sensor

$\bar{A} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for 2 sensors

$\bar{A} = 3 \times 10^{-9}$ for all combinations

PC = 3

TURBINE GENERATOR CONTROL SYSTEM

Turbine Generator Control Valves (TGCVs) Inadvertently Open

Basic assumption is that TGCVs inadvertently opened when turbine is not available, such as during startup or after a turbine trip given that the TGCVs successfully closed. A mission time of 24 hours was used for startup. For the TGCVs this is somewhat conservative. A 1 hour mission time was used for the case where the TGCVs open after a successful turbine trip.

1. EHC Logic Fails High--Given that a transient has already occurred, that the TGCVs inadvertently opening would make the transient worse, no repair, and a mission time of 1 hour, the $\bar{A}$ is:

$$\bar{a} = \lambda t = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$$

$$PC = 1$$

2. TGCVs Fail in Open Position--the failure mode would be a wire fault that would cause one or more valves to inadvertently open. The wire fault failure rate would be 1×10^{-8}/hr. Thus, 2 should reflect the correct wire fault with PC = 2.

3. Handswitch Fails--Same as 2 above. This should reflect the correct wire/contact fault with PC = 2.

Turbine Bypass Valves (TBVs) Inadvertently Open

Basic Assumption is that turbine is available, but that the TBVs inadvertently open.

1. EHC Logic Fails High--Given that a transient has already occurred, that inadvertent opening of a TBV would make the transient worse, no repair, and a mission time of 1 hour; then the $\bar{A}$ is:

$$\bar{a} = \lambda t = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$$

PC = 1

2. Bypass Valves Fail to Open Position--The failure mode would be a wire fault that would cause one or more TBVs to open. A wire fault failure rate is 1×10^{-8}/hr. This present failure mode should reflect the correct wire fault with PC = 2.

Turbine Bypass Valves (TBVs) Fail Open (Fail to Close)

Basic assumption is that TBVs are required to close. This may occur after a turbine trip given that the TBVs have successfully opened and are now required to close or during a startup. A mission time of 24 hours was used for startup which is conservative with respect to the TBVs.

1. EHC Output Logic Fails High--given that a transient has occurred, that a turbine trip was either the transient initiator or occurred as a result of the transient, that failure of the TBVs will make the transient worse, no repair and a 1 hour mission time, then the $\bar{A}$ is:

$$\bar{a} = \lambda t = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$$

PC = 1

2. Bypass Valves Fail in Open Position--Assumption is that failure of any one TBV to close is failure to stop TBV operation.

$$\bar{a} = 1 \times 10^{-3}/D \text{ per valve}$$

$$\bar{a} = 9 \times 10^{-3} \text{ for failure of any 1 of 9 TBVs to close}$$

PC = 1

MAIN STEAM SYSTEM

High Steam Flow

1. One or More Pressure Relief Valves Open from setpoint drift--Browns Ferry plant utilizes 13, Target Rock, 2 stage, pilot operated, combination safety-relief valves. Failure rate for inadvertent opening (premature opening) of a code safety or relief valve is 1×10^{-5}/hr. The valves themselves have no associated control system (for safety code application). In a BWR plant application, there is no access during operation for repair. Assumed nonrepairable and 1 hour mission. Opening of a single valve can initiate the transient.

   $\bar{a} = \lambda t = (1 \times 10^{-5}/hr)(1\ hr)(13\ valves) = 1 \times 10^{-4}$

   PC = 1

2. Automatic Depressurization System (ADS) Valves fail open due to control logic failure.

   $\bar{a} = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$
   PC = 1

3. Controllable Pressure Relief Valve Fails Open due to switch failure.

   $\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$
   PC = 2

4. Pressure Relief Valve Fails Open due to pilot operator failure.

   $\bar{a} = (1 \times 10^{-5}/hr)(1\ hr) = 1 \times 10^{-5}$
   PC = 1

Low Steam Flow to Auxiliary Loads

1. One or more Motor Operated Extractor Steam Supply Valves Close--

   Conditions assumed as stated on analysis sheet: Loss of steam supply to one feedwater heater is limiting condition, sufficient to initiate transient.

   Wiring shorted to power. Nonrepairable. Mission time = 1 hour.

   For control circuit

   1×10^{-8}/hr

   $\bar{a} = (1 \times 10^{-8}/\text{hr})(1 \text{ hr}) = 1 \times 10^{-8}$

   PC = 2

2. One feedwater heater level controller output fails high.

   Same as 1 except assumed calibration shift as fault condition.

   $\bar{a} = (3 \times 10^{-5}/\text{hr})(1 \text{ hr}) = 3 \times 10^{-5}$

   PC = 1

EECWS PROVIDES EXCESSIVE COOLING WATER FLOW TO RHR

1. Manual switch shorts on EECWS pump(s) and a motor operated valve (MOV) inadvertently opens are the most likely faults if it is assumed that RHR Service Water has already been required (i.e., is already in service). Assuming a one hour mission time and no repair:

$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for manual switch short or MOV

$\bar{A} = (1 \times 10^{-8})(1 \times 10^{-8}) = 1 \times 10^{-16}$ for both switch and MOV

PC = 3

RHR FAILURE TO CONTROL RATE OF HEAT REMOVAL

1. Given that a transient has already occurred, that inadvertent RHR initiation will make the transient worse, a one hour mission time, and no repair, then the unavailability is:

   $\bar{a} = (8 \times 10^{-6}/hr)(1\ hr) = 8 \times 10^{-6}$ for LOSP

   $\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for pressure switch

   $\bar{A} = (8 \times 10^{-6})\ (1 \times 10^{-8}) = 8 \times 10^{-14}$ No calibration shift because pressure instrument is 1 out of 2 twice. Switch fault is more likely.

   PC = 3

   In reality, the probability may be even less likely due to the fact that the valves cannot physically open even if an open signal is present because the pressure is too high.

2. <u>Low Pressure Coolant Injection (LPCI) Logic</u>--given the same assumptions as above

   $\bar{a} = (1 \times 10^{-6}/hr)(1\ hr) = 1 \times 10^{-6}$ for one logic unit

   $\bar{A} = (1 \times 10^{-6})(1 \times 10^{-6}) = 1 \times 10^{-12}$ for failures of 2 units

   $\bar{A} = (1 \times 10^{-12})$ 4 combinations $= 4 \times 10^{-12}$

   PC = 3

3. High Drywell and Reactor Pressure--given the same assumptions as above:

$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for drywell switch

$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for reactor pressure switch

$\bar{A} = (1 \times 10^{-8})(1 \times 10^{-8}) = 1 \times 10^{-16}$ for failure of both

PC = 3

4. Reactor Vessel Low Level Switches--given the same assumptions as above:

$\bar{a} = (3 \times 10^{-5}/hr)(1\ hr) = 3 \times 10^{-5}$ for one level instrument

$\bar{a} = (3 \times 10^{-5})(3 \times 10^{-5}) = 9 \times 10^{-10}$ for failure of 2 instruments

$\bar{A} = (9 \times 10^{-10})(4\ \text{combinations}) = 4 \times 10^{-9}$

PC = 3

RHRSW PROVIDES EXCESSIVE COOLING WATER FLOW

1. Manual Switch Shorts--given that a transient has already occurred and that excessive cooling will make the transient worse, a one hour mission time and no repair.

$$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$$

PC = 2

2. Flow Control Valve Fails Open--given same conditions as above.

$$\bar{a} = (1 \times 10^{-7}/hr)(1\ hr) = 1 \times 10^{-7}$$

PC = 2

INSERTION OF RODS WHILE AT POWER

1. <u>Drive and Exhaust Valves Fail</u>--given that a transient has already occurred, that scram would make the transient worse, a one hour mission time, and no repair:

$\bar{a} = (1 \times 10^{-8}/hr)(1\ hr) = 1 \times 10^{-8}$ for each valve

$\bar{a} = (1 \times 10^{-8})(1 \times 10^{-8}) = 1 \times 10^{-16}$ for both valves

$\bar{A} = (1 \times 10^{-16})$ (185 valve sets) $= 2 \times 10^{-14}$ for 185 sets of valves

PC = 3

2. Given that the same conditions as 1 above apply, then the unavailability value is the same. PC = 3.

3. Since three items must fail versus the two items discussed above, and given that the same conditions as 1 above apply, then the set of faults will be even less likely than 1 above. PC = 3.

TABLE E-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 E-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-8/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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 E-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 squure 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. Commercial 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-2802, 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. McClymont, A. S., and Poehlman, B. W., ATSW: A reappraisal; Part 3: Frequency of Anticipated Transients, EPRI NP-2230, 1982.

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

APPENDIX F

OVERFILL AND OVERCOOLING POSTULATED TRANSIENT SCENARIOS

APPENDIX F

SCENARIOS SECTION

1. INTRODUCTION

This phase of the overfill and 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 Browns Ferry 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 OVERFILL ACCIDENT

3.1 Browns Ferry Licensing (FSAR) Accident Analysis

Main Steam Line Break Accident: The reactor is assumed to be at design power with vessel level and pressure normal for the initial conditions. The steam pipe is assumed to be instantly severed by a circumferential break. The break is physically arranged so that coolant discharge through the break is unobstructed. These assumptions result in the fastest depressurization rate of the nuclear system.

The steam flow through both ends of the break increases to the value limited by critical flow considerations. The flow from the upstream side of the break is limited initially by the main steam line flow restrictor. The flow from the downstream side of the break is limited initially by the

downstream break area. The decrease in steam pressure at the turbine inlet initiates closure of the main steam line isolation valves within about 200 milliseconds after the break occurs. Also, main steam line isolation valve closure signals are generated as the differential pressures across the main steam line flow restrictors increase above isolation setpoints. The instruments sensing flow restrictor differential pressures generate isolation signals within about 500 milliseconds after the break occurs.

A reactor scram is initiated as the main stream line isolation valves begin to close. In addition to the scram initiated from main steam line isolation valve closure, voids generated in the moderator during depressurization contribute significant negative reactivity to the core even before the scram is complete. Because the main steam line flow restrictors are sized for the main steam line break accident, reactor vessel water level remains above the top of the fuel throughout the transient.

The steam flow rate through the upstream side of the break increases from the initial value of 1000 lb/sec in the line to 2000 lb/sec (about 200% of rated flow for one steam line) with critical flow initially occurring at the flow restrictor. The steam flow rate was calculated using an ideal nozzle model. Tests conducted on a scale model over a variety of pressure, temperature, and moisture conditions have been used to substantiate the flow models capability to predict the steam flow behavior in the presence of a flow restrictor.

The steam flow rate through the downstream side of the break consists of equal flow components from each of the unbroken lines. The pipe resistance and local restrictions in the unbroken lines result in critical flow initially occurring at the downstream side break location. The steam flow rate in each of the unbroken lines increases from an initial value of 1000 lb/sec to 1530 lb/sec.

The total steam flow rate leaving the vessel is approximately 6600 lb/sec, which is in excess of the steam generation rate of

4000 lb/sec. The steam flow-steam generation mismatch causes an initial depressurization of the reactor vessel at a rate of 35 psi/sec. The formation of bubbles in the reactor vessel water causes a rapid rise in the water level. The analytical mode causes a rapid rise in the water level. Thus, the water level reaches the vessel steam nozzles at 2 to 3 seconds after the break. From that time on a two-phase mixture is discharged from the break. The two-phase flow rates are determined by vessel pressure and mixture enthalpy. The vessel depressurization is calculated using a digital computer code in which the reactor vessel is modeled as five major nodes. The model includes the flow resistance between nodes, as well as heat addition from the core.

Two-phase flow is discharged through the break at an almost constant rate until late in the transient. This is the result of not taking credit for the effect of valve closure on flow rate until isolation valves are far enough closed to establish critical flow at the valve locations. The slight decrease in discharge flow rate is caused by depressurization inside the reactor vessel. The linear decrease in discharge flow rate at the end of the transient is the result of the assumption regarding the effect of valve closure on flow rate after critical flow is established at the valve location.

The following total masses of steam and liquid are discharged through the break-prior to isolation valve closure:

Steam	25,000 pounds
Liquid	160,000 pounds

Analysis of fuel conditions reveals that no fuel rod perforations due to high temperature occur during the depressurization, even with the conservative assumptions regarding the operation of the recirculation and feedwater systems. MCHFR remains above 1.0 at all times during the transient. No fuel rod failures due to mechanical loading during the depressurization occur because the differential pressures resulting from the transient do not exceed the the designed mechanical strength of the core assembly.

After the main steam line isolation valves close (10.5 sec), depressurization stops and natural convection is established through the reactor core. No fuel cladding perforation occurs even if the stored thermal energy in the fuel were simply redistributed while natural convection is being established; cladding temperature would be about 1000°F, well below the temperatures at which cladding can fail. Thus, it is concluded that even for a 10.5 second main steam line isolation valve closure, fuel rod perforations due to high temperature do not occur. For shorter valve closure times, the accident is less severe. After the main steam line isolation valves are closed, the reactor can be cooled by operation of any of the normal or standby cooling systems. Since the MCHFR never drops below 1.0, the core is always cooled by very effective nucleate boiling.

3.2 Sequence of Events

Initial conditions: 100% design power with reactor vessel level and pressure normal for the initial conditions.

Event	Time (Seconds)
100% operation steady-state.	0
Steam line ruptures, auxiliary a-c power is lost, recirculation pumps and feedwater pumps are tripped.	10
Reactor trip is initiated due to the loss of steam pressure at the turbine.	10.2
Main steam isolation valves start to close from signal generated across the flow restrictor nozzle.	10.5
Water enters the main steam lines as a steam-water mixture due to excessive swell due to void formations.	11.5
Feedwater flow is terminated as turbine-driven feedwater pumps stop.	14
Main steam isolation valves close and the overfill accident is terminated.	20.5

4. POSTULATED MORE SEVERE ACCIDENT

Through the course of this study there have been no failures of control grade systems or components identified that could create a more severe accident or aggravate the documented accident. It is terminated by safety grade components and systems which would have to sustain multiple failures to preclude termination of the accident.

Multiple failures of safety grade components and systems is beyond the scope of this task.

5. SEQUENCE OF EVENTS FOR OVERFILL TRANSIENT

5.1 Browns Ferry Licensing (FSAR) Transient Analysis

Failure of the feedwater flow controller in the maximum demand (115% flow) mode.

The transient was initiated from the low end of the analytical automatic flow control range (68% rated power) producing a more severe steam/feed flow mismatch and level transient than would be produced at higher power. The feedwater pumps were assumed to accelerate to their maximum capability of 115% of rated flow.

Sensed and actual water level increase during the initial part of the transient at about 4.0 inches/second. The high water level main turbine trip and feedwater turbine trip was initiated at 5 seconds when sensed level had increased about 19-21 inches preventing excessive carry-over from damaging the turbines. Scram occurs simultaneously with the turbine trip, limiting the neutron flux peak and fuel thermal transient so that no fuel damage occurs.

The turbine bypass system opens to limit the pressure rise. The lower set relief valves open only momentarily and no excessive overpressure of

the nuclear system process barrier occurs. The bypass valves close at about 24 seconds, bringing the pressure in the vessel under control during reactor shutdown.

Although lower initial power conditions would result in more rapid increases in level, this case represents the maximum thre.t to fuel clad and nuclear system process barriers. Obviously, no power transient will occur if the reactor is shut down.

5.2 Sequence of Events

Initial conditions: 68% rated power reactor feedwater system in automatic.

Event	Time (second)
68% rated power	0
Feed pump accelerates to 115% of rated flow	10
High level trip setpoint	15
Main turbine trips	
Feedwater turbine trips	
Reactor scram	
Main turbine bypass valve(s) open	

6. POSTULATED MORE SEVERE TRANSIENT

The same initial conditions will be assumed. 68% rated power, feedwater system in automatic. As indicated in Appendix D and Appendix E, there is a relatively high probability of failure for the selected level instrument and it is assumed to be the initiating event.

This failure is assumed to result in an indicated low level and corresponding increase in feed flow rate to 100% or greater.

The result of this initiating event is assumed to be a reactor water level increase of approximately 3.0 inches/sec or greater. If an aggravating failure of a second reactor level circuit is assumed, the main turbine and feed pump turbine high level trips will be disabled (2 out of 3 high levels required for trips).

Based on these assumptions it can be postulated that in approximately 32 seconds water will reach the main steam line nozzles and begin to enter the steam lines. (Assumed initial level of 561 inches and main steam line nozzles at 658 inches).

6.1 Sequence of Events

Initial conditions: 68% rated power reactor feedwater system in automatic normal reactor vessel water level 561 inches.

Event	Time (second)
68% operation	0
Selected level circuit fails low feed pump accelerates to 100% or greater	10
High level trip setpoint reached 2 out of 3 level trip fails low	15
Water reaches main steam line nozzles at 658" level	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 reactor water level 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 loss of power bus or a seismic event could cause failure of two or more level circuits.

Additional failures which were identified as potential initiators or aggravators were considered to be bounded by the postulated more severe transient scenario. For example, inadvertent HPCI and/or RCIC initiation could be assumed, but redundant safety grade high level switches are installed to terminate flow from these sources. See Table F-1 for a complete listing of additional failures.

6.3 Conclusions

Although defining the actual consequences of an overfill transient are 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 the high pressure coolant injection (HPCI) turbine might be disabled, main steam isolation valves and safety relief valve(s) could be damaged due to thermal stresses or water loadings.

Operator action might be postulated to terminate the transient or limit the consequences by manually tripping the feed pump and/or reactor and/or the main turbine. 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. 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 F-1. OVERFILL POSTULATED AGGRAVATING FAILURES

System	Ranking	Postulated Effects
Recirculation pumps (low flow) *(C.M.F. 1)	B1	Could cause level swell and slightly faster level rise
Reactor water cleanup system (letdown failure) *(C.M.F. 1,2)	B1	Disables letdown path (not normally used)
Control rod drive system (rod withdrawal) *(C.M.F. 1,2,4)	B3	Rod withdrawal--increase in reactor power
Main steam system (relief or safety open) *(C.M.F. 1,2)	B1	Could cause level swell and slightly faster level rise
Turbine generator system (power increase) *(C.M.F. 1,2,4)	B1	Could cause level swell and slightly faster level rise
Turbine bypass system (inadvertent open) *(C.M.F. 1,2,4)	B1	Could cause level swell and slightly faster level rise
HPCI RCIC RHR CSS system (inadvertent start) *(C.M.F. 1,2,3,4)	A3	Could cause faster level rise

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

7. SEQUENCE OF EVENTS FOR OVERCOOLING ACCIDENT

7.1 Browns Ferry Licensing (FSAR) Accident Analysis

There is no identified design basis accident for the overcooling event in the Browns Ferry FSAR.

8. POSTULATED MORE SEVERE ACCIDENT

During the course of this study there has been no control grade component or system identified whose operation or failure either singularly or in combination with or without safety grade components or systems that could result in a design basis accident for an overcooling event.

9. SEQUENCE OF EVENTS FOR OVERCOOLING TRANSIENT

9.1 Browns Ferry 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 vessel or reduce the temperature of water being delivered to the vessel. The event that results in the most severe transient in this category is the loss of feedwater heater.

A feedwater heater can be lost if the steam extraction line to the heater is shut, the heat supply to the heater is removed, producing a gradual cooling of the feedwater. The reactor vessel receives cooler feedwater which produces an increase in core inlet subcooling. Due to the negative void reactivity coefficient, an increase in core power results. The loss of 100°F of the feedwater heating capability represents the maximum heat loss expected by a single heater (or group of heaters) which can be tripped or bypassed by a single event. The reactor is assumed to be at design power conditions on automatic recirculation flow control when the heater is lost. For this analyzed case, the feedwater flow delay time of approximately 25 seconds between the heaters and the feedwater sparger is neglected. The plant would contihue at steady-state conditions during this

delay period. The recirculation flow control system responds to the power increase by reducing core flow so that steam flow from the reactor vessel to the turbine remains essentially constant through the transient. Neutron flux increases above the initial value to produce turbine design steam flow with the higher inlet subcooling. Normally the reactor would be on the manual flow control, and this neutron flux increase would have reached within 1% of the scram setting. In the case with automatic control, reactor power settles out slightly below the scram setting, but with core flow reduced to about 90%. The average power range monitors provide an alarm to the operator at about 20 seconds after the cooler feedwater reaches the reactor vessel. Because nuclear system pressure remains essentially constant during this transient, the nuclear system process barrier is not threatened by high internal pressure. All fuel parameters remain below the limiting values at which fuel damage could occur.

This transient is less severe from lower power levels for two main reasons: (a) lower initial power levels will have initial fuel parameter values less limiting than the values assumed here; and (b) the magnitude of the power rise decreases with the initial power condition. Therefore, transients from other reactor operating states or lower power levels within operating state F will be less severe.

9.2. Sequence of Events

Initial conditions: 100% design power reactor recirculation system in automatic.

Event	Time (Seconds)
100% operation	0
Feedwater heater(s) is loss and feedwater temperature decreases 100°F.	10
Recirculation flow decreases to compensate for the power increase and thus maintain steam pressure to the turbine-generator constant.	
Average power range monitors alarm to inform the operator of the transient.	30

10. POSTULATED MORE SEVERE TRANSIENT

The same initial conditions will be assumed.

100% design power; reactor recirculation system in automatic control.

The initiating event for this transient will be an inadvertent startup of the High Pressure Coolant Injection (HPCI) pump. This is further aggravated by the loss of one feedwater heater string. The subsequent heat loss to the reactor vessel appears to be capable of exceeding the previously analyzed transient. As the colder water enters the reactor vessel the power should commence increasing and recirculation flow should decrease to maintain steam pressure constant at the turbine-generator.

10.1 Sequence of Events

Initial Conditions: 100% design power; recirculation flow in automatic

Event	Time (Seconds)
100% operation	0
Inadvertent HPCI startup with simultaneous loss of feedwater heater string causing an overall cooling of the reactor vessel water in excess of 100°F.	10
Recirculation flow decreases to maintain steam pressure constant at the inlet to the turbine-generator.	
Average power range monitors alarm to inform the operator of the power increase	a

a. Time to be supplied by computer model.

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 nonsafety 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 core 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 F-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 significant efforts to run computer models and 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. 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 F-2. OVERCOOLING POSTULATED AGGRAVATING FAILURES

Failure System/Component	Failure Mode	Ranking	Postulated Effect
Reactor Core Isolation Cooling System *(C.M.F. 1,2,3,4)	Failure to shutdown automatically	A-2	Continued flow of relatively cold water to the reactor vessel causing excessive cooldown rate.
	Inadvertent startup when not required	B-2	Produces a supply of cold water to be pumped into the reactor vessel.
Primary Overpressure Protection System *(C.M.F. 1,2)	Inadvertent opening of a relief or safety valve	B-1	Causes an increased steam flow from the reactor vessel and additional cooldown of the primary water.
Reactor Recirculation Flow System *(C.M.F. 1)	Flow controller fails in the high flow mode	B-1	Causes increased recirculation flow and higher heat transfer rate and therefore a cooling transient to the bulk of the coolant.
Core Standby Cooling Control and Instrumentation System *(C.M.F. 1,2,3,4)	Failure of High Pressure Coolant Injection (HPCI) system to shutdown automatically	B-1	Continued high flow rate of relatively cold water to the reactor vessel may result in an excessive cooldown rate.
	Inadvertent startup of HPCI system when not required	B-2	Provides a high volume source of relatively cold water to the reactor vessel.

TABLE F-2. (continued)

System/Component	Failure Mode	Failure Ranking	Postulated Effect
Feedwater Control System *(C.M.F. 1,3,4)	High feedwater flow rate and failure to shutdown on high level	B-1	High feedwater flows at low power will cause a cooling transient.
Electro-Hydraulic Control System (EHC) *(C.M.F. 1,2,4)	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. 1,2,3,4)	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. 1,2,3,4)	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, 2--Control and Service Air, 3--Heating, Ventilation and Air Conditioning, 4--Fire Protection.

APPENDIX G

DOCUMENTED OVERFILL AND OVERCOOLING TRANSIENTS

APPENDIX G

DOCUMENTED OVERFILL AND OVERCOOLING TRANSIENTS

The following transients have been quoted from the referenced volumes of the Nuclear Power Experiences.[1] These excerpts are copyrighted and permission to use them has been received from NPE[1] for this report.

1. OVERFILL TRANSIENTS

Nuclear Power Experiences
Vol. BWR-2
IX. Instr. & Cont.
F. Process Syst.
p. 1, 2 and 3

3. LEVEL RECORDER PEN STICKS - PARTIAL BLOWDOWN CABLE DAMAGE

Dresden 2 - June 70 (power escalation testing)

The reactor was at 75% power when a spurious signal from the electrohydraulic control of the turbine caused the turbine-control valve to open from 75% to the load-reference setting of 80% and all the turbine-bypass valves to open (115% of rated flow). The turbine then tripped and caused a reactor scram. At time 3 sec the pressure-vessel water-level monitors tripped because of steam-bubble collapse. The resulting increase in feedwater (FW) flow cause the 2 operating FW pumps to trip off due to low suction pressure. At time 7 sec one feedwater pump restarted automatically but delivered water at a varying rate, apparently due to suction-pressure variations.

At 22 sec the turbine-bypass valves closed, apparently due to disappearance of the spurious signal. At 33 sec the main steam-line valves closed automatically due to low pressure (<850 psig) in the pressure vessel. At this time the water level in the pressure vessel was varying over a wide range owing to the pressure changes and FW cooling influencing both the

void volume and water volume. At about 50 sec, the water level was rising again, but the level-indicator chart pen being observed by the operator stuck. Not knowing that the level was still increasing, the operator switched the FW control to manual and further increased the flow rate. Before it was discovered that the pen was stuck, the water level had risen enough to flood the main steam lines and the isolation-condenser steam line. At 1 min and 30 sec, the stuck pen was discovered (by tapping the case) and the FW flow was reduced to minimum but could not be reduced to zero owing to leakage past the valves.

The continued input of water coupled with after-heat from the reactor core and closure of the main steam line valves caused the pressure to begin increasing rapidly. The isolation-condenser system was actuated manually, but it was shut off immediately due to a too-low trip setting of the condensate-return-line flow required by an erroneous Tech Spec. (This error had already been discovered, and steps were being taken to correct the trip-setting requirements.) The fact that the condenser was not operating was not discovered until several mins later. An attempt to reopen the main-steam-line valves to dump steam through the turbine-bypass valves failed because the valves had not been reset from the earlier trip that had closed them. When the reactor pressure reached 1050 psig at 3 min and 45 sec, the operator manually opened an electromatic pressure relief valve to dump steam to the pressure-suppression pool until the pressure fell to 960 psig at 5 min and 38 sec. This action had to be repeated at 6 min. At 6 min and 3 sec, a 2 psig dry-well pressure initiated an ECCS start, isolated the reactor-building ventilation, and actuated the standby gas-treatment system. This was followed by automatic tripping of the recirculation pumps and automatic startup of the standby diesel generators. The low pressure spray and LPCI systems started but did not inject because the reactor pressure exceeded the pump head of both systems. The HPCI system started but did not inject, because it had been valved out earlier for repairs after proof-testing its backup systems as provided for in the Tech Specs. Actual injection by this system would have been automatically inhibited by the high-water signal from the pressure vessel water level monitors.

Intermittent manual opening of relief valves controlled the reactor-vessel pressure between 840 and 1097 psig until the isolation condenser was reset and manually actuated at about 9 min and 45 sec and was operated for 5 to 15 min before being intentionally isolated by the operator. An area survery showed no radioactivity outside the containment system.

At 13 min and 8 sec, erratic signals started from the reactor power instrumentation and indicated steam or water damage to cables or connections in the drywell. By 30 min the operating FW pump had been tripped manually, and the water level was being held by the ~60 gpm provided by the CRD pumps. The reactor-vessel pressure was decreasing without intentional venting owing to leakage through safety valves, which apparently had opened at about the time the first pressure-relief valve was operated. The temperatures within the drywell were checked at this time on the local recorder. The highest temperature at the moment was 205°F, but the recorder had run out of paper, so that the temperature history during the incident was lost. The pressure in the drywell was still above 5 psig, but the actual value was not known because the high-range pressure monitor was out of service. To reduce the dry-well pressure, the operator opened a 2 in. line to the standby gas-treatment system. The stack off-gas radioactivity increased from 10,000 to 25,000 Ci/sec over a period of about 1/2 hr and then subsided.

At time 1 hr and 15 min, the reactor-vessel pressure was down to 200 psig, and the water level was under control. The main-steam-line valves had been opened, and the vessel was being vented through the turbine-bypass valves to the main condenser. The pressure in the drywell was still above 5 psig, so 5 of the 7 dry-well cooling units were put into service. By time 2 hr the dry-well pressure was down to 2.2 psig and could be monitored by the low-pressure monitor that was in service.

Radiation surveys showed that no significant release to the environment had occurred. Samples taken in the dry well indicated about 100 times the MPC of I-131 (82 times the next day). Operations and radiation-protection personnel equipped with air packs entered the drywell the next day to make a radiation survey and to obtain Staplex air samples. The radiation level

was about 1 R/hr. They observed water cascading from the upper part of the dry well from the vicinity of one of the main steam lines on which were mounted an electromatic relief valve and 2 safety valves.

Since the radioiodine level in the dry well was not falling rapidly enough, flow to the standby gas-treatment system was increased and allowed to draw air from the building as a sweep through the dry well. By 2 days after the incident, personnel were able to enter the dry well for a preliminary damage inspection. Two safety valves on one main steam line were being held slightly open by the positions of their operating handles, which had apparently been struck by the jet from a 3rd safety valve mounted on an adjacent main steam line.

Damage was confined to equipment within the drywell and was caused by the steam and water discharged through the safety valves. A total of about 30 ft of thermal insulation needed replacement on one main steam line, a feedwater riser, and a recirculation riser. Low resistance was found in 5 valve motors, a floor drain pump motor, and a dry-well-cooling blower motor. Seven dry-well electrical penetrations had small leaks through the inboard sides of their double seals. Two of 4 SRM cables were shorted or open. Four of 8 IRM cables had low insulation resistances. Ninety-three local PRM cables were shorted, 10 were open, and 61 were operable. Control cables to the TIP indexer were shorted. Two safety valves were jammed partly open owing to their lifting levers having been rotated by the steam and water jet from a 3rd safety valve.

Damage to plastic connector caps and cable insulation indicated that temperatures in excess of 250°F had occurred. Calculations based on steam conditions in the dry well indicated that the max temperature could have been no higher than 320°F and that the wall temperature was much less. Tempilstick marks on the walls indicated that 200°F was not exceeded. The containment-structure design temperature is 281°F at 0 psig.

The max pressure experienced by the pressure vessel and the main steam lines during the incident was determined to be less than the design pressure.

Tests with new samples of local PRM cables revealed that failures of center conductors occurred by buckling at as low as 220°F and that drifting of the center conductor caused shorts at as low as 300°F. This type of failure was enhanced by handling abuse, twisting, and crowding in ducts. Not all tests produced failure, even up to 500°F for 1 hr. Since these cables are vendor specified for continuous operation at 275°F, the same kind of cable was reinstalled but with great care and with less crowding in ducts. SRM and IRM cables were not tested, since it was known that their temperature ratings were less than that of the local PRM cables. They were replaced with a new type of cable having a temperature rating of 350°F. New ducts were provided to separate the SRM and IRM cables from the local PRM cables to avoid crowding. The TIP indexer control cables were replaced with new cables rated for 300°F.

The main-steam-line safety valves that lifted were inspected and tested in accordance with the manufacturer's recommended criteria and the ASME and Illinois Boiler Code requirements. Their associated rupture disks were replaced, and the valves were oriented so that damage to other equipment by their discharge would be minimized. Since lifting levers on the valves were not required by the ASME Code, approval to remove them was requested from the Illinois Boiler Board.

Motors on all valves were dried and passed inspection. One of 7 dry-well-cooling blower motors had to be replaced. All leaks in the inboard electrical-penetration seals were repaired. The FW control system was improved to minimize control-valve leakage, insensitivity of flow control, and low suction trip caused by pump-runout conditions.

The sequence and starting times of the EECS components were not according to design during the incident, although their actual use was not required. The system controls were revamped to conform to the design requirements.

The condensate-return-isolation trip point on the isolation condenser was raised from 120 to 300% of normal flow to agree with the design intent and the operating conditions. The Tech Specs were revised to reflect this.

The electrohydraulic-control system, in which the spurious signal that triggered the incident originated, was revised to minimize noise pickup. Specifically, the malfunctioning device, a potentiometer located at some distance from the pressure-amplifier card, was replaced with a ceramic potentiometer located near the pressure-amplifier card, and some associated terminals were eliminated. Cables from the electrohydraulic-control adjustment panel were rerouted so that the signal cables were separated from power cables. A control circuit relating the automatic load-following circuits, the recirculation-flow-control system, and the electrohydraulic-control load-frequency-control circuit was rearranged to eliminate the possibility of introducing erroneous voltages to the electrohydraulic-control panel.

Although the actions of the operators resulted in a safe and more or less orderly shutdown despite equipment malfunctions, a review of events indicated that the existing procedures were not altogether adequate. Much emphasis had been placed on the dangers of allowing the pressure-vessel water level to fall below the top of the fuel, but not enough emphasis was given to the dangers of high-water-level situations. Both the normal and emergency operating procedures were reviewed and revised to place more emphasis on the seriousness of high-water problems. The standby gas-treatment system was used as a venting path to reduce the pressure in the dry well when the only knowledge of the pressure there was that it was greater than 5 psig. This was done under closely controlled conditions and through a 2 in. bypass line rather than the 18 in. line provided. The gas-treatment system, however, was designed to operate at near atmospheric pressures and was tested at only 1.5 psig. Therefore, it was felt that a safer procedure would have been to reduce the dry-well pressure to below 2 psig by condensing steam with the torus sprays or, if necessary, the dry-well sprays before venting to the gas-treatment system. New procedures and revisions of existing procedures were issued to establish this.

The abnormal part of this incident began with the loss of water-level control, which was caused by the operator observing a water-level indicator that had a stuck pen.

It was known that the isolation condenser needed a greater condensate-return-line capability, however, it appears that no special procedures regarding its use and limitations were observed. After initial actuation of the condenser, several minutes elapsed before the operator was aware that it had almost immediately quit functioning.

The duration of the outage was ~1 1/2 mos. (gb,od)

Nuclear Power Experiences
Vol. BWR-2
XVI. Operational Probs.
C. Misc.
p. 2 and 3

7. OPERATOR PLACES FW SYSTEM IN MANUAL, THEN COULD NOT CONTROL TRANSIENT

Nine Mile Pt. 1 - Dec 71

Routine testing of the reactor protection high/low level water level sensors was being conducted while the plant was at 601 MWe. The sensor support was accidentally bumped causing each high level trip sensor to operate resulting in a turbine trip. A reactor scram resulted from the turbine anticipatory trip signal because the load was greater than 45%.

Following the scram, the reactor water level decreased rapidly due to void collapse. The FW control system responded by overfeeding, as it should, when in the automatic mode. The FW system was left in the automatic mode for ~20 sec after the scram, and then switched to the manual mode, because the FW flow to the reactor was high in the operation's opinion. Manual action was too slow and excessive FW flow continued to the reactor. FW flow was reduced to zero at ~2 min after water overflowed into the main steam lines. Several operations of the electromagnetic relief valves occurred for ~17 min after which reactor level was brought under control. The emergency condenser was then placed in service to control reactor pressure.

Investigation of the FW system has shown that the control response is adequate to handle the transient after a scram. The decision by an operator to place the system in manual is a judgment decision based on the interpretation of the instrumentation he is observing. Once he has made the decision and goes to the manual mode; he must be extremely dexterous as level varies so rapidly for the first few minutes following the scram that it becomes almost impossible to differentiate the variables and perform the correct manipulations in the required interval. At this time, level was

near the +3 ft level, and flow was greater than 6 X 10^6 lbs/hr. Flow was reduced to 2 X 10^6 lbs/hr at 2 min after the scram. Data indicated that overflow of water into the steam lines occurred about 2 min after the scram. Some FW flow continued for the next 2 min before being reduced to zero.

They concluded that placing the FW system in manual when fast response is required may cause a level problem if the operator does not pay close attention to the system during the transient. A review of expected system response was given to the operators. (kr,oc)

Nuclear Power Experiences
Vol. BWR-2
IX. Inst. & Cont.
D. Turbine Cycle
p. 6 and 7

19. FEEDWATER TRANSIENT - DRYWELL PRESSURIZED

Dresden 3 - Dec 71

The plant was at 792 MWe when a condensate booster pump tripped. Personnel heard noises coming from the pump just prior to the trip, however, complete teardown and inspection of both the condensate pump and booster pump revealed no damage. Recorder charts revealed no anomalous behavior. The pump is tripped automatically on undervoltage or overcurrent. The pump motor breaker showed no trip target.

Loss of the pump resulted in a low FW pump suction pressure condition, since 2 condensate booster pumps are inadequate to supply the required water at that power level. The 2 operating FW pumps tripped on low suction pressure. The standby reactor FW pump started automatically when the operating FW pumps tripped. The standby pump reaches full flow in ~6 sec. Following the decrease in FW input, the reactor water low level trip scrammed the reactor at 14 sec.

Reactor water level continued to decrease and reached a low point of ~-20 in. (~123 in. above top of fuel). Level then began to increase and the operator took manual action in anticipation of a rapid level increase.

When reactor water level reached -12 in., it appeared to hesitate and the operator attempted to increase level. Level began to increase rapidly, and as soon as the operator verified that level was increasing, he again reduced the manual output control potentiometer to zero. As reactor water level came through zero, the operator started closing the FW regulating valve motor operated isolation valve, again in anticipation of a rapid

level increase. As the valve closed, FW flow was reduced from 5.7 X 10^6 to 2.3 X 10^6 lb/hr. At some time during the closure of this valve, it stalled due to high dp across the gate.

When the standby reactor FW pump started, flow increased to the point where the FW regulating valve went into a "runout" condition (flow control mode). This was substantiated by various instrumentation.

The FW regulating valve locked out in an open position. Subsequent testing indicated that the lockout condition was probably caused by low air pressure which resulted from rapid movement of the valve.

Reactor pressure decreased following the pump trip due to shrinkage from the cold FW, and initially, loss of steam to the turbine. At 1 min 5 sec, main steam line low pressure of 850 psig initiated a Group I isolation signal and the MSIV's closed.

Reactor pressure reached a low point of 795 psig. At that point FW input and decay heat caused reactor pressure to increase. Reactor water level continued to increase and the low reactor water level trip automatically reset at 1 min 21 sec. Reactor water level continued to increase from a FW input of ~5.7 x 10^6 lb/hr and reached the high water level trip point of +48 in., at which point the turbine stop valves tripped. The control valves had already closed while attempting to maintain pressure.

Reactor pressure continued to increase from FW input and the operator manually cut in the isolation condenser. But reactor water level was above the isolation condenser supply nozzel and since the condenser was essentially operating as a water to water heat exchanger, it had little effect on pressure. The level reached the level of the main steam lines at ~2 min 45 sec, and began to fill them. A safety valve lifted. Pressure had reached 1020 psig and decreased rapidly when the valve opened. At this point water had probably filled most of the steam lines. It is believed that the safety valve did not lift from pressure actuation. Primary system water released to the drywell through the safety valve flashed to steam, and pressurized the drywell. Drywell pressure reached 2 psig at 5 min

11 sec, and the reactor containment high pressure trip was actuated. This started both diesel generators, the core spray pumps, and LPCI pumps automatically. The HPCI received an initiation signal, but tripped on high reactor water level. The reactor recirculation pumps tripped and a containment isolation (Group II) was initiated. All ECCS subsystems functioned as designed.

Drywell pressure continued to increase, due to input from the safety valve, and peaked at 20 psig at ~6 min 30 sec. The safety valve remained open for ~1 1/2 min $\pm$ 30 sec.

At 7 min, suppression cooling was initiated via recirculation of the torus water through the containment cooling heat exchangers. The torus sprays were not placed in service.

At 8 min, the first indications of LPRM failure were observed. At this point the shutdown condition of the reactor had already been observed. At 13 min the operator tripped the operating reactor feed pump. At this time reactor water level was ~130 in. Reactor pressure peaked at 1025 and dropped to 980 psig when the reactor feed pump was tripped. Reactor pressure then began to increase again due to decay heat input.

At ~23 min a reactor high pressure sensor tripped and reactor pressure peaked at 1044 psig. Reactor pressure then decreased due to loss of water inventory when an unsuccessful attempt was made to place the cleanup dimeneralizer system in service. Pressure dropped to 950 psig and again began to increase from decay heat input. A check of the trip indicated that it was set lower than the other 3 sensors. At ~3 hr 47 min containment pressure had decreased to 4.5 psig.

At ~4 hrs, a jumper was installed to permit opening the reactor water sample isolation valves so that a sample could be collected. Reactor blowdown to reduce water level could not be established without first collecting a water sample and high level isolates the sample line.

Analysis indicated normal activity and reactor water blowdown via the cleanup system was established at 5 hrs. Vessel water level had increased to +45 in. at this time due to continued input of water from the CRD system.

At ~12 hrs, drywell pressure had decreased to 1.75 psig and the containment high pressure trips automatically reset. ECCS systems no longer had an initiation signal and these systems were returned to standby condition and the drywell coolers were restarted manually.

At ~13 hrs, reduction of reactor water level to below the main steam lines was initiated and at ~17 hrs, level had been decreased to +76 in.

Analysis of the first sample of containment atmosphere indicated radioactivity slightly above normal.

Controlled cooldown of the primary system continued using the cleanup system. At ~33 hrs reactor pressure had been reduced to 180 psig and the shutdown cooling system was placed in service.

Additional drywell atmosphere sample analysis indicated reduced radioactivity level at ~40 hrs, drywell deinerting, was instituted. At 44 hrs an initial entry was made for atmospheric sampling. Radioactivity levels were low and the first entry for drywell inspection was made ~46 hrs after the incident.

The following equipment was damaged:

- The rupture discs on 4 of the 8 safety valves were ruptured. This may not be related to the incident since this condition had been encountered previously. Additionally one safety valve rupture disc was completely blown out.

- An electromatic valve solenoid operator was damaged by the steam jet from a safety valve. One steam discharge "rams horn" on the safety valve was directed towards the electromatic valve. The cover on the solenoid

assembly of this valve was blown off. The holding coil circuit of the solenoid assembly was found open. Wiring to a position indicating limit switch was also damaged, rendering the position indication inoperative.

- Miscellaneous insulation and paint was damaged.

- Sections of ventilating duct in the vicinity of the steam jet were dislodged.

- Essentially all of the LPRM cables were found damaged.

- One containment cooling fan motor was found to have a ground caused by moisture in the containment. The other 6 cooling fan motors were found to be in good condition.

2. OVERCOOLING TRANSIENTS

Nuclear Power Experiences
Vol. BWR-2
IX. Instr. & Cont.
D. Turbine Cycle
p. 20 and 21

71. FAILED COUNTER CARD IN EHC SYSTEM, MODE SWITCH NOT IN RUN - SCRAM, BLOWDOWN, FAST COOLDOWN

Cooper - Nov 80 - 93% power

A reactor scram occurred during an APRM functional test. Following the scram the reactor coolant temperature change exceeded the normal cooldown rate of 100°F/hr. The apparent cause of the occurrence was attributed to a failed counter card (W-Hogan 398522) in the Digital Electrohydraulic Control System for the main turbine. The failed card caused the main steam bypass valves to remain open following the scram. The 825 psig reactor pressure closure of the MSIV did not occur because the "mode" switch was manually taken out of "Run" shortly after the scram.

The main steam bypass valves control reactor pressure during startup and after a reactor scram when the MSIV's are open.

During this event, the reactor depressurized from ~1000 to ~210 psig in 9 min. This caused the reactor vessel metal temperature to decrease ~150°F during the next hour. This temperature transient was similar to the "stuck open relief valve" transient and was not limiting in the reactor vessel thermal cycles analysis at that time.

The failed component was replaced and tested. A review of the operator actions during tests of that type and actions following scrams were being reviewed. (icq)

Nuclear Power Experiences
Vol. BWR-2
V. Recirc, Steam, Relief
C. Relief & Safety Valves
p. 72

238. RELIEF LIFTED - EXCESSIVE COOLDOWN RATE

Peach Bottom 3 - June 79 - 95% power

A main steam relief valve lifted spontaneously causing torus water volume to reach 130,675 ft^3 2.6% above the Tech Spec limit of 127,300 ft^3. After the relief valve opened and attempts to reclose it were unsuccessful, the reactor was manually scrammed. The reactor cool-down rate reached a max of 114°F in 1 hr 14°F above the Tech Spec limit of 100°F/hr. The relief valve was open for about 95 min, being reseated when reactor pressure was reduced to 135 psig.

The relief valve (Target Rock) was replaced with another qualified valve. The valve that lifted was sent to Wiley Lab for inspection to etermine the reason for failure. A VT of the drywell and torus interior and exterior was performed prior to return to power, and all areas were found to be in satisfactory condition. The duration of the outage was 44 hr. (gbc)

Nuclear Power Experiences
Vol. BWR-2
XVI. Operational Probs.
C. Misc.
p. 113 and 114

446. SCRAM, LOW REACTOR PRESSURE - CONDENSATE INJECTED INTO VESSEL, EXCESSIVE COOLDOWN RATE

Hatch 2 - Nov 78 (power ascension testing) - shutdown

Due to an injection of condensate water into the reactor vessel following a reactor scram from rated pressure, reactor pressure decreased due to main turbine seals supplied by nuclear steam to below condensate booster pump pressure and allowed condensate water to be injected into the reactor vessel through the FW lines, resulting in a cooldown rate of 119°F/hr exceeding the max cooldown rate of 100°F/hr. The MSIV's were closed and injection of condensate water to the vessel stopped. Reactor coolant temperatures were back within limits in 15 min.

The cause of the event was personnel error. During the scram and vessel depressurization, personnel allowed condensate water to be injected into the reactor vessel when pressure decreased below the condensate booster pump discharge pressure, thus causing the rapid cooldown. Personnel were cautioned about reactor pressure decreases below a system pressure that could inject into the vessel during an emergency condition and to observe pressure decrease and level increase very closely in transient conditions to prevent exceeding reactor cooldown rates. Evaluation of the occurrence confirmed that due to evaluation of other temperatures indications for overall reactor coolant systems and by observing reactor vessel metal temperatures (ΔT's), that no significant stress occurred to the reactor vessel or coolant systems. (fkb)

327. REACTOR PRESSURE INDICATOR MAINTENANCE AFFECTED PRESSURE RECORDER - LOW REACTOR PRESSURE ALLOWED CONDENSATE BOOSTER PUMP INJECTION - EXCESSIVE COOLDOWN

Brunswick 1 - Feb 77 - shutdown

The reactor had been scrammed due to a low condenser vacuum turbine trip and the reactor was being cooled down slowly (~40°F/hr). RCIC was being used to maintain reactor vessel water level and the Startup Level Control Valve was in manual and open 60%. During the cooldown, reactor pressure decreased to less than condensate booster pump discharge pressure (~400 psig). This allowed the condensate booster pumps to feed the RPV. Reactor vessel level increased rapidly and reactor vessel temperature decreased due to the cold FW addition. RCIC tripped on high reactor vessel level. The outlet valves on the No. 5 FW heaters were shut and the startup level control valve was shut to terminate the reactor vessel level increase and subsequent cooldown. However, the cooldown between 1300 and 1400 was 110°F, which exceeded the Tech Spec max allowed cooldown rate.

An I&C Technician was performing maintenance on a reactor pressure indicator, which was reading ~200 psig high. This required the level selector switch to be set to the Level "A" position. However, in the Level "A" position both the reactor pressure indicator and reactor pressure recorder were supplied with the same pressure compensating signal that supplied the reactor water level control system. Although the operator who was watching the reactor pressure recorder did realize that actual reactor pressure was ~200 psig lower than indicated on the indicator, he did not realize that the pressure recorder was also affected. Therefore, as actual pressure decreased to 400 psig, the condensate booster pump began to supply FW to the RPV. This event was to be reviewed by all licensed personnel.

All Shift Foremen and Control Operators were to be cautioned to more closely review any maintenance work which might affect this instrumentation. All licensed personnel were to be instructed to use and compare all available indication and not to linger on one indication.

(dlu)

6. REFERENCES

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