ornl

NUREG/CR-4265
Volume 1
ORNL/TM-9640/V1

OAK RIDGE
NATIONAL
LABORATORY

MARTIN MARIETTA

An Assessment of the Safety Implications of Control at the Calvert Cliffs-1 Nuclear Plant Volume 1

S. J. Ball
R. E. Battle
E. W. Hagen
L. L. Joyner
A. F. McBride
J-P. A. Renier
O. L. Smith
R. S. Stone

Prepared for the
U.S. Nuclear Regulatory Commission
Division of Engineering Technology
Office of Nuclear Regulatory Research
Under Interagency Agreement DOE 40-550-75

8607070481 860430
PDR ADOCK 05000317
P PDR

OPERATED BY
MARTIN MARIETTA ENERGY SYSTEMS, INC.
FOR THE UNITED STATES
DEPARTMENT OF ENERGY

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from

Superintendent of Documents
U.S. Government Printing Office
Post Office Box 37082
Washington, D.C. 20013-7982

and

National Technical Information Service
Springfield, VA 22161

NUREG/CR-4265
Volume 1
ORNL/TM-9640/V1
NRC Distribution R1, RG, R4

Instrumentation and Controls Division

AN ASSESSMENT OF THE SAFETY IMPLICATIONS OF CONTROL AT THE CALVERT CLIFFS-1 NUCLEAR PLANT
Volume 1

S. J. Ball, Program Manager

Authors and Contributors:

P. N. Austin[1]
S. J. Ball
R. E. Battle
S. J. Caruthers[1]
N. E. Clapp, Jr.
F. H. Clark
R. D. Dabbs[2]
J. D. Freels[2]
E. W. Hagen
K. M. Henry
S. J. Hurrell[1]
L. L. Joyner[3]
C. G. Lawson
C. W. Mayo[1]
T. C. Morelock
A. F. McBride[1]
J. P. Renier
O. L. Smith
R. S. Stone
W. A. Waddell

Manuscript Completed: September 30, 1985
Date of Issue: April 1986

[1]Science Applications, Inc., Oak Ridge, Tenn.
[2]Technology for Energy, Knoxville, Tenn.
[3]Joyner Engineers and Trainers, PC., Forest, Va.

Prepared for the
Division of Engineering Commission
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555
Under Interagency Agreement DOE 40-550-75

NRC FIN. Nos. B0467 and B0816

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831
operated by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under Contract No. DE-AC05-84OR21400

TABLE OF CONTENTS

LIST OF FIGURES vii

LIST OF TABLES viii

ACRONYMS xv

ABSTRACT xvii

1. EXECUTIVE SUMMARY 1

1.1 BACKGROUND 1
1.2 OBJECTIVES 1
1.3 APPROACH 2
1.4 RESULTS 3

2. INTRODUCTION 7

2.1 BACKGROUND 7
2.2 OBJECTIVES 8
2.3 APPROACH 10
2.4 REPORT ORGANIZATION AND CONTENTS 10

3. CALVERT CLIFFS NUCLEAR POWER PLANT SYSTEMS AND OPERATIONS 15

3.1 IDENTIFICATION AND SELECTION OF SYSTEMS PERTINENT TO SICS 17
3.1.1 Selection Methodology 17
3.1.2 Summary of Systems Selected for FMEA 20
3.2 PLANT OPERATING EXPERIENCE 29
3.2.1 Introduction 29
3.2.2 Calvert Cliffs Units 1 and 2 29
3.2.3 Other C-E Plant Relevant Operating Experiences 44
3.2.4 Summary and Conclusions 52

4. DETERMINATION OF SICS SEQUENCES FOR ANALYSIS 55

4.1 FMEA OBJECTIVES AND METHODOLOGY 55
4.1.1 Selection and Application of FMEA Methodology 55
4.1.2 Accident Sequence Development Methodology . . . 57
4.2 IDENTIFICATION OF SIGNIFICANT CONTROL SYSTEM FAILURES 58
4.2.1 System-Level Failure Modes and Effects Analysis (FMEA) 59
4.2.2 Component-Level FMEA 78
4.3 ACCIDENT SEQUENCE DEVELOPMENT 132
4.3.1 Summary of Significant Accident Sequences 132

TABLE OF CONTENTS (continued)

4.3.2 Development and Evaluation of Accident Sequences 133
4.4 IDENTIFICATION OF OPERATOR EFFECTS 146
4.5 ELECTRICAL FAILURES THAT COULD CONTRIBUTE TO SIGNIFICANT ACCIDENT SEQUENCES 148
4.5.1 Electrical System Failures that Affect the Capability to Reduce Primary System Pressure 150
4.5.2 Electrical System Failures that Affect Steam Generator Overfill 152
4.5.3 Quantitative Analysis of Electrical Failure 154
4.6 INSTRUMENT AIR FAILURES THAT COULD CONTRIBUTE TO SIGNIFICANT ACCIDENT SEQUENCES 155
4.7 GENERIC IMPLICATIONS OF CALVERT CLIFFS-1 SCENARIOS . . 162
4.7.1 Background 162
4.7.2 Water Injection and Pressurizer Pressure Relief Features in Other C-E Plants 162
4.7.3 Combinations of Identified Failures with Generic Implications 163

5. QUANTIFICATION OF SEQUENCE FREQUENCY 167

5.1 SUMMARY OF FREQUENCY QUANTIFICATION RESULTS 167
5.2 QUANTIFICATION OF SMALL-BREAK LOCA SEQUENCES 168
5.2.1 Small-Break LOCA Sequences Involving Insufficient Core Cooling 168
5.2.2 Small-Break LOCA Sequence Involving Pressurized Thermal Shock Conditions 172
5.3 STEAM GENERATOR OVERFILL 173
5.3.1 Feedwater Valve Receives Closure Signal from Turbine Trip Circuitry 174
5.3.2 Feedwater Regulating Valve Circuit Fails to Receive Closure Signal from Turbine Trip Circuitry 175
5.4 INITIATING EVENT PROBABILITIES 177

6. AUGMENTED FAILURE MODE AND EFFECTS ANALYSIS 179

6.1 RETRAN MODELING OF CALVERT CLIFFS-1 179
6.1.1 Overview of the Model 179
6.1.2 Model Validation 182
6.1.3 Transients Run with the Model 182
6.1.4 Calculation Results 183
6.1.5 Conclusions 188
6.2 MODULAR MODELING OF CALVERT CLIFFS 189
6.2.1 Simulator Description 189
6.2.2 Simulator Results 191

7. RESULTS AND CONCLUSIONS 207

TABLE OF CONTENTS (continued)

8. RECOMMENDATIONS FOR RESOLUTION OF USI A-47 213

8.1 BACKGROUND 213
8.2 INSIGHTS FROM THE SICS STUDY OF CALVERT CLIFFS-1 . . . 214

9. RECOMMENDATIONS FOR FUTURE WORK 217

REFERENCES 219

LIST OF FIGURES

2.1 Program flow for study of safety effects of nuclear power plant control system failures 11

3.1 System selection methodology 18

4.1 Reactor trip event tree 136

4.2 Steam line break event tree 137

4.3 Small-break LOCA event tree 138

4.4 Loss of MFW event tree 140

4.5 Loss of non-emergency ac power event tree 140

4.6 SG overfeed event tree (excess FW flow) 145

4.7 Functional block diagram of pressurizer relief valve control 151

5.1 Insufficient core cooling LOCA sequence fault tree 170

5.2 Fault tree of SG overfill when regulating valve circuit receives turbine trip signal 175

5.3 Fault tree of SG overfill when regulating valve circuit fails to receive turbine trip signal 177

6.1 RETRAN model of Calvert Cliffs-1 180

6.2 SG-A FW flow with SG-A steam flow reading failed high at 1940 lb/s 185

6.3 SG-A water level with SG-A measured water level reading failed 10 in. below set point 192

6.4 SG-A steam flow with SG-A measured water level reading failed 10 in. below set point 192

6.5 SG-A outlet quality with SG-A measured water level reading failed 10 in. below set point 192

6.6 Average core coolant temperature with SG-A measured water level reading failed 10 in. below set point 192

6.7 Reactor power with SG-A measured water level reading failed 10 in. below set point 193

6.8 Steam line A pressure with SG-A measured water level reading failed 10 in. below set point 193

LIST OF FIGURES (continued)

6.9 SG-A FW flow with SG-A measured water level reading failed 10 in. below set point 193

6.10 SG-A water level with SG-A MFW valve failed full open in 1.5 s 193

6.11 SG-A FW flow with SG-A MFW valve failed full open in 1.5 s 194

6.12 SG-B wide-range water level with SG-A MFW valve failed full open in 1.5 s 194

6.13 Average core coolant temperature with SG-A MFW valve failed full open in 1.5 s 194

6.14 Pressurizer pressure (psia) with SG-A MFW valve failed full open in 1.5 s 194

6.15 Pressurizer water level with SG-A MFW valve failed full open in 1.5 s 195

6.16 SG-A water level with SG-A MFW valve failed open in 1.5s; MFW isolation valve failed open 195

6.17 SG-A outlet steam quality with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open 195

6.18 SG-A exit steam flow with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open 195

6.19 Average core coolant temperature with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open 196

6.20 Pressurizer pressure with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open 196

6.21 Pressurizer water level with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open 196

6.22 SG-A water level with SG-A MFW valve frozen in place on reactor/turbine trip 196

6.23 Average core coolant temperature with SG-A MFW valve frozen in place on reactor/turbine trip 197

6.24 SG-A exit steam flow with SG-A MFW valve failed full open in 1.5 s (repeated after recent Calvert Cliffs-1 design change) 197

LIST OF FIGURES (continued)

6.25 Average core coolant temperature with SG-A MFW valve failed full open in 1.5 s (repeated after recent Calvert Cliffs-1 design change) 197

6.26 Pressurizer pressure with SG-A MFW valve failed full open in 1.5 s (repeated after recent Calvert Cliffs-1 design change) 197

6.27 Pressurizer water level with SG-A MFW valve failed full open in 1.5 s (repeated after recent Calvert Cliffs-1 design change) 198

6.28 SG-A exit steam flow with SG-A MFW valve failed in place on reactor trip (repeated after recent Calvert Cliffs-1 design change) 198

6.29 Average core coolant temperature with SG-A MFW valve failed in place on reactor trip (repeated after recent Calvert Cliffs-1 design change) 198

6.30 Pressurizer pressure with SG-A MFW valve failed in place on reactor trip (repeated after recent Calvert Cliffs-1 design change) 198

6.31 Pressurizer water level with SG-A MFW valve failed in place on reactor trip (repeated after recent Calvert Cliffs-1 design change) 199

6.32 SG-A FW flow with SG-A steam flow reading failed low at 1110 lb/s 199

6.33 SG-A measured water level with SG-A measured level failed 10 in. above set point and low and low-low level trips failed 199

6.34 MFW valve A area with SG-A measured level failed 10 in. above set point and low and low-low level trips failed 199

6.35 SG-A FW flow with SG-A measured level failed 10 in. above set point and low and low-low level trips failed 200

6.36 Pressurizer pressure with SG-A measured level failed 10 in. above set point and low and low-low level trips failed 200

6.37 SG-A measured water level with SG-A measured level failed 10 in. above set point and low and low-low level trips failed 200

LIST OF FIGURES (continued)

6.38 Reactor power with SG-A measured level failed 10 in. above set point and low and low-low level trips failed . . . 200

6.39 SG-A FW flow with MFW valve A failed closed in 5 s 201

6.40 SG-A water level (narrow range) with MFW valve A failed closed in 5 s 201

6.41 SG-B water level (narrow range) with MFW valve A failed closed in 5 s 201

6.42 Reactor power with MFW valve A failed closed in 5 s 201

6.43 Average core coolant temperature with MFW valve A failed closed in 5 s 202

6.44 Pressurizer pressure with MFW valve A failed closed in 5 s 202

6.45 Pressurizer water level with MFW valve A failed closed in 5 s 202

6.46 SG-A with MFW valve A failed closed in 5 s 202

6.47 Pressurizer pressure with both PORVs failed open 203

6.48 Reactor power with both PORVs failed open 203

6.49 Pressurizer water level with both PORVs failed open 203

6.50 Average core coolant temperature with both PORVs failed open 203

6.51 SG-A water level with both PORVs failed open 204

6.52 Pressurizer pressure with one PORV failed open 204

6.53 Pressurizer water level with one PORV failed open 204

6.54 Average core coolant temperature with one PORV failed open 204

6.55 Steam volume fraction with one PORV failed open 205

6.56 Pressurizer pressure with small break (0.0015 ft^2) in loop A hot leg 205

6.57 Pressurizer water level with small break (0.0015 ft^2) in loop A hot leg 205

LIST OF FIGURES (continued)

6.58 Average core coolant temperature with small break (0.0015 ft^2) in loop A hot leg 205

6.59 Reactor power with small break (0.0015 ft^2) in loop A hot leg 205

6.60 Voiding in vessel upper head with small break (0.0015 ft^2) in loop A hot leg 206

LIST OF TABLES

3.1.	Summary of Calvert Cliffs systems selected for FMEA	21
3.2.	Summary of Calvert Cliffs systems not selected for FMEA . .	25
3.3.	Calvert Cliffs-1 relevant operating experiences	30
3.4.	Calvert Cliffs-2 relevant operating experiences	34
3.5.	Relevant operating experiences at other C-E plants (scrams/trips and transients)	38
3.6.	Relevant operating experiences at other C-E plants	45
4.1.	Summary of system-level failure modes and effects analysis	60
4.2.	Reactor coolant system FMEA summary	80
4.3.	Chemical and volume control system FMEA summary	88
4.4.	Pressurizer level regulating system FMEA summary	97
4.5.	Reactor coolant pressure regulating system FMEA summary . .	102
4.6.	Reactor regulating system FMEA summary	106
4.7.	Main feedwater and condensate FMEA summary	107
4.8.	Feedwater regulating system FMEA summary	113
4.9.	Main steam, atmospheric dump, and turbine by-pass systems FMEA summary	116
4.10.	Component cooling system FMEA summary	119
4.11.	Service water system FMEA summary	124
4.12.	Salt water system FMEA summary	131
4.13.	Summary of FSAR Chapter 14 initiating events	134
4.14.	Summary of impact of instrument air failure on key reactor systems and components	159
5.1.	Basis of failure rates for steam generator overfill fault tree	176
5.2.	Approximate frequency of initiating events/sequence precursors based on Calvert Cliffs and other C-E plant operating histories	178

ACRONYMS

Note: Acroynms identified and used only once in the text are not included in the following list.

AFAS	auxiliary feedwater actuation signal
AFS	auxiliary feedwater system
AFW	auxiliary feedwater
ATWS	Anticipated Transient Without Scram
BG&E	Baltimore Gas and Electric Company
B&W	Babcock and Wilcox
BWR	boiling-water reactor
CCW	component cooling water
C-E	Combustion Engineering
CEA	control element assembly
CVCS	chemical and volume control system
dP	pressure differential
ECCS	emergency core cooling system
EFW	emergency feedwater
EOP	Emergency Operating Procedure
E/P	electric-to-pneumatic
ESF	essential safety features
ESFAS	engineered safety features actuation system
FMEA	failure modes and effects analysis
FSAR	Final Safety Analysis Report
FW	feedwater
gpm	gallons per minute
HPI	high-pressure injection
HPSI	high-pressure safety injection
HPT	high-pressure turbine
IA	instrument air
I&C	Instrumentation and Controls
ICS	Integrated Control System
INEL	Idaho National Engineering Laboratory
I/P	current-to-pneumatic
LER	Licensee Event Report
LOCA	loss-of-coolant accident
LPSI	low-pressure safety injection
LWR	light-water reactor
MCC	motor control center
MFW	main feedwater

MMS	modular modeling system
MSIV	Main Steam Isolation Valve
NNI	nonnuclear instrumentation
NRC	Nuclear Regulatory Commission
NSAC	Nuclear Safety and Analysis Center
NSIC	Nuclear Safety Information Center
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
OTSG	once-through steam generator
PORV	pilot-operated relief valve
PPS	plant protection system
PRA	probabilistic risk assessment
PTS	pressurized thermal shock
PWR	pressurized water reactor
RC	reactor coolant
RCDT	reactor coolant drain tank
RCS	reactor coolant system
RPS	reactor protection system
RRS	Reactor Regulating System
RWST	Refueling Water Storage Tank
RWT	Refueling Water Tank
ry	reactor year
SB-LOCA	small-break LOCA
S&C	sense and command
SG	steam generator
SGIS	Steam generator isolation system
SI	safety injection
SIAS	safety injection/actuation system
SICS	Safety Implications of Control Systems [Program]
SIS	safety injection signal
SRW	service water system
TAP	task action plan
TBV	turbine bypass valve
TMLP	thermal margin low pressure
USI	Unresolved Safety Issue
UTSG	U-tube steam generator
VCT	volume control tank

ABSTRACT

This study examined the consequences of possible control system malfunctions at the Calvert Cliffs-1 Nuclear Power Plant as technical support for an NRC program to assess the safety implications of nuclear power plant control systems. Plant systems capable of initiating plant overcooling and undercooling were identified, as well as those with potential for overfill events in the steam generators.

Failure mode and effects analyses were conducted on these candidate plant systems, with computer analysis applied where appropriate. This latter process utilized a detailed RETRAN model of the Calvert Cliffs Plant using adaptations made as part of this program. Where failures with safety consequences were found, probabilities of the pertinent scenarios were developed. Several control system failures were identified as being of possible safety concern. Of these, two were selected as being of sufficient interest to warrant further study and followup using plant simulations.

The first of the two major areas deals with the potential for steam generator overfill. Some postulated overfeed events require timely operator action, and if they are not terminated in time, the steam generator can overfill and inject liquid into the steam line.

The second major sequence of interest is a critically sized small-break loss-of-coolant accident (SB-LOCA). An SB-LOCA can be initiated by control system malfunctions as well as by passive failure mechanisms such as steam generator tube ruptures. Our initial concern arose from the fact that the high-pressure safety injection (HPSI) system pumps can deliver coolant at a head of no more than 1275 psi, and that consequently there may be situations in which the primary coolant system pressure is high enough that the HPSI pumps cannot adequately make up for the net inventory loss, with the latter ultimately leading to core uncovery and fuel damage. Subsequent analyses indicated a very small probability of fuel damage for this scenario.

Consequences of the events of major concern were examined by computer analysis, and probabilities for their precursors were estimated. Other results presented include an analysis of plant operating experiences germane to the Safety Implication of Control Systems (SICS) project. This review centered on Calvert Cliffs Unit 1, but also derived data from Unit 2 and the other operating Combustion Engineering plants. This report also examines the industry-generic conclusions that can be derived from this plant-specific study of Calvert Cliffs.

1. EXECUTIVE SUMMARY

1.1 BACKGROUND

This report on the Safety Implications of Control Systems (SICS) is the second of an Oak Ridge National Laboratory (ORNL) series incorporating detailed analyses of specific plants, the first of which was a study of Oconee-1 (ORNL/TM-9444).[1] This report investigates Calvert Cliffs-1, an 850-MW(e) Combustion Engineering (C-E) pressurized water reactor (PWR) owned and operated by Baltimore Gas & Electric Co (BG&E). The two plants are similar in that they are both PWRs and are of early 1970s vintage. Their most important differences, for the purposes of this study, are their different types of steam generators (once-through at Oconee, U-tube at Calvert Cliffs) and different control philosophies. The Oconee Plant uses a completely integrated and extensive control system, while several of the major parameters at Calvert Cliffs are under manual (operator) control. In effect, at Calvert Cliffs this makes the operators a more crucial part of the "control systems" that are factored into the SICS study. Calvert Cliffs also has a much lower pressure high-pressure safety injection (HPSI) system for emergency cooling (1275 psia versus 2800 psia for Oconee), which may be an important consideration in small-break loss-of-coolant accident (SB-LOCA) sequences.

The program is sponsored by the U.S. Nuclear Regulatory Commission Division of Engineering Technology. The NRC Program Manager is Demetrios L. Basdekas.

1.2 OBJECTIVES

The major objective of the ORNL-SICS program is to provide technical support to the U.S. Nuclear Regulatory Commission (NRC) staff for their task of resolving the Unresolved Safety Issue (USI) A-47. Primary guidance for this task is provided by the A-47 Task Action Plan (TAP), which states that resolution of A-47 may be accomplished by performing ". . . an in-depth evaluation of the control systems that are typically used during normal plant operation and <verifying> the adequacy of current licensing design requirements or <proposing> additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent nonsafety-grade control system failures." The definition of "unacceptable risk" as a criterion for considering (or not) a given set of control system failures is subject to engineering judgment and hence to a variety of interpretations. In general, the loss of a control system or power supply will result in some loss of process control and/or information available to the operator. In most cases, however, the operator will still have sufficient means available to correct the problem or, if a trip occurs, to bring the plant to a safe shutdown condition. The sequences deemed of interest to this study are those which (1) significantly impede, delay, or defeat a plant protection system action; (2) cause the

transient to exceed the bounds of the accidents defined as "design basis" in the Final Safety Analysis Report (FSAR); or (3) challenge the safety systems frequently enough that the probability of plant damage is increased significantly. The interpretations put on the limits of acceptability are discussed in more detail in the body of the report.

The ORNL contribution to A-47 resolution consists of two detailed plant-specific investigations that are, to the extent possible, to be used to arrive at generic criteria and solutions to the overall safety concerns.

The limitations of the study, which were imposed to keep it to a manageable size, are defined in the following ground rules:

1. Single failures. Because of the very large number of control systems in a PWR, the number of situations encompassed by arbitrary combinations of multiple failures would be extremely large. Hence only single failures are considered in a systematic fashion; however, multiple failures are included in the study if they are found to be "interesting" or logical follow-ons of a particular scenario. What is generally looked for is the minimum number or most likely combination of component failures that would be required to generate, perpetuate, or exacerbate the accident scenario of interest. The likelihood of double or multiple failures can be assumed to be high enough to be of interest if one or more of the failures can be categorized as undetected, or if the failures can be assumed to be due to the loss of a common power supply or to another common precipitating event or problem.

2. Operator action. In general, operator inaction or misaction is to be considered if the information presented the operator is misleading/confusing/insufficient, or if the time available to diagnose the problem and accomplish the required tasks is short (Sect. 4.4 elaborates on what is meant by terms such as "misaction" and "short").

3. Event categories. Primarily, steam generator (SG) overfeed or dryout and core undercooling or overcooling events will be investigated. However, if other significant problems are found, they are pursued.

4. Power supplies. Loss of power supplies (ac, dc, instrument air) are considered.

1.3 APPROACH

In both the Oconee and Calvert Cliffs studies, the failure modes and effects analysis (FMEA) technique was employed. FMEA is a standard technique used to make systematic, qualitative searches for significant failures and consequences. The FMEA process, as it is adapted to this program, consists of identifying a failure class (such as reactor undercooling) and then defining broad functional conditions that must occur

to lead to this failure. Each control system is examined, noting its possible modes of failure and their effects on the failure class in question. This leads to the identification of the broad effects of postulated system failures and determines the subsystem malfunctions that can give rise to those failures. This process has been referred to as the "broad FMEA." Certain sequences are identified as being of major interest and, if not fully resolved by the broad FMEA, are made the subjects of computer simulation for further study. This part of the study is called the "augmented FMEA." Other sequences of interest come to light by virtue of reviews of operating experiences or by exercising the plant simulators.

1.4 RESULTS

Several control system failures have been identified which are of possible safety concern. Of these, two were selected as being of enough concern to warrant further study and follow-up using plant simulations. Several others were also designated as noteworthy, though not of sufficient concern to require further analysis.

The first major area deals with the potential for SG overfill. If a main feedwater (MFW) control valve should fail open, either through mechanical failure or through certain failures of an electronic control circuit, the SG will be overfed. Some postulated overfeed events require timely operator action, and if they are not terminated in time, the SG will overfill and inject liquid into the steam line. The momentum transfer from the water to the steam line can induce a motion of the steam line against its supports, which in turn could lead to failure of the supports and possible deformation or rupture of the steam line. The amount of damage that would actually occur to the steam line in any given overfill accident scenario is by no means clear. While the lines are designed to withstand seismic events and substantial deadweight loads, they are not designed to survive severe dynamic loadings due to, for example, a main steam isolation valve slamming shut against a high-velocity steam-water flow. Furthermore, the time available to the operator to take corrective action may be quite small, depending on the particular scenario. Some overfill scenario simulations indicate that water could begin entering the steam lines as early as 3 to 5 min after the start of the transient.

The second major sequence of interest is a critically sized SB-LOCA. Small-break loss-of-coolant accidents can be initiated by control system malfunctions, as well as by passive failure mechanisms such as SG tube ruptures. Our initial concern was based on the fact that the HPSI system pumps can deliver coolant at a head of no more than 1275 psi, and that consequently there may be situations in which the primary coolant system pressure is high enough that the HPSI pumps cannot adequately make up for the net inventory loss, which could lead to core uncovery and fuel damage. The normal plant makeup system can inject 132 gpm into the primary loop independent of loop pressure (since they are positive-displacement pumps). The FSAR indicates that equivalent break or leak

sizes as small as 0.1 ft^2 have been analyzed and can be dealt with by the safety system. Our hypothesis was that between a leak size corresponding to the 132-gpm makeup flow and a leak size of 0.1 ft^2, there may be a range of leak sizes large enough to reduce the primary system inventory significantly and yet too small to depressurize from the normal operating pressure of 2250 psi to the point at which the HPSI can function. The equivalent 132-gpm leak size is two orders of magnitude smaller than a 0.1 ft^2 hole. In the currently-used emergency operating procedure (EOP) for LOCAs, this situation is not covered satisfactorily; however, BG&E is currently in the process of upgrading this and other EOPs. Two mitigating factors make this a low-probability event. First, there is a lot of time available to take corrective action (perhaps up to an hour or more, depending on the size of the leak), making the possibility of misdiagnosis and erroneous action relatively low. One study of a different type PWR estimated that the probability of misdiagnosis in the early stages of SB-LOCAs would be about 0.05 (see Sect. 4.4). The second mitigating factor is that both the RETRAN analyses by ORNL and calculations reported in a proprietary study by C-E showed that if such a problem did exist, it would be limited to a very small range of break sizes, thus decreasing its likelihood.

Among the areas of somewhat less concern, deserving at least brief documentation, are the following two items:

1. A turbine trip signal is generated by two out of four SG high level signals. A trace of the logic shows that the two-out-of-four logic channels funnel ultimately into the equivalent of a single OR gate whose failure could defeat the trip on this parameter. (The OR "gate" consists of multiple independent components, but it controls a single relay.) It is likely, however, that such an overfill would have other dynamic consequences that would lead to a turbine trip by another parameter.

2. There appear to be four valves in the component cooling water circuit, any one of which failing closed would lead to a cutoff of cooling water to the reactor coolant pump seals. Such a condition, prolonged for a time of the order of minutes, could lead to seal failures that would be classified as SB-LOCAs. Such events are bounded by SB-LOCA events in the FSAR.

Numerous other possible failures, detailed in Sect. 4, might lead to a SB-LOCA, but they are bounded by cases presented in the FSAR.

Results of the augmented FMEAs--simulator analyses of sequences of particular interest--are given in Sect. 6. Results are reported for the RETRAN study of postulated SG overfill and dryout scenarios, and SB-LOCAs. A backup simulation utilizing the modular modeling system (MMS) was also developed for the Calvert Cliffs-1 Plant and is operational, but results were neither required nor available in time to be included in this report.

Estimates of frequency of occurrence for the significant sequences identified in the SICS study are presented in Sect. 5. The estimate for the critically sized SB-LOCA leading to insufficient core cooling was less than one event every 100,000 reactor years, while the estimated SG overfill was about one per 100 reactor years.

Other significant results in this report include the finding that the plant design is such that failures in both the plant electrical systems and plant instrument air systems, because of the built-in backups, are unlikely to cause major problems with plant operation or the ability of the operators to bring the plant to a safe shutdown condition. Although some postulated instrument failures led to temporary loss of all instrument air, the affected area could be isolated by proper operator action and the air supply to the rest of the system restored. Only in the case of some postulated header breaks was the problem area found to be unisolable. In one interesting and complex postulated sequence following a LOCA, however, a situation may arise where automatic isolation of the service water system could result in failure of the instrument air and containment air supplies.

Other results presented include an analysis of plant operating experiences germane to the SICS project. This review centered on Calvert Cliffs-1 but also derived data from Unit 2 and the other operating C-E plants. The operating history of Calvert Cliffs is generally similar to other plant sites (except those that have had serious problems, such as the Three Mile Island-2 core melt and the Browns Ferry fire). Of the two types of sequences identified as being of significant SICS concern, no events at Calvert Cliffs could classify as SB-LOCAs, and only one event at another C-E plant could; also, three SG overfeeds at Calvert Cliffs resulted in high-level trips of the turbine and reactor. However, with the possible exception of the overfeed event due to a MFW regulating valve failure at Calvert Cliffs-2, none progressed to anywhere near a serious situation and should be considered only as precursors to sequences of concern. This SG overfeed event at Calvert Cliffs-2 involved a mechanical failure in a MFW regulating valve that required prompt operator attention to prevent overfill. Also, 11 cases of SG low-level trip occurred at Calvert Cliffs (mostly during startup), and again, although no serious problems resulted, these challenges to the auxiliary feedwater (AFW) system can be classified as possible precursors to potential dryout or overheating sequences. A rough estimate of the frequencies involved may be derived from noting that these are approximately the total of such events (there may have been others, depending on the completeness of the reporting systems) that occurred in 19 plant years of Calvert Cliffs operation and 88 plant years of operation of all C-E plants. Two other events of particular interest to SICS were the loss of the service water system due to an air compressor after-cooler leak, and a flooding event that affected control and safety system operation. Analyses of the whole spectrum of Licensee Event Report (LER) events at C-E plants (and the power reactor industry in general) have shown that those related to maintenance and testing problems have resulted in the most frequent challenges to the plant protection systems (PPSs). Improvements in procedures, on-line testing

systems, and man-machine interface and communications systems (particularly in this plant, where so much of the control is manual) are recommended to reduce the frequency of PPS challenges.

One area of study not covered in this report but included in the A-47 TAP is the effects of external events such as earthquake, fire, flood, and sabotage. Due to the fact that the SICS Program is terminating, there are no specific plans to consider either these or the other recommended followup items.

2. INTRODUCTION

2.1 BACKGROUND

The SICS Program at ORNL was initiated in June 1981. The purpose of this program is to conduct research on light water reactor (LWR) safety concerns related to USI A-47. USI A-47 addresses the general problems of compromises to plant safety as a result of failures or malfunctions of control systems. Such failures may drive the plant into unsafe conditions outside the envelope of plant protection, may interact with and fail elements of the plant protection system, or may increase the probability of failure through frequent challenges to the plant protection and other safety systems. In the context of this study, "control systems" constitute a far broader set than sensors and electronic logic elements. For the purposes of SICS, control systems comprise all operational equipment and personnel whose functioning can affect the dynamics of the plant. Thus this category includes plant operators as well as pumps, valves, motors, rod drives, heaters, power sources, and the sensors, controllers, and actuators that control their operation.

This report on SICS is the second of two by ORNL incorporating detailed analyses of specific plants. The first was a study of the Oconee-1 reactor, and is reported in ORNL/TM-9444.[1] The three Oconee units are Babcock and Wilcox (B&W) PWRs owned and operated by Duke Power Co. The current study is an investigation of SICS concerns at Calvert Cliffs-1, one of two 850-MW(e) C-E PWR units owned and operated by BG&E. In addition to the usual internal reviews, the May 31, 1985 draft of this report was reviewed by NRC, BG&E, and several subcontractors working on the ORNL SICS program, including C-E, the reactor vendor. Their comments, suggestions, and corrections were incorporated into this final version where appropriate.

The Calvert Cliffs and Oconee plants are similar in that they are PWRs of about the same vintage. Oconee-1 began commercial operation in 1973 and Calvert Cliffs-1 began in 1975. Their most important differences, for the purposes of this study, are that they have different types of SGs (once-through at Oconee, U-tube at Calvert Cliffs), and different control philosophies. Oconee's once-through steam generators (OTSGs) respond faster and have much less secondary water inventory than do the Calvert Cliffs U-tube steam generators (UTSGs). The OTSGs also produce superheated steam and do not have steamwater separators. The faster response of the OTSGs (as well as thermal-hydraulic design features of the B&W core) enable the B&W plants to follow electrical load demand changes more readily than the C-E plants. Because of this, however, it is necessary for B&W plants to use a more extensive automatic control system. In contrast, several of the major control parameters in the C-E plants, such as reactor power and steam flow to the high-pressure turbine (HPT), are under manual (operator) control. In effect, this design makes the Calvert Cliffs operators an integral and much more crucial part of the control systems factored into the SICS study.

Another significant difference in plant design that figures into a dominant accident sequence, the SB-LOCA, is that the Calvert Cliffs Plant has a much lower pressure HPSI system for emergency cooling (1275 psia versus 2800 psia for Oconee).

The ORNL SICS Program is closely related to a similar program at Idaho National Engineering Laboratory (INEL). The INEL program charter is similar, and its scope includes a Westinghouse PWR and a General Electric boiling water reactor (BWR). Results of the INEL studies are reported in refs. 2 and 3. The ORNL SICS Program was coordinated with another USI research effort at ORNL, USI A-49, known as pressurized thermal shock (PTS). This coordination consisted of information exchanges and occasional joint meetings of program management staff. An additional staff person was assigned the task of overseeing the coordination. The PTS program has also studied Oconee-1 and Calvert Cliffs-1.[4,5] The Calvert Cliffs Plant was also the subject of another PTS study performed by Electric Power Research Institute (EPRI) on the small steam line break scenario.[6] Another NRC-sponsored program at ORNL that evaluates system interactions (USI A-17) provides useful analyses and surveys of operating plant histories, some of which relate to SICS.[7]

The SICS Program is sponsored by the NRC Division of Engineering Technology in the Office of Nuclear Regulatory Research (RES). The NRC Project Manager for this program is Demetrios L. Basdekas.

2.2 OBJECTIVES

The major objective of the ORNL SICS Program is to provide technical support to the NRC for their task of resolving USI A-47. Primary guidance for this task is provided by the A-47 TAP.[8] The resolution involves reviews of nonsafety-grade control systems for selected plants (one for each LWR vendor) to assure adequate separation from the safety systems and to demonstrate that the effects of failure of these nonsafety systems do not lead to accidents that are not already bounded by the FSAR design-basis accidents. The TAP further states that resolution of A-47 may be accomplished by performing ". . . an in-depth evaluation of the control systems that are typically used during normal plant operation and <verifying> the adequacy of current licensing design requirements or <proposing> additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent nonsafety grade control system failures."

The definition of "unacceptable risk" as a criterion for considering (or not) a given postulated accident sequence is subject to a variety of interpretations. In general, the loss of a control system or power supply will result in some loss of process control and/or information available to the operator. In most cases, however, the operator will still have to bring the plant to a safe shutdown condition. The criteria for sequences to be considered by this study call out those sequences which (1) significantly impede, delay, or defeat a plant protection system action; (2) cause the transient to exceed the bounds

of those accidents defined as design basis in the FSAR, or (3) cause "excessively frequent" challenges to the safety system. The definition of what constitutes excessively frequent challenges depends on the particular system(s) being challenged and on some engineering judgment. For example, if a safety system is being challenged at a rate much greater than that of the industry average, there are clearly design, operator training, and/or maintenance problems that should be addressed. If the safety system being challenged has shown a history of problems in responding properly, the definition of excessive frequency should be more restrictive.

The ORNL contribution to A-47 resolution consists of two detailed plant-specific investigations that are, to the extent possible, to be used to arrive at generic criteria and solutions to overall safety concerns.

The limitations of the study, which were imposed to keep it to a manageable size, are defined in the following ground rules:

1. Single failures. Because of the very large number of control systems in a PWR, the number of situations encompassed by arbitrary combinations of multiple failures would be extremely large. Hence only single failures are considered in a systematic fashion; however, multiple failures are included in the study if they are found to be "interesting" or logical follow-ons of a particular scenario. What is generally looked for is the minimum number or most likely combination of component failures that would be required to generate, perpetuate, or exacerbate the accident scenario of interest. The likelihood of double or multiple failures can be assumed to be high enough to be of interest if one or more of the failures can be categorized as potentially undetected, (i.e., if they could exist for sufficient periods of time without detection, or if they can be assumed to be due to the loss of a common power supply or to another common precipitating event).

2. Operator action. In general, operator inaction or misaction (i.e., doing the wrong thing) is to be considered if the information presented the operator is misleading, confusing, or insufficient, or if the time available to accomplish the required task is short compared to what is considered to be a reasonable amount of time (or compared to what NRC has mandated as a minimum allowable response time).

3. Event categories. Primarily, SG overfeed or dryout and core undercooling or overcooling events will be considered. (This is a ground rule of the TAP.) The terms SG overfeed and SG overfill require more definition. In the current study, overfeed refers to situations in which the feedwater (FW) supply is significantly in excess of the requirements due to a malfunction or misoperation, while overfill refers to the cases where the SG level is high enough to cause liquid to be carried into the steam lines. If other significant problems are uncovered, however, they are pursued.

4. Power supplies. Loss of power supplies (ac, dc, and instrument air) are considered.

2.3 APPROACH

In both the Oconee and Calvert Cliffs studies, the FMEA technique was employed. FMEA is a standard technique used to make systematic, qualitative searches for significant failures and consequences. The FMEA process, as it is adapted to this program, consists of identifying a failure class (such as reactor undercooling) and then defining broad functional conditions that must occur to lead to this failure. Each control system is examined, noting its possible modes of failure and their effects on the event in question. This examination leads to the identification of the effects of postulated system failures and determines the subsystem malfunctions that can give rise to those failures. This process has been referred to as the "broad FMEA." Certain sequences will be identified as being of major interest and, if not fully resolved by the broad FMEA, require computer simulation for further study. This part of the study is called the "augmented FMEA." Other sequences of interest come to light by reviewing operating experiences or by exercising the plant simulators.

Figure 2.1, "Program flow for study of safety effects of nuclear power plant control system failures," was generated originally for the Oconee-1 SICS report but applies also to the present study. It may be useful for understanding the processes by which each postulated failure is considered and then either discarded or carried through to the final step of recommending corrective action.

2.4 REPORT ORGANIZATION AND CONTENTS

The FMEA process by nature requires many detailed investigations, all with complete documentation. A majority of the cases examined do not lead to safety-related scenarios of interest; the results are reported only to justify their exclusion from further consideration. Also, of the failures that are of concern, a group of similar events may require detailed attention for only the most extreme, or bounding, case. To avoid burying the important results within a large mass of less significant data, much of the detail is relegated to appendices, which will be published in Vol. 2 of this report. There the background information, details of the procedures used for selecting systems for analysis, system descriptions, and FMEA tables can be found. This descriptive material is essential to an understanding of the FMEA processes, since selection or rejection of postulated component failures is crucially dependent on the analyst's understanding of the impact of each component failure on its own and neighboring subsystems as well as on the overall plant.

In the main body of the report, the rationale, process, and results of the task of selecting the systems pertinent to the SICS study is given

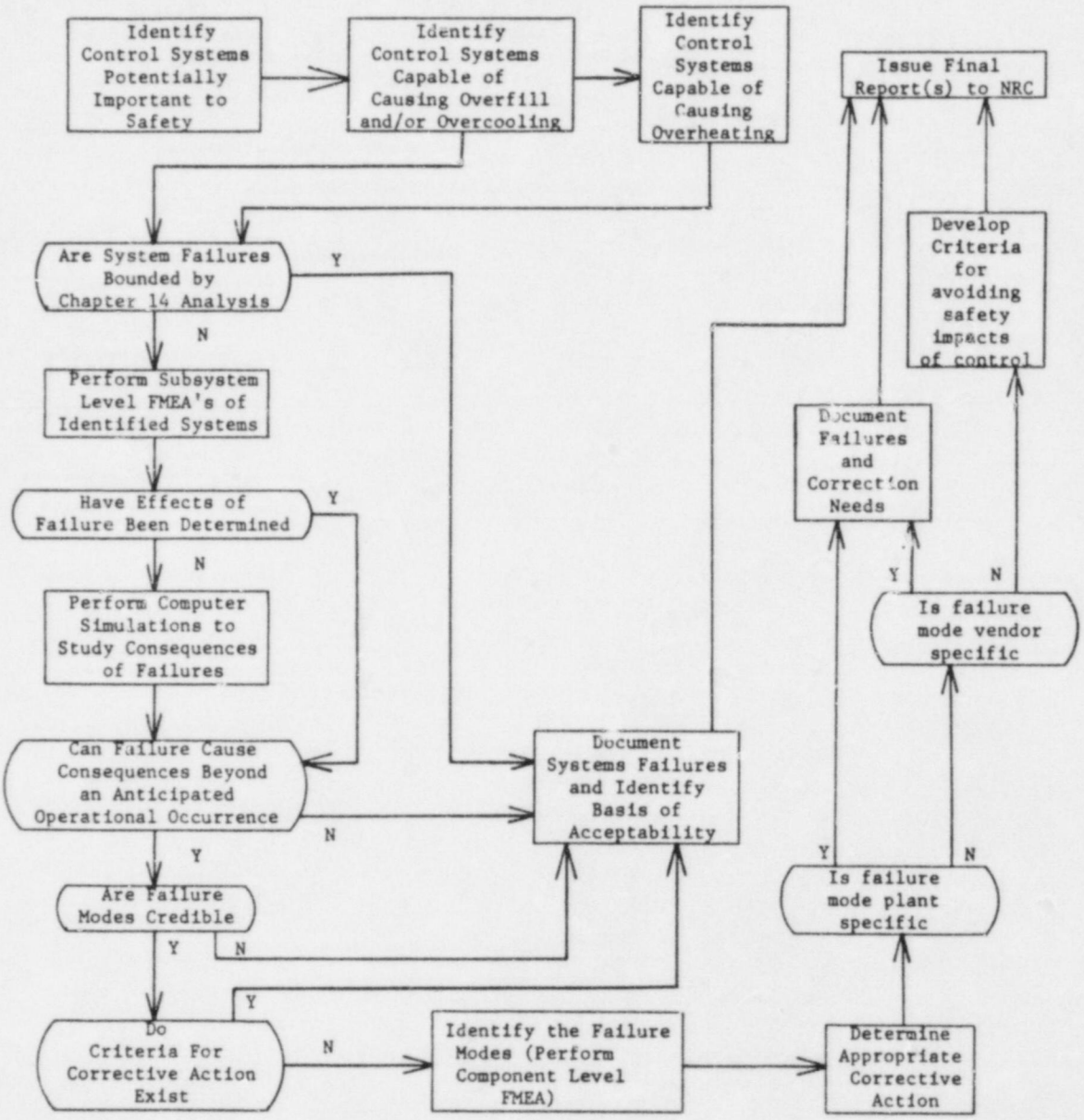

Fig. 2.1. Program flow for study of safety effects of nuclear power plant control system failures.

in Sect. 3.1. A survey and analysis of relevant plant operating experiences, which help to link the postulated FMEA-generated failures and transients with "reality," are in Sect. 3.2. This study includes data on the two Calvert Cliffs units as well as on other C-E plants. Section 4 contains the major results of the broad FMEA. Here all of the control system failures considered to be significant are identified and described. The methodology is given in Sect. 4.1, and Sect. 4.2 elaborates on the sequences. Section 4.3 summarizes the most important sequences found to be of interest to the Calvert Cliffs SICS study, and is the section giving the most pertinent detailed descriptions of the major findings. Section 4.4 is a brief discussion of the identification of operator effects, including a discussion of the possible applicability of the "confusion matrix" technique to this type of investigation. Section 4.5 describes how the plant electrical system FMEA ties in to the other analyses, and outlines the most important conclusions from that work. Section 4.6 is a similar write-up on the instrument air system. Section 4.7 discusses the applicability of the results of the Calvert Cliffs-1 study to the other C-E plants, and how combinations of identified failures are treated. Major findings from these results are summarized briefly in the Executive Summary (Sect. 1.4). A somewhat more detailed summary is given in the Results and Conclusions (Sect. 7).

Sequence frequency quantification (Sect. 5) describes the probabilities associated with the important sequences identified in the SICS study. Also noted are some tie-ins to Calvert Cliff and other C-E plant operating experiences which give indications of approximate probabilities for precursors or initiating events, at least for the relevant sequences reported.

Section 6, the augmented FMEA section on thermal hydraulic analysis, discusses the two alternate Calvert Cliffs simulators, RETRAN and the MMS. The RETRAN model version of Calvert Cliffs-1 is based on a proprietary RETRAN input deck obtained from BG&E and expanded to include features deemed necessary for the present study. The MMS simulation currently has a less versatile model of the plant than does RETRAN (e.g., it is not set up to simulate SB-LOCA scenarios); however, its flexibility is expected to be of benefit for any future scoping studies. Brief descriptions of the simulation models are included. Results of RETRAN runs for SG overfill and dryout sequences and for selected SB-LOCA scenarios are presented.

Results and conclusions, recommendations for resolution of A-47, and recommendations for future work in SICS-related areas are presented in Sects. 7, 8, and 9 respectively.

Five appendices are contained in Volume 2 of this report. Appendix A gives details on selection of the systems for analysis, Appendix B gives detailed descriptions of all the plant systems of interest to the SICS study, and Appendix C gives detailed FMEA tables for each system. Appendix D is a separate report on plant electrical system FMEAs, and

Appendix E documents ORNL's responses to BG&E comments on the May 1985 draft of this report. The authors appreciate BG&E's thorough review of this report. Their comments and criticisms helped improve its technical accuracy.

3. CALVERT CLIFFS NUCLEAR POWER PLANT SYSTEMS AND OPERATIONS

The Calvert Cliffs Nuclear Plant, operated by BG&E, has two identical PWR units, each rated at 845 MW(e) [2700 MW(t)], with a nuclear steam supply system (NSSS) supplied by C-E. Unit 1 has been in operation since October 7, 1974, and Unit 2 since November 30, 1976, for a total of almost 19 reactor years of operating experience at Calvert Cliffs. Each unit has two SGs of the U-tube type with four centrifugal reactor coolant pumps, two pumps (and two cold legs) per SG. The main steam system for each unit includes four 1800-rpm tandem compound axial flow turbines--one high-pressure turbine and three low-pressure turbines.

Feedwater for each unit is supplied to the SGs by two turbine-driven main feed pumps operating in parallel at a rate of 15,000 gpm. The SG steam side volume is relatively large compared with Westinghouse and B&W designs, holding a nominal water inventory of 137,000 lb at full power. At full power, the steam side is typically operated at 850 psia and 525°F. Secondary side pressure is controlled by turbine loading or four turbine bypass valves and two atmospheric dump valves per unit, one atmospheric dump valve on each main steam line. Eight safety relief valves on each steam line (a total of 16 per unit) provide pressure relief backup. The four turbine bypass valves together can pass 40% of full power steam flow, and the two atmospheric dump valves can relieve 5%

The primary side, which mainly consists of the reactor vessel and core and the tube side of the SGs typically operates at 2250 psia. Reactor coolant is circulated by the reactor coolant pumps through the core and the two SGs at a nominal rate of 61 million lb/h/SG, where the heat generated in the core is transferred to the secondary side fluid. Reactor coolant entering the SGs is typically at 600°F and is returned to the core through the cold legs at 548°F. A single 1500-ft^3 pressurizer is connected to one of the two hot legs by a surge line. Reactor coolant system (RCS) volume and pressure are maintained by control of the pressurizer parameters. The pressurizer is equipped to protect the RCS from overpressure with two power-operated relief valves set to open at 2385 psig and two spring-loaded safety relief valves set to relieve at 2485 and 2550 psig.

The plant is equipped with many systems for power operation and plant safety. Major systems tied to the primary side include a reactor protective system to initiate reactor trip, a control element drive system, a chemical and volume control system to provide makeup water to the RCS, a nuclear instrumentation system, and regulating systems. Seven regulating systems provide the signal processing and control functions required for operation of the NSSS. These systems provide information and controls for reactor regulation, control element drive position, reactor coolant pressure, pressurizer level, MFW flow to the SGs, atmospheric steam dump and turbine bypass valves, and steam flow to the HPT.

Reactor safeguards are initiated by the engineered safety features actuation system (ESFAS), which initiates safety injection on the primary side and AFW on the secondary side, when required, as well as other safeguard functions such as containment isolation. Plant containment systems include the actual containment structure, a containment air recirculation and cooling system, a purge system for hydrogen removal, containment spray for cooling and post accident iodine removal, and containment penetration room ventilation control.

Process auxiliaries provide hydrogen and nitrogen gas; sampling; radiation monitoring; waste processing for reactor coolant wastes, gaseous wastes and solid wastes; reactor component handling during refueling; spent fuel storage and cooling; plant and instrument air; and process cooling water. Other plant auxiliaries include fire protection, plant communications, and plant ventilating systems.

The cooling water systems at the plant include the salt water cooling system, the service water system, the component cooling system, and the circulating water system. The salt water cooling system provides the ultimate heat sink for the service water and component cooling water (CCW) systems. The circulating water system, also a salt water system, cools the main condenser. The service water system, a two-train redundant system, removes heat from turbine plant components, the containment coolers, the spent fuel pool, and the emergency diesel generators (DGs). The component cooling system cools the reactor coolant pumps, the high- and low-pressure safety injection pumps, and the sample coolers. It also provides shutdown cooling and generally serves as the intermediate cooling system and barrier between radiological reactor auxiliary systems containing radioactive fluids and the salt water cooling system. The CCW system is designed with redundancy, but its two trains are not isolated.

The main power for the Calvert Cliffs Station is supplied by two separate 500-kV/13.8 kV plant service transformers connected to the 500-kV switchyard. Plant backup is provided by another 13.8-kV supply through a high-reliability 69-kV/13.8-kV transformer from the Southern Maryland Electric Cooperative System. Power from the Unit 1 and Unit 2 generators at 25 kV and 22 kV, respectively, is fed to the main unit transformers and out to the 500-kV switchyard buses. Either 500-kV bus can supply loads for both units. The 13.8-kV system powers the reactor coolant pump loads and the 4-kV distribution systems via two 13.8-kV service buses. Separation of unit loads and redundant safety buses is provided at the 4-kV level. Three DGs supply the plant emergency loads to the safety-related buses, with one of the three shared between Units 1 and 2. Plant dc loads are supplied through four independent and isolated channels, each equipped with batteries and two battery chargers. The four dc channels are shared between the two units. Each channel powers two vital 120-V ac instrument buses, one per unit, through static inverters. The vital buses power essential instrumentation and reactor protection circuits. They can also be supplied from the 480-V ac motor control centers (MMCs) through transformers. In addition, a battery-backed 250-V dc bus and a reserve 125-V dc bus are shared by the two units.

A complete list of Calvert Cliffs systems is provided in Appendix A (Vol. 2 of this report). This list was developed as a basis for the identification and selection of systems pertinent to the scope of this analysis (safety implications of control systems). The selection and identification process is summarized in Sect. 3.1. More detailed system descriptions of the systems selected for detailed analysis are provided in Appendix B in Vol. 2 of this report. Additional information is provided in the Calvert Cliffs FSAR[9] and the various BG&E system descriptions.

Section 3.2 highlights the plant operating experiences pertinent to this analysis.

3.1 IDENTIFICATION AND SELECTION OF SYSTEMS PERTINENT TO SICS

A primary task of the control systems analysis is to perform FMEAs on plant systems to develop accident scenarios for simulation. Performing detailed FMEAs on the large number of systems in a nuclear power station is not practical. Therefore, a method is required to (1) identify all Calvert Cliffs systems, and (2) systematically select those control systems requiring FMEAs. The methodology must also provide a means of tracking and reevaluating systems not selected for FMEA to ensure completeness.

3.1.1 Selection Methodology

The methodology developed to identify and select plant systems for analysis is depicted in Fig. 3.1. The method was implemented in six basic steps:

1. Identify and list all Calvert Cliffs systems.
2. Exclude and list systems beyond the scope of the control systems analysis.
3. From the balance of systems, select and list for FMEA all systems having a direct interface with the RCS (including the RCS itself). These systems make up the primary RCS interface systems.
4. From the balance of systems, select and list for FMEA all systems having a direct interface with any of the primary RCS interface systems. These systems make up the secondary RCS interface systems.
5. From the balance of systems, select and list for FMEA all systems having a direct interface with safety systems. These systems make up the safety system interface systems.
6. Compile and reevaluate all systems not selected for FMEA. Based on the reevaluation, additional systems may be selected for FMEA.

The first task, identification of Calvert Cliffs systems, is basic to subsequent control systems analyses. Two principal sources of information were used to identify the plant systems, a generic PWR plant systems list[9] and the Calvert Cliffs FSAR.[10] The method used to identify systems employed the generic systems list as a base. The specific Calvert Cliffs systems with functions analogous to each of the

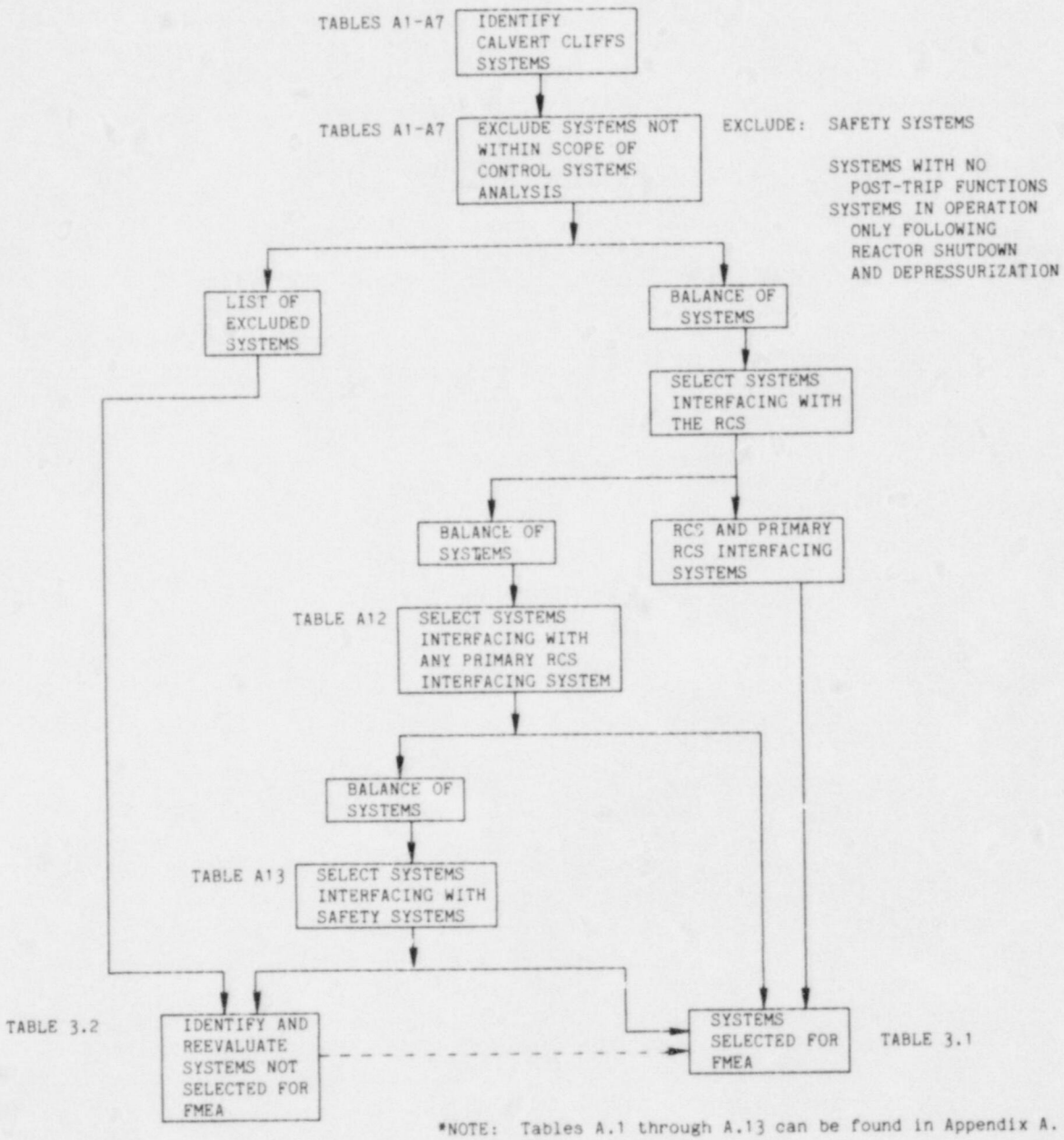

Fig. 3.1. System selection methodology.

generic systems were then identified, primarily from the FSAR descriptions. In this way all generic PWR system functions would have an identified Calvert Cliffs Plant system, or the omission could be identified and resolved using supplementary information. In a similar manner, the identified Calvert Cliffs systems were compared to the systems described in the FSAR to ensure that all systems and functions of importance were included.

Once the Calvert Cliff systems were identified, the functions of these systems were evaluated to narrow the number of plant systems to the specific scope of the plant control systems analysis. In this way the analytic effort could be focused on plant control systems analyses, minimizing analyses that would be duplicated in other programs in progress. The systems not considered within the program scope included the following:

1. Standby safety systems: Standby safety systems have been evaluated extensively in other programs, and the study of their failure modes in this control systems analysis would be redundant. However, safety qualification of a system is insufficient basis for exclusion; therefore, safety systems performing a control function were included in the analysis. Furthermore, the response of safety systems to transients initiated by control system failure were considered because identifying control system failures that degrade safety functions is a major objective of the program.

2. Systems isolated by reactor trip: During power operation, the plant systems are controlled within specified parameter limits. If these limits are exceeded, a reactor trip will be initiated. Failure to trip (failure of a standby safety system) is being studied as part of the Anticipated Transient Without Scram (ATWS) Program and will not be considered in this analysis. Once the reactor is tripped, some plant systems are isolated and cannot affect the course of the posttrip transient [e.g., the control element drive (control) system]. Since a reactor trip transient is not itself of concern in this analysis, systems isolated following reactor trip were not evaluated in the control systems analysis.

3. Shutdown systems: Certain Calvert Cliffs Plant systems such as the residual heat removal system shutdown cooling system and reactor refueling equipment are manually placed in service following shutdown and depressurization of the reactor. The residual heat removal systems are being evaluated in other analysis programs. Since these shutdown systems would not be placed in service in response to control system-induced transients, their failure modes were not evaluated in this program.

The above evaluation divides the Calvert Cliffs systems into two categories: systems excluded for the specific reasons listed above, and the balance of plant systems. Failures in the systems included in the balance of systems list have the potential to affect plant transients to

varying degrees. These systems were next evaluated to assess their potential to affect RCS overcooling, RCS undercooling, SG overfill, or the performance of safety systems.

The balance of systems list is categorized based on an evaluation of the functional interfaces of each system. The potential to affect RCS undercooling or overcooling was evaluated first by selecting the systems having a direct interface with the RCS. These are the primary RCS interface systems. In addition, a second evaluation was made to identify those systems not included in the primary interface systems list but having an interface with a primary RCS interface system. These systems are the secondary RCS interface systems.

The potential for affecting safety system performance was also evaluated based on functional interfaces. Systems not included as a primary or secondary RCS interface system were selected for analysis if an interface with a safety system could be identified.

From the lists of selected and nonselected Calvert Cliffs systems, two categories developed: a list of systems to be analyzed further and a list of systems not selected. The systems to be analyzed consist of the primary and secondary RCS interface systems and the safety system interface systems. The nonselected systems include all others: those excluded based on specific program scope definitions and those having no identified primary RCS, secondary RCS, or safety system interface.

The final analysis in the system selection process is the reevaluation of nonselected systems. Each of the nonselected systems was individually reevaluated to assess whether it could impact RCS overcooling, undercooling, or safety system performance on some other basis (e.g., a particularly important tertiary RCS interface). In addition to the initial qualitative reevaluation, the list of nonselected systems may be reevaluated at any time based on the results of detailed systems FMEAs.

For details of system selection (intermediate results, etc.), refer to Appendix A, "Selection of Systems for Analysis."

3.1.2 Summary of Systems Selected for FMEA

Completion of the first five steps of the methodology described in Sect. 3.1.1 results in the selection of 35 systems and the exclusion of 36 systems. A list summarizing the systems selected for FMEA and the criteria used in selecting them is provided in Table 3.1. A list summarizing the systems eliminated from further analysis and the basis for their elimination is provided in Table 3.2.

Systems selected for system-level and component-level FMEA include those which have a direct interface with the RCS, those which interface with a primary interface of the RCS, and those which interface with safety systems.

Table 3.1. Summary of Calvert Cliffs systems selected for FMEA

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Selection
N04	Reactor Coolant System (RCS)	Response of RCS provides the basis for evaluating control system failures
N04.A (and N09.B)	Reactor Regulating System	Direct RCS interface, part of RCS, establishes pressurizer level setpoint
N04.B (and P03.B)	Reactor Coolant Pressure Regulating System	Direct RCS interface, part of RCS
N09 (and N05)	Chemical and Volume Control System (CVCS)	Primary RCS interface
N09.A	Pressurizer Level Regulating System	Primary RCS interface, controls flow to and from the RCS
N09.C	Electric Heat Tracing	Part of CVCS system, secondary RCS interface
C03 (and C08)	Containment Air Recirculation and Cooling System	Primary RCS interface, provide cooling for pressurizer components, CEDM and incontainment RCS instrumentation components
C05	Containment Purge System	Secondary RCS interface, Containment Air Recirculation and Cooling System (C03) provides cooling for purge system electrical components
C08.B	Pressurizer Compartment Cooling	Primary RCS interface, consists of ductwork used to cool the pressurizer compartment
E01 (and E07)	500 KV Switchyard and Unit Transformer	Offsite Power
E02	13,800, 4160 and 480 Volt Station Power Distribution Systems	Motive power for major plant components in selected systems
E03	125 Volt DC and 120 Volt AC Electric Power Systems	Powers selected Instrumentation systems

Table 3.1 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Selection
E06	Plant Computer	Primary RCS interface, interfaces with RCS instrumentation
P01 (and P03)	Main Steam System	Primary RCS interface, interactive interface
P02 (and P04.A)	Turbine Generator and Condenser System	Secondary RCS interface, interface with Main Steam System (P01), provides isolation of steam flow from main steam lines
P02.A	Turbine Generator Control System	Secondary RCS interface, interface with Auxiliary Control Panels (S04), S04 provides turbine trip from outside the control room
P03.A	Steam Dump and Turbine Bypass Control System	Secondary RCS interface, interface with Main Steam System (P01), provides control of steam dump
P05 (and P04.B)	Condensate and Feedwater System	Primary RCS interface, interactive interface
P05.A	Feedwater Regulating System	Primary RCS interface, interactive interface
P07	Steam Generator Blowdown System	Primary RCS interface, due to interface with steam generators
P08	Auxiliary Boiler Steam System	Secondary RCS interface with Condensate and Feedwater System (P05) following plant shutdown. Safety system interface with Safety Injection System (S03), provides plant heating which heats refueling water storage tank

Table 3.1 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Selection
W01.A	Waste Gas Processing System	Secondary RCS interface, interface with CVCS (N09) due to intermittent venting of volume control tank
W01.B1 (and W04.A)	Reactor Coolant Waste Processing System	Secondary RCS interface, interface with CVCS (N09), reactor coolant is diverted from CVCS for processing
W01.B2	Miscellaneous Waste Processing System	Secondary RCS interface, interface with Steam Generator Blowdown System (P07), processes blowdown
W01.C	Solid Waste Processing System	Secondary RCS interface, interface with CVCS (N09), provides intermittent disposal for CVCS spent resins
W02	Radiation Monitoring System	Secondary RCS interface, interface with Steam Generator Blowdown System (P07), monitors blowdown radiation and isolates blowdown line
W03.A	Component Cooling Water System	Primary RCS interface, cools RCS components
W03.B	Service Water System	Secondary RCS interface, interfaces with Condensate and Feedwater System (P05), Containment Air Recirculation and Cooling System (C03), and others
W04.B	Salt Water Cooling System	Secondary RCS interface, interface with component cooling water system (W03.A), provides heat sink for CCW
W07.B	Instrument Air System	Secondary RCS interface with CVCS (N09), required for operation of CVCS valves

Table 3.1 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Selection
W08	Sampling System	Primary RCS interface
W09.A	Hydrogen Gas System	Secondary RCS interface with CVCS (N09), provides H_2 to RCS makeup
W09.B	Nitrogen Gas System	Safety system interfacing system, provides nitrogen for SI accumulators
X05.B1	Turbine Building Ventilating System	Secondary RCS interface with Condensate and Feedwater System (P05) provides Cooling for Turbine Building Electrical Components
X05.D	Auxiliary Building Ventilating System	Safety system interfacing system, believed to provide cooling to CVCS (N09) components

*See Appendix A.

Table 3.2. Summary of Calvert Cliffs systems not selected for FMEA

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Non-Selection
N01	Reactor Core	Out of program scope since it is a safety system
N02	Control Element Drive Mechanisms (CEDM)	Do not influence transients following reactor trip
N03	Control Element Drive Systems	Do not influence transients following reactor trip
N06	Reactor Protective System (RPS)	Out of program scope since it is a safety system and has no function following reactor trip
N07	Nuclear Instrumentation System (NI)	Out of program scope since the NI has no function following reactor trip
N08	Shutdown Cooling System	Out of program scope since the system is only used following plant shutdown and depressurization
S02	Engineered Safety Features Actuation System (ESFAS)	Out of program scope since the system is a safety system
S03.A	High Pressure Safety Injection Subsystem (HPSI)	Out of program scope since the system is a safety system
S03.B	Safety Injection Tanks	Out of program scope since these tanks are part of a safety system
S04	Auxiliary Control Panels and Other Local Control Panels	Considered a safety system
S03.C	Low Pressure Safety Injection Subsystem (LPSI)	Out of program scope since the system is a safety system
S05	Auxiliary Feedwater System (AFS)	Out of program scope since the AFS is a safety system
C02	Containment Structure	Out of program scope since the containment structure and penetrations are safety systems

Table 3.2 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Non-Selection
C04	Containment Isolation System	Out of program scope since the Containment Isolation System is a safety system
C07.A	Electric Hydrogen Recombiner	Out of program scope since post accident hydrogen control systems are safety systems
C07.B	Hydrogen Purge System	Out of program scope since post accident hydrogen control systems are safety systems
C08.A	CEDM Cooling System	Do not influence transients following reactor trip
C10.A	Containment Spray System	Out of program scope since system is a safety system
C10.B	Containment Iodine Removal System	Out of program scope since system is a safety system
C11	Containment Penetration Room Ventilation System	Out of program scope since system is a safety system
E04	Emergency Diesel Generators	Out of program scope since emergency power systems are safety systems
P06	Circulating Salt Water Cooling System	System has no primary or secondary interface with the RCS and no interface with safety systems. It does interface with Turbine Generator and Condenser System (P02), and this is a tertiery RCS interface
W05	Reactor Component Handling Equipment	Out of program scope since equipment only operates during cold shutdown

Table 3.2 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Non-Selection
W06	Spent Fuel Storage System	System has no primary or secondary interface with the RCS during power operation and no interface with identified safety systems
W06.A	Spent Fuel Pool Cooling System	System has no primary or secondary interface with the RCS during power operation and no interface with identified safety systems
W07.A	Plant Air System	System has no primary or secondary interface with the RCS and no interface with identified safety systems (Note: Plant air compressors backup the function performed by the instrumentation compressors)
X02	Fire Protection System	System has no primary or secondary interface with the RCS and no interface with identified safety systems
X03	Plant Communications System	System has no primary or secondary interface with the RCS and has no interface with identified safety systems. Although formal FMEA of the plant communication systems is not considered necessary, the importance of communication in post-accident recovery is recognized, as discussed in Section 3.2.
X05.A (and X05.D1)	Control and Cable Spreading Rooms Ventilating System	Out of program scope since system is a safety system
X05.B2	Auxiliary Feedwater Pump Room Emergency Cooling System	Out of program scope since system is a safety system

Table 3.2 (continued)

Calvert Cliffs System ID*	Calvert Cliffs System	Reason for Non-Selection
X05.C (and X05.D4)	Diesel Generator Rooms Ventilating System	Out of program scope since system is a safety system
X05.D2	Access Controlled Area Ventilating Systems	Systems have no primary or secondary interface with the RCS and have no interface with identified safety systems
X05.D3	Switchgear Rooms Ventilating System	Out of program scope since system is a safety system
X05.D5 (and X05.E)	Spent Fuel Pool Ventilating System	System has no primary or secondary interface with the RCS and has no interface with identified safety systems
X05.D6	Radwaste Area Ventilating System	System has no primary of secondary interface with the RCS and has no interface with identified safety systems
X05.D7	ECCS Pump Room Ventilating System	Out of program scope since system is a safety system

*See Appendix A.

3.2 PLANT OPERATING EXPERIENCE

3.2.1 Introduction

Interest in process control system performance and safety implications for nuclear power plants has been extant for some time. Some component faults and/or failures have on occasion triggered sequences of occurrences that have resulted in reactor transients, some requiring safety system intervention. A study of plant operating experiences relevant to SICS has two purposes. First, such a study may uncover or suggest sequences of interest not detected by broad FMEA or simulator exercises. Second, some rough idea of the probabilities of the major sequences or sequence precursors may be derived from the rate at which control system malfunction events have occurred.

Operating experiences for Calvert Cliffs Units 1 and 2 were reviewed to identify and place in perspective possible significant events pertinent to the RCS. Special attention was given to system overfill/overcooling and underfill/undercooling experiences that had significant implications for reactor safety. Also noted were related man-machine events, some of which required special mention and a few others that appeared generic in safety significance and that could have happened in any plant. These are all noted to provide another data source for FMEA modeling and analysis.

Information was collected from readily available operating experience reports, LERs, regulatory documents, and three data bases: (1) Sequence Coding and Search System Database for LERs, (2) NSIC file on the DOE RECON System, and (3) Nuclear Power Experience and Data Source, by S. M. Stoller Corp. The period reviewed for the two units at Calvert Cliffs was from initial operation through early 1985. The data banks were reviewed first for unit transients and scrams, second for manual trips, and then for other events significant to this report (see Tables 3.3, 3.4, and 3.5). Loss or impairment of systems or subsystems for various reasons were examined for significance, collated, and analyzed for impact on power plant safety. A scan of similarly acquired data for the other C-E plants was then made for the purpose of uncovering trends and generic or common problems. A brief discussion of observations and comments follows.

3.2.2 Calvert Cliffs Units 1 and 2

Our review of operator errors that produced transients in the control of the reactor indicated that Calvert Cliffs appeared to have more than the industry average. This is probably due to the fact that many of the major parameters are under manual (operator) control. In effect, this makes the Calvert Cliffs operators a much more crucial part of the control systems and results in their actions being factored into the SICS study. One manifestation of this occurs at low power (i.e., either during startup or shutdown). Many of the perturbations reviewed were loading changes at the main turbine that were caused when the operator

Table 3.3. Calvert Cliffs-1 relevant operating experiences

Date	LER	Description (cause, consequences, corrective actions)
5/23/75	75-036	FW header stop valve failed; quenching of header steam voids produced damaging water hammers. Auxiliary feedwater system procedures were modified.
8/14/75		Excessive condenser temperature rise caused by fish impingement on intake screens.
4/2/76		Failure of a surge suppressor on B phase of 11A reactor coolant pump motor (22-h forced outage).
9/5/76		Unit tripped due to false rod drop signal (16-h forced outage).
9/29/76		Trip caused by control problem resulting from malfunction of computer input circuitry (18-h forced outage).
10/13/76	76-042	Pressurizer level control and heaters lost; failure of computer control card.
4/2/77		Malfunction of turbine control system resulted in intercept valve closure (10-h forced outage).
5/2/77		Repaired vacuum trip sensing line on No. 11 feedpump turbine (8-h forced outage).
5/18/77	77-33	Azimuthal power tilt exceeded limit; power level changed at low powers. Operator error. (Similar occurrences: LERs 77-81, 77-87, 77-89, 77-90, 77-98, 77-99, 77-102, 77-103, 77-108, 77-125, 78-008, and 78-028.)
4/11/78		High SG level (16-h forced outage).
4/13/78		Electrical noise initiated spurious reactor trip (31-h forced outage).
5/11/78		Electrical noise caused spurious signal in reactor protection system (10-h forced outage).
10/10/78		13-kV circuit breaker tripped; cause unknown (14-h forced outage).
10/20/78	78-047	13-kV breaker tripped, resulting in a unit scram; cause unknown.

Table 3.3 (continued)

Date	LER	Description (cause, consequences, corrective actions)
11/16/78		Operational error while bypassing condensate filter system (4-h forced outage).
1/22/78		High water level in No. 12B FW heater (5-h forced outage).
6/4/79	79-015	Low pressure injection pump stopped; defective procedures.
7/19/79	79-020	PORV failed to close fully after lifting; PORV out of adjustment following maintenance.
7/26/79		High water levels in FW heater (17-h forced outage).
8/12/79		Low SG level (7-h forced outage).
9/6/79		Failed ΔP controller on No. 12 FW regulating valve (9-h forced outage).
10/6/79		Loss of power to No. 12 SG feed pump speed control circuit (6-h forced outage).
12/4/79	79-071	Loss of power to 500-kV bus; solid state relay card failure in circuit breaker.
2/11/80	80-007	PORV inadvertently opened; spurious signal from pressure transmitter. Technician conducting a surveillance review.
3/1/80		Loss of all circulating water pumps due to leak in No. 14 circulating water pump cooler onto the high water level trip circuitry in the intake structure (9.7-h forced outage).
3/25/80		Voltage instability on reactor trip bus (24.1-h forced outage).
4/21/80		Turbine/reactor trip due to voltage swings on motor generator sets for control element drive system (15.5-h forced outage).
4/25/80		Undervoltage to reactor trip breakers while trouble-shooting motor generator sets (13.8-h forced outage).
5/20/80	80-027	Loss of both service water system redundant trains (23.2-h forced outage).

Table 3.3 (continued)

Date	LER	Description (cause, consequences, corrective actions)
12/20/80	80-058	Shutdown cooling flow lost; breaker opened spuriously. Cause undetermined.
1/16/81		Trip caused by low SG level (8.1-h forced outage).
1/16/81		No. 12 FW regulating valve malfunctioned (16.8-h forced outage).
3/13/81		Tripped on low SG level when No. 12 FW regulating valve failed to shut due to controller problem (16.3-h forced outage).
6/14/81		Tripped due to low SG level (11.0-h forced outage).
6/30/81		Malfunction of instrument air dryers (5.4-h forced outage).
8/30/81	81-067	Tripped while performing test on reactor protection system due to loose latch arm on No. 4 breaker (21.4-h forced outage).
9/15/81		Tripped on low SG level (3.1-h forced outage). Pressurizer level deviations and RCS temperature swings caused by manual control during low power level operation. (Similar occurences: 81-040, 81-054, 81-057, 81-069, 82-037, 82-050, 82-061, 82-073, 82-079, 83-005, 83-055, 83-070, and 83-078.)
7/6/80	82-038	Reactor tripped on high SG level due to loss of No. 11 feed pump (5.6-h forced outage).
7/11/82		Tripped while conducting power-to-load unbalance test (4.6-h forced outage).
8/4/82		Tripped due to an undervoltage spike on reactor bus (28.5-h forced outage).
8/22/82		Tripped on low SG caused by loading main turbine too rapidly (8.9-h forced outage).
11/9/82	82-068	Loss of power to FW regulating valves (18.6-h forced outage).
12/8/82		Low voltage to control rods (12.8-h forced outage).

Table 3.3 (continued)

Date	LER	Description (cause, consequences, corrective actions)
3/19/82	82-010	Plant computer failures rendered in-core detector monitoring system inoperable (defective analog multiplexer card).
11/30/83	83-065	Two of four pressure transmitters on SIAS out of calibration; SI caused by environmental effects on transmitters. Transmitters will be modified or replaced.
4/15/83	83-015	Plant computer failures rendered in-core detector monitoring system inoperable (out-of-step selections of multiple analog inputs blew a fuse).
1/27/84	84-002	All eight reactor trip breakers opened simultaneously; cause unknown.
7/24/84	84-007	Power lost on a 4160-V emergency bus during testing due to operator error. Labeling on undervoltage logic modules to be improved.
8/28/84	84-009	Trip caused by imminent loss of circulating water; traveling water screens clogged with fish.
10/2/84	84-013	Trip caused by imminent loss of circulating water; traveling water screens clogged with fish.

Table 3.4. Calvert Cliffs-2 relevant operating experiences

Date	LER	Description (cause, consequences, corrective actions)
12/27/76	76-010	RCS temperature decreased; lack of operator experience.
12/27/76	76-011	Pressurizer level dropped below limit; during low power operations, the operator found it necessary to scram the reactor in order to stabilize the situation.
2/3/77	77-009	Computer inverter dc input fuse blew; actuation of computer inverter synchronization disconnect switches produced a slight phase mismatch.
4/15/77		Malfunction of a trip breaker (6-h forced outage).
4/17/77		Loss of No. 21 feedpump due to spurious thrust wear detector signal (8-h forced outage).
10/27/77	77-041	RPS high reactor power tripped unit; transient due to dropped CEA near detector (bypasses installed to permit maintenance also permitted a 2-out-of-4 trip).
12/30/77		Located and removed a ground on No. 21 battery bus that caused the generator field breaker to open (19-h forced outage).
1/3/78		A ground on No. 21 MSIV control circuit caused valve to shut (21-h forced outage).
2/2/78	78-001	MSIV closed causing reactor trip; dual grounds in the control circuitry.
2/7/78	78-002	Diesel generator tripped on generator fault; reverse power trip. During test, output of main units was increased.
2/21/78		Lost SG feed pump No. 22 due to an erroneous thrust bearing excessive wear signal (13-h forced outage).
3/14/78		While troubleshooting for a ground on No. 21 125-V dc bus, relay activation caused generator field breaker to open and unit to trip (15-h forced outage).

Table 3.4 (continued)

Date	LER	Description (cause, consequences, corrective actions)
4/11/78		Lost 500-kV bus (23-h forced outage).
4/13/78		Lost 500-kV bus (18-h forced outage).
6/26/78		Operational error while testing turbine-generator overspeed protection circuitry (14-h forced outage).
7/4/78		While channel B RPS was bypassed for calibration, a channel C 120-V transformer overheated. When several C modules tripped operator erroneously energized channel B, which resulted in a trip (143-h forced outage).
7/23/78		Speed controller failed, causing No. 22 feedpump to overspeed and trip (13-h forced outage).
8/14/78		Level control problem on No. 22 heater drain tank (18-h forced outage).
8/24/78	78-026	Azimuthal power tilt exceeded limits; power level change. Operator error. (Similar occurrences: 79-047, 81-042, 81-044, 82-009, 82-040, 83-009, 83-014, 83-055, and 83-070.)
9/14/78	78-027	CEA dropped into the core; spike in power supply. Design modification under review.
12/7/78	78-043	CEA dropped to bottom of core; spike in power supply (during surveillance testing).
3/1/79		Low water level in No. 21 SG (15-h forced outage).
5/7/79		Blown fuse on dc power to No. 21 inverter (9-h forced outage).
9/8/79		Failure of capacitor in No. 21B reactor coolant pump motor (140-h forced outage).
9/19/79		Loss of 21 MFW pump speed controller (17-h forced outage).
10/12/79		Trip during low vacuum trip test (4-h forced outage).
5/10/80		Loss of excitation to all main circulating water pumps (20.1-h forced outage).

Table 3.4 (continued)

Date	LER	Description (cause, consequences, corrective actions)
8/20/80		High pressurizer pressure when a technician inadvertently initiated SG isolation signal (5.3-h forced outage).
9/14/80	80-043	Erratic level transmitter in SI tank (27.5-h forced outage).
3/15/81		Trips due to low SG level when No. 22 FW regulating valve closed (4.8-h forced outage).
4/12/81	81-021	Reactor trip on high SG level; returning to full load from a leak in No. 21 condenser, the operator shot an excessive amount of boric acid into the reactor coolant system (169.1-h forced outage).
4/19/81		Returning from the above outage, the reactor tripped on low SG level due to problems with the turbine auto stop oil system on the No. 21 FW regulating bypass valve controller (8.1-h forced outage).
9/23/81		Main steam isolation valve No. 21 failed to open (38.8-h forced outage).
2/24/82		Reactor tripped on low SG level while trouble-shooting the automatic control circuit on No. 21 FW regulating valve; maintenance error (8.8-h forced outage).
4/17/82		Technician error caused reactor to trip when two control element assemblies dropped into the core (13.3-h forced outage).
7/14/82		Failure of the signal integrator supplied to the speed control on both MFW pumps. No. 2 unit was reduced to various load levels almost an entire month due to condenser tube leaks (21.7-h forced outage).
8/23/82		Trip due to loss of high-pressure oil pressure on No. 22 SG feed pump (60.8-h forced outage).
4/2/82	82-016	Plant computer failures rendered in-core detector monitoring system inoperable; analog/digital systems faulted.

Table 3.4 (continued)

Date	LER	Description (cause, consequences, corrective actions)
2/3/83	83-007	Deenergization of 2 RPS channels caused PORVs to open; blown fuse in channel inverter due to crossed leads from testing.
8/24/83	83-041	Reactor tripped on high pressure and both PORVS open; malfunction in main turbine control circuitry.
10/11/83	83-054	MFW regulating valve failed to close; fouled relay in valve positioner.
10/19/83	83-060	Water from a clogged toilet seeped down a conduit to the cable spreading room and tripped 3 circuit breakers.
4/15/84	84-003	Auto trip from loss of 22B coolant pump; surge capacitor failed in pump breaker. Periodic replacement of capacitors initiated.
4/26/84	84-005	Independence between diesel generators defeated by maintenance activity coupling an uncommon electrical power supply lineup.
10/3/84	84-008	Trip produced from low SG water level; cause of tripped feed pump not identified. Feed control system to be evaluated.

Table 3.5. Relevant operating experiences at other C-E plants
(scrams/trips and transients)

Arkansas-2	Ft. Calhoun	Maine Yankee	Millstone-2	Palisades	San Onofre-2	San Onofre-3	St. Lucie-1
Operating							
84-04		84-09	84-02		84-20	84-32	84-03
84-21		84-01	80-19[a]	83-151	84-17	6/11/80[a]	
84-19			79-09[a]		83-119a		76-41[a]
84-11					83-002[a]		76-30[a]
84-08					82-003		
84-03							
Maintenance							
80-91	78-45[a]			9/16/71[a]			
84-01							
Test							
84-20		84-08	62-35[a]				84-07
84-05							
84-01		12/14/72[a]	78-14[a]				78-19
		84-01					
77-43[a]							
77-8[a]							
Single failure							
84-06	84-14	74A-49			84-15	84-43	84-22
	84-13						
84-05							
	80-15[a]						
	78-29[a]						

Table 3.5 (continued)

Arkansas-2	Ft. Calhoun	Maine Yankee	Millstone-2	Palisades	San Onofre-2	San Onofre-3	St. Lucie-1
Degraded component							
82-45[a]	74-A-58[a]	5/19/73	76-42[a]	77-44	84-19	84-24	77-27
	80-22[a]	77-21	6/7/73	1/8/75[a]	76-24[a]	83-141	84-03
	79-104[a]			2/14/72	83-135	83-99	77-43[a]
	79-55[a]					82-168	
	77-6[a]						
	79-72[a]						
	4/4/75[a]						
	79-45[a]						
Disabled system							
	78-30			80-20	78-03a		83-103
	77-23						
84-04							
							84-08
84-09							
84-03							
82-50[a]							
81-56							
80-71[a]							
80-64[a]							
Electrical faults and noise							
83-10	84-13	84-09	76-48	77-58			77-26
	4/7/80	81-03	10/10/73		77-47		
	80-42						
	78-5[a]						

Table 3.5 (continued)

Arkansas-2	Ft. Calhoun	Maine Yankee	Millstone-2	Palisades	San Onofre-2	San Onofre-3	St. Lucie-1
Others							
84-24 12/18/72	84-07	4/12/74			84-50		84-37[a]

[a]LERs categorized as transients.

was manually controlling the level in the SGs. The transient usually began with excessive FW flow to the SG to maintain level. This resulted in an RCS temperature decrease, the shrink producing a pressurizer level drop below the technical specification limits. The resulting LER often mentions that several such events occurred within a short time frame in addition to listing other similar LERs. Procedural changes or reviews were often given as the corrective measures taken. Such events did not occur randomly but appeared to happen in groups.

3.2.2.1 Calvert Cliffs Unit 1. Transients, scrams, trips, forced unit outages in excess of 3 h, and a few other happenings relevant to this special study are listed in Table 3.3. Two of the events merit closer study as common cause multiple failures. These have been singled out and are described and discussed below.

3.2.2.1.1 Loss of both service water system redundant trains (LER 80-027). Shortly after the No. 12 service water subsystem was returned to service following routine cleaning of its service water heat exchanger tubes (saltwater side), the operator received low pressure alarms on both No. 11 and No. 12 service water subsystems; valve line-ups were immediately verified to be correct. The reactor was manually tripped at 1803 due to high main turbine bearing temperatures. A subsequent investigation revealed that No. 11 and No. 12 service water systems had become airbound.

The cause of air ingress into the service water system was complete failure of a tube in the No. 11 instrument air compressor after-cooler. The compressed air, being at a higher pressure than service water, entered the service water system and apparently accumulated in the No. 12 service water heat exchanger, whose outlet valve was shut while tube cleaning was in progress on the saltwater side. The service water system is equipped with vent valves designed to maintain the system free of air. However, as air became trapped in the idled heat exchanger, air ingress exceeded the air removal capability of the heat exchanger's two vent valves. The vent valves on the operating header maintained the service water system air free until the air bubble was released from the idled heat exchanger. When the heat exchanger was returned to service, the air bubble was released into the system and, since No. 11 and No. 12 service water subsystems are not independent in the turbine building, both No. 11 and No. 12 service water pumps lost suction with a consequent loss of all service water flow.

3.2.2.1.2 Reactor trip breakers opened simultaneously without known cause (LER 84-002). During normal Mode 1 operation, all eight reactor trip breakers opened simultaneously without apparent cause. Following the reactor trip, the operators, by observing annunciators in the control room, quickly ascertained that the trip breakers had opened and properly carried out the procedure for reactor trip (i.e., Emergency Operating Procedure No. 1). All safety systems functioned as expected following the event. No personnel errors occurred during the event.

Post-trip reviews verified that no input parameters to the reactor protective system had exceeded their set points immediately prior to the event. Although a surveillance test had been terminated on the reactor protective system matrix relays 30 s prior to the event, there was no clear correlation between the reactor trip and the surveillance test. Review of post-trip data confirmed that the reactor trip breakers were restored to normal prior to the event.

Following the reactor trip, a nonsafety-related MFW pump tripped; however, the remaining MFW pump and the AFW system were available throughout the event to provide secondary makeup water for decay heat removal as necessary. In addition, the motor-driven AFW pump started automatically following the trip.

3.2.2.2 Calvert Cliffs Unit 2. Transients, scrams, trips, forced outages in excess of 4 h, and a few other happenings relevant to this study are listed in Table 3.5. Three additional events have been singled out for discussion on the basis of lessons to be learned.

The first two could have happened at any plant, but did in fact happen at Unit 2. The first involved a break in communications. This event is indicative of the need for an operational aid that would correlate the consequences of equipment/systems interactions during maintenance. Actions taken during testing should also be included in the analysis. The second example raises two questions: (a) the habitability of the control room due to gases, fumes, and smoke generated in the cable spreading room directly underneath, and (b) the effects of water (sprays, mist, drips, etc.) from ruptured tubing or piping and fire sprinklers within range of the electrical equipment. Cabinets and covers are not water tight, but if made so could cause overheating due to a lack of ventilation (a Catch-22).

3.2.2.2.1 Diesel generator inoperability (LER 84-005). Ac safety bus 24 A 480 V was removed from service for preventive maintenance. To maximize DG 21 availability, its auxiliaries (fuel oil transfer pump, room ventilation fan, air start system air compressor, and various other engine auxiliaries, normally supplied from 24 A 480 V ac bus via MCC 204R) were kept energized by powering MCC 204R from MCC 214R via a tie breaker. This lineup allowed DG 12 to power DG 21 auxiliaries but in turn removed the independence between the two DGs. DG 21 was declared out of service but not logged as such since only one diesel was required to be operable.

Personnel on the next shift failed to recognize the dependence of DG 21 on DG 12 and placed DG 12 out of service for preventive maintenance. Although operations personnel were aware that Unit 2 480 V Bus 24 A was out of service, the correlation was not made between that work and its effect on DG 21 operability. Consequently, both diesels were made inoperable.

Later, a Senior Licensed Operator noted that both DGs were inoperable and containment integrity had not been established as required. Restoration of DG 12 to operability was in progress at the time and was continued until it was declared operable, terminating the event.

3.2.2.2.2 Flooding in control room affects central element assembly (CEA) electrical equipment (LER 83-060). Water from a clogged toilet overflowed into the control room area. From there it traveled under control cabinets where it seeped under the fire barrier material and through the floor and the conduit that leads to the ceiling of the cable spreading room below. The water then dripped from the conduit down onto the Shutdown Group Coil Power Programmer cabinets, where it tripped multiple breakers for three of the four CEAs within the cabinet.

Investigation discovered that a crowbar lodged in the toilet's drain line had obstructed and caused nondissolving paper material to block the line. It is suspected that the crowbar was left in the line during initial construction.

The affected compartments were wiped dry and sprayed with a water-dispersing solvent. Further investigation revealed that the main circuit breaker for CEA 46 had tripped and that water was still present in the plugin modules. All modules were replaced with spares, and the CEA was tested with satisfactory results. The CEA 48 circuit breaker for the primary power supply was found tripped. The circuit breaker was reset, and the power supply was tested for proper voltage with satisfactory results. The CEA 49 primary power supply circuit breaker was also found tripped; upon reset of the breaker, the power supply failed and was replaced with a spare. All tripped circuit breaker problems were attributed to the water in the cabinet. The fire barrier was inspected and found intact and functional.

3.2.2.2.3 Main feedwater regulating valve fails to close (LER 83-054). This was an overcooling transient produced by overfilling of the SG caused by a stuck open FW valve, and is significant since it contained five independent failures:

1. the No. 23 MFW pump tripped;
2. the No. 21 FW regulating valve failed to close;
3. the No. 21 MFW pump speed controller stuck in the high-speed position;
4. a turbine bypass valve failed in the 50% open position; and
5. a reactor coolant (RC) pump vapor seal failed 1.5 h after the reactor trip.

In addition, pressurizer pressure behavior during pressurizer refill demonstrated an interesting phenomenon that can result when the liquid and vapor phases are not in thermodynamic equilibrium. This phenomenon, which can occur when recovering from a transient in which the pressurizer is nearly drained, can result in a temporary decrease in pressure after the level has been returned to normal and all heaters are

on. This pressure response is contrary to what one might normally expect and could be initially puzzling to plant operators.

Number 22 FW pump tripped due to a leak in the pump's hydraulically operated control system while the plant was operating at 100% power. In an attempt to avert a plant trip, the operators began reducing power by borating and inserting control rods. The feed-flow/steam-flow mismatch was too great and the plant tripped. Following the plant trip, the No. 21 FW regulating valve failed to close. This caused the No. 21 FW pump's speed to increase, resulting in a rapid rise in the No. 21 SG level. The operator's attempt to decrease FW flow by placing the No. 21 MFW pump controller in manual and trying to decrease pump speed failed because the pump speed controller had stuck in the high-speed position due to an accumulation of dirt in the mechanism. Feedwater flow was isolated to SG 21 ~3 min after reactor trip, when the operators tripped the No. 21 MFW pump and shut the MFW isolation valve. The excessive feeding of SG No. 21 had caused RCS pressure to drop sharply due to overcooling. Reactor coolant temperature dropped ~50°F in 3 min and pressure decreased to ~1660 psig, causing safety injection (SI) system actuation. The severity of the overcooling transient was heightened by the effect of a turbine bypass valve that stuck 50% open due to mechanical binding.

3.2.3 Other C-E Plant Relevant Operating Experiences

A list of relevant transients and scrams in C-E plants other than Calvert Cliffs is presented by LER numbers or event dates in Table 3.5, and a few other relevant events are presented in Table 3.6. These experiences were reviewed to seek out possible common traits or singular events that might be peculiar to C-E plants. Again a common thread appeared to be in the manual control of SG levels when the unit is at low power levels. The ten events selected as having special significance are described in Sects. 3.2.3.1 to 3.2.3.10.

The first event was a case where loss of MFW challenged the AFW system and an AFW pump tripped, a consequence of three independent failures. The second event could be classified as a potential small LOCA produced by RCS discharge to the containment sump. The third, again the result of leaky valves, was a SG overfill. Gas binding of all three charging pumps and of the shutdown cooling pumps are examples 4 and 5. Example 6 is again a breakdown in communications: noise enters from assorted causes. In example 7, the thermal margin low-pressure reactor protection trip was actuated by the operation of the pressurizer quench tank vent valve. The last three examples occurred during testing/ surveillance and resulted from faulty test equipment.

3.2.3.1 St. Lucie, Unit 2: Reactor Trip Due to Low Steam Generator Level (LER 84-004). While at 100% power the MFW pump tripped due to low suction pressure, and the reactor subsequently tripped on low SG level. Following the trip AFW pump 2C started, then tripped on overspeed. A single steam safety valve on the SG A also stuck partially open

Table 3.6. Relevant operating experiences at other C-E plants (Miscellaneous)

Plant	Date	LER	Event
St. Lucie-1	12/19/81	81-056	Both MSIVs closed for no apparent reason; cause unknown.
Palisades	1/4/81	82-004	Safety injection occurred during shifting of electric power supply for preferred bus.
San Onofre-2	3/14/82	82-002	Shutdown cooling was lost and an inadvertent boron dilution resulted from the interaction of two separate valving operations conducted simultaneously.
St. Lucie-1	8/16/81	82-037	1A3 4.16-kV bus lost when an operator closing the breaker door jarred the load shedding relay in the vital/monitor tie breaker, opening the breaker.
St. Lucie-1	10/23/82	82-050	All charging pumps became gas bound when the volume control tank was pumped dry and hydrogen was admitted to pump suction.
St. Lucie-1	11/26/82	82-062	Inadvertent safety injection signal followed by loss of vital power supplies, caused when a test switch was positioned incorrectly during a monthly preventative maintenance test.
St. Lucie-1	12/30/82	82-071	Output breaker of the 1A static inverter opened, dropping one of four 120-V ac instrument busses during maintenance.
St. Onofre-2	11/9/82	82-136 and 82-138	Loss of power to FW control system due to inadvertent dislodging of a power cord (two occurrences).
San Onofre-2	11/14/83	83-151	Manual trip from an unexpected pressurizer pressure and level decrease; caused by erroneously opened emergency boration valve.

Table 3.6 (continued)

Plant	Date	LER	Event
San Onofre-3	11/19/83 12/22/83	83-103 83-120	Both MFW pumps tripped due to low suction pressure caused by low level in condensate storage tank (two occurrences).
Palisades	4/8/84	84-004	Two spurious right channel safety injection signals during refueling; caused by a short-circuit in test equipment.
Palisades	8/4/84	84-015	All major turbine operation valves closed from loss of electrohydraulic control fluid pressure. A fitting on the pump discharge worked loose from excessive system vibration.
Ft. Calhoun-1	3/14/84	84-003	Dc power to control room panel A1-41B lost because wrong maintenance procedure was followed. Unit trips on thermal margin low pressure signals. Noise spikes introduced into the TMLP calculator when the pressurizer quench tank vent valve was operated.
Ft. Calhoun-1	5/16/84	84-007	Ventilation system actuated when the reactor coolant drain tank filled with coolant and then discharged to a floor drain via back leakage thru check valves.
Ft. Calhoun-1	7/22/84	84-013	Thermal margin low pressure reactor protection system tripped the reactor when a signal cycled the pressurizer quench tank vent valve.
Maine Yankee	1/12/84	84-001	Plant tripped because of low condensate system pressure and low suction pressure caused by operational techniques.
Maine Yankee	6/22/84	84-008	Loss of load RPS channel tripped reactor; caused by lack of communications between control room and field test.

Table 3.6 (continued)

Plant	Date	LER	Event
Millstone 2	1/6/84	84-001	During routine surveillance on the ESFAS, faulty test equipment generated partial actuations.
San Onofre 2	3/9/84	84-016	Inadvertent actuation of safety injection, containment cooling, and containment spray systems during a 31-day surveillance on the plant protection system.
San Onofre 3	2/22/84	84-004	Inadvertent actuation of engineered safety functions during plant protection system surveillance.
St. Lucie 2	1/29/84	84-003	Turbine trip produced by high-high SG level caused by leakage of three main feed regulating valves.
St. Lucie 2	2/9/84	84-004	Low suction pressure to MFW pump tripped plant; cause not positively identified. AFW trip followed.
St. Lucie 2	8/30/84	84-005	FW isolation valve closed unexpectedly; caused by testing equipment.

following the trip. Approximately 40 min was required to reset the safety. Cooldown from the open safety was successfully controlled.

The cause of the low suction pressure to the FW pumps was not positively determined. Condensate pump vent line design probably contributed. The design is being changed to allow proper venting during strainer cleaning.

The AFW pump 2C tripped due to transients on a power supply during AFW actuation. The cause was not identified immediately. However, repeated testing over a period of six days revealed the problem. The safety valve had stuck open because a cotter pin was missing from a spindle nut. When the safety opened (as expected), the nut vibrated down and held the valve partially open. A modification eliminated this problem.

3.2.3.2 Ft. Calhoun, Unit 1: VIAS Actuation During Startup (LER84-007). During normal operation, the alert and alarm set points of Containment Air Particulate Monitor RM-050 are adjusted to alert the operator in the event of a significant increase in containment airborne activity. During refueling the alarm set point is lowered considerably and set at the occupational limit for unidentified isotopes. When the alarm is actuated, it indicates the necessity for respiratory protection measures for personnel inside containment.

As the RCS is pressurized during startup, the RCS/SI interface check valves may leak until RCS pressure is high enough to seat them tightly. On the day of the occurrence, one or more of these interface check valves began leaking.

Back-leakage through those check valves normally is controlled by automatic cycling of interface check valve leakage pressure control valves. The pressure control valves began cycling to relieve the check valve leakage (per design), thus pressurizing the SI leakage-return header. The relief valve on this header, SI-222, lifted and relieved to the reactor coolant drain tank (RCDT) as designed. Because the RCDT pumps were in manual and lined up to the SI Refueling Water Storage Tank (RWST) rather than to waste, the RCDT filled up and its relief valve lifted and discharged to the floor drain header, thus filling the containment sump. Airborne activity in containment increased, causing RM-050 to go into alarm and thus initiating the ventilation isolation actuation system (VIAS).

The problem was identified, and pressure in the SI leakage return header was immediately reduced by opening the crosstie valve (HCV-2983) from the header to the Volume Control Tank (VCT) in the Chemical and Volume Control System (CVCS). Opening HCV-2983 allowed relief valve SI-222 to reclose, effectively terminating the loss of RC to the containment sump.

3.2.3.3 St. Lucie, Unit 2: Turbine Trip/Reactor Trip Due to High Steam Generator Water Level (LER 84-003). While increasing power from 0 to 30% after an outage, the operator was transferring FW control from the 15% bypass valves to the MFW regulating valves. During this evolution a

Hi-Hi SG level turbine trip occurred, resulting in a reactor trip. The Hi-Hi SG level occurred due to leakage through the SG A main feed regulating valve. As the main feed block valves were opened in preparation for transfer from the 15% bypass valves, leakage through the SG A main feed regulating valve caused the SG A level to increase. Leakage through the SG B main feed regulating valve is significantly smaller than through the SG A. While the operator turned his attention to the SG A to reduce level, the level in SG B began to decrease. The operator's attention was then diverted to restoring the level in SG B, whereupon the level in SG A reached Hi-Hi and the turbine tripped, which tripped the reactor. All automatic systems functioned properly, the reactor was restarted, and the plant returned to 100% power.

3.2.3.4 St. Lucie, Unit 1: All Three Charging Pumps Become Gas-Bound (LER 82-050). A reactor trip/turbine trip occurred on low SG water level following loss of feed when one of the condensate pump motors tripped on differential phase current and a FW pump tripped on low suction pressure. Pressurizer level had returned to above the heater cutoff, and the primary plant had stabilized at no-load T_{avg} and 1960 psia when all three charging pumps became gas bound. The pumps were restored to operation one at a time by repeated venting after filling the volume control tank high in the operating band. During the period the charging pumps were inoperable, the pressurizer level fluctuated about the heater cutoff set point with variations in T_{avg}. When the first charging pump was restored, the pressurizer level was returned to the no-load set point. Two charging pumps were operating at reduced flow within 15 min, and all three were restored to operability well within the required time limits. The charging pumps became gas bound when the VCT was pumped dry and hydrogen was admitted to the pumps' suction.

3.2.3.5 San Onofre, Unit 2: Loss of Shutdown Cooling and a Boron Dilution (LER 82-002, 82-003). After initial fuel loading, an operator backflushed a filter in the shutdown cooling purification system. This normally consists of passing 350-psig nitrogen through the isolated filter and dumping the gas to the filter crud tank. As a result of either a system malfunction or an operator error, the nitrogen passed through the purification line back into the suction of the shutdown cooling [Low Pressure Safety Injection (LPSI)] pumps. At essentially the same time, shutdown cooling flow from the in-service LPSI pump fell from 4000 gpm to zero. Subsequent attempts to establish flow with the alternate pump were unsuccessful. The pumps and piping high points were vented,and shutdown cooling flow was reestablished within 90 min.

During the attempt to reestablish shutdown cooling flow suction of LPSI, pump PO-16 was transferred from the RCS to the RWST. Opening of the RWST line occurred concurrently with the closing of the RCS line so that for several minutes a path existed from the RWST into the RCS under the pressure head of the RWST. During this interval ~6000 gal of water at an approximate average boron concentration of 1640 ppm was added to the RCS. This resulted in a dilution from 2004 to 1962 ppm, equivalent to a

reactivity addition of about 0.64% Δk/k. Since RCS boron concentration remained well above the minimum required for Mode 6 (1720 ppm), plant safety was not affected by this event.

The operating procedure for the shutdown specifies that the RCS suction line be closed before the RWST suction line is opened. To prevent recurrence of this situation, a caution statement will be added to the procedure emphasizing the need for closing the RCS suction line before opening the RWST suction line.

The pathway for injecting nitrogen gas into the shutdown cooling system exists only when the purification system is in operation. Therefore, procedures for operating the backflushable filter will be revised to require isolating the purification system prior to any backflushing operation and personnel will be alerted to the potential for loss of flow when using this system.

3.2.3.6 Maine Yankee: Reactor Trip Caused by Loss of Load During Plant Startup (LER 84-008). On June 22, 1984, operations personnel were performing a plant startup following a refueling shutdown. The operator was increasing reactor power to ~12 to 15% in preparation for trip testing the main turbine. The wide-range logarithmic ex-corenuclear instrumentation channel power level indicated 9% power when the level 1 bistable activated on Linear Power Ex-core Nuclear Instrumentation Channel 8. The level 1 bistable enables the loss of load and symmetric offset trips and disables the startup rate trip at 15% power. The four ex-core linear power channels indicated 11 to 14.5%. The discrepancy between the wide-range and linear power channels existed because a calorimetric adjustment had not been performed since the previous operating cycle. The Channel 8 bistable activated before 15% because its set points were adjusted conservatively.

The main turbine was brought to 1800 rpm for trip testing, and control rods were partially inserted to stabilize reactor power and perform the calorimetric adjustment. The adjustment was based on the computer-calculated in-core power level derived from the fixed in-core monitoring system. The computer value of 8.5% agreed well with the indicated wide-range logarithmic power. The linear power channels were all indicating significantly higher.

The Plant Shift Superintendent informed the control room when he was ready to trip the turbine locally. A short time later, the control room operators recognized the reactor scram potential of turbine trip testing until the remaining linear power channels were properly adjusted away from the 15% loss-of-load trip set point. Control room operators attempted to contact the local test station via the plant paging system to delay the test, but the noise level in the turbine area prevented communication and the turbine was tripped. The level 1 bistable on linear power Channel 5 activated at about the same time, causing two of the four reactor protective system (RPS) loss-of-load channels to trip the reactor.

Control room operators initially did not recognize the potential significance of tripping the turbine before calorimetric adjustment was completed. The Plant Shift Superintendent at the local turbine test station was not informed of the situation and could not be contacted due to the noise level in the turbine area.

3.2.3.7 Ft. Calhoun, Unit 1: Noise Spike Causes Inadvertent Reactor Trip (LER 84-013). At 2150 on July 22, 1984, while operating at 83% power, the Ft. Calhoun Station Unit No. 1 received trip signals on both A and C channels of the thermal margin low pressure (TMLP) reactor protective system trip circuits. Since the reactor protective system acts to trip the reactor on a two-out-of-four channel trip logic, the reactor subsequently tripped.

Tripping of the A and C TMLP trip channels of the RPS was initiated by noise spikes received by temperature loops feeding TMLP calculator inputs. These noise spikes occurred while operating the pressurizer quench tank vent valve, HCV-155. Actual TMLP conditions were not present at the time of the trip.

Following the reactor trip, specific temperature indicators were verified to react coincident with the cycling of HCV-155. These temperature indicators are associated with temperature loops that feed input signals to the A and C TMLP calculators. Subsequent troubleshooting revealed that the noise problem initiated in temperature loop cabling that traveled through a control room panel. In addition, it is important to note that the spiking problem associated with the cycling of HCV-155 was intermittent but was consistently present during monitoring of the temperature input to the C channel TMLP calculator. That is, for 10 or 12 out of every 15 HCV-155 cycles, significant spikes were received at the TMLP calculator input. However, the spiking problem associated with the A channel TMLP calculator temperature inputs could not be duplicated.

3.2.3.8 St. Lucie, Unit 2: Reactor Trip During Auxiliary Feedwater Actuation Signal (AFAS) Functional Test (LER 84-005). A reactor trip occurred during performance of the logic matrix portion of the monthly AFAS functional test. Post-trip review and troubleshooting indicated that the trip was caused by the unexpected closing of an A Train FW isolation valve, resulting in a low SG level RPS trip. The closure of the FW isolation valve resulted from high resistance across an AFAS Channel A interposing relay contact during logic matrix testing, effectively satisfying Channel A actuation logic. After the high contact resistance was corrected, a complete AFAS functional test was performed satisfactorily.

3.2.3.9 Palisades: Safety Injection Actuation (LER 84-004). While the reactor was shut down for refueling, electrical checkout activities on preferred ac Bus Y-20 resulted in two spurious right channel safety injection signal (SIS) actuations. Investigation indicated that each incident resulted from voltage spikes caused by a short circuit in a piece of test equipment (voltage checking light) which was being used on

Y-20. The voltage spike caused a SIS block relay to drop out, allowing a previously present low-pressure signal to initiate a right channel SIS. Personnel performing the checkout were unaware at the time that they had caused the first SIS actuation. Checkout activity continued on Y-20 until the second occurrence, at which time several Y-20 fuses blew.

A review of the Y-20 circuit design revealed that circuit protection features in Y-20 should have functioned to prevent a voltage spike from causing a SIS actuation. Circuit protection features will be evaluated to determine if they are appropriate for their application in Y-20.

3.2.3.10 Millstone Pt. Unit 2: Emergency Core Cooling System (ECCS) Partial Actuation (LER 84-001). Two random actuations of ESFAS equipment occurred. The plant was in Mode 2 at 0.4% power for the first occurrence (1/6/84) and in Mode 2 at 0.6% power for the second occurrence (1/9/84).

Plant instrumentation and controls (I&C) technicians were performing routine surveillance on the ESFAS using the manual test insertion test equipment. During the surveillance the operators notified the I&C technicians that an actuation had occurred. The test equipment was secured, and ESFAS equipment was restored to normal. Since the surveillances were planned in advance, the possibility of actuation had been anticipated and precautions had been taken in each case.

The cause of the actuation is unknown. A possible cause is electromagnetic interference (noise) from the test equipment.

3.2.4 Summary and Conclusions

Other than the manual FW control problems at low power levels, the operating experiences at Calvert Cliffs-1 and -2 do not appear to be any different than the general run of those at most other operating nuclear power plants. (By "the general run," we intend to exclude major accidents or near major accidents such as have occurred at other nuclear facilities on a few occasions.) At Calvert Cliffs there were one-of-a-kind events which, if left unmitigated, might have led to serious consequences, but none progressed to a serious situation. The potential SG overfill and small-break LOCA events from the combined sequences of 11 C-E operating units at 8 plant sites were adequately handled by the existing procedures and trained personnel. Sometimes these transients produced secondary effects which, when coupled with faulted equipment, compromised a safety system train, but the results were always anticipated by emergency procedures.

Maintenance and testing problems are generic for the industry and deserve more attention. Improvements would result in significantly fewer challenges to the reactor safety system and the plant protection systems. Improvements in the man-machine interface would greatly alleviate the severity and reduce the frequency of these happenings.

The relatively large degree of manual (operator) control in C-E plants makes it desirable to improve plant communications, both within the control room and between the control room and personnel in the plant areas. Better coordination among operations, maintenance, and testing activities is needed and is something that could be provided with the existing technology without an expensive or extensive backfit.

4. DETERMINATION OF SICS SEQUENCES FOR ANALYSIS

In Sect. 3.1, the systems making up the Calvert Cliffs Nuclear Station were identified. Based on the SICS Program scope and the functional proximity of systems to the RCS and safety systems, 35 control systems having potential safety implications were selected for more detailed analysis. These control systems have been listed in Table 3.1

The analysis of the failure modes of these systems are presented and discussed in Sect. 4. The FMEA and event sequence analysis methods are briefly discussed in Sect. 4.1, and in Sect. 4.2 the results of the system- and component-level FMEAs are discussed and significant results presented. In Sect. 4.3 the significant system failure modes identified in Sect. 4.2 are evaluated in terms of developed accident sequences. Calvert Cliffs and other C-E designed plant operating experiences relative to major identified accident sequences have been discussed in Sect. 3.2.

4.1 FMEA OBJECTIVES AND METHODOLOGY

The objective of performing FMEAs on the control systems selected in Sect. 3.1 is to identify failure modes with effects having potential safety implications for the Calvert Cliffs Plant. The basis for choosing the FMEA methodology and the application of this methodology to the SICS Program is discussed in Sect. 4.1.1.

Once the system failure modes and their effects are tabulated, the effects that may contribute to accident sequences of concern can be identified. These failure modes can then be combined with other initiating events or equipment failures to assess their safety implication in the context of accident sequences. The sequence development methodology is discussed in Sect. 4.1.2.

4.1.1 Selection and Application of FMEA Methodology

In general, two systems failure analysis methodologies are available to analyze the relationship of failures and their effects: "top-down" methods such as fault trees, and "bottom-up" methods such as FMEA. Each method has advantages depending on the analysis objective, and the reasons for selecting the FMEA methodology are discussed here. It also is noted that the two analysis methods offer different insights into analyses of system failures and therefore are often used together.

Top-down methods typically are used when a system failure state is known and the combinations of failed components producing this failed state are desired (e.g., define the combinations of failed components of a fluid system resulting in a system flow rate of less than 500 gpm). Because the top-down method yields a complete listing of failures resulting in a particular failed state, it is particularly useful in assessing the probability of the failed state.

The FMEA method, in contrast, proceeds from the opposite direction. Given a set of equipment, this method defines the failure modes and evaluates the effects of each. FMEAs typically are used to find undesirable failure modes of systems where the particular modes of failure are not known on some other basis. FMEAs are useful for the detailed analysis of a limited scope of equipment. However, FMEAs will not necessarily identify all combinations of failures leading to any of the effects identified, and therefore cannot be used directly to assess probabilities of these effects unless other methods such as fault trees are used in conjunction with the FMEA.

The scope of the SICS Program limits the equipment studied to control systems and does not specify the failure modes. Therefore, FMEA was chosen as the appropriate assessment method. Fault trees are used in the SICS Program to evaluate the probabilities of selected system failure modes of significance once they are identified (see Sect. 5). In addition, it is recognized that due to federal design requirements for nuclear power plants and extensive regulatory design reviews, control system failure modes with safety significance are expected to be subtle. The FMEA method is expected to be particularly useful in identifying subtle failure modes.

The FMEA method was applied to the SICS analysis in two levels of detail. At Calvert Cliffs, 35 systems were identified as control systems within the scope of the program. To analyze this number of systems efficiently, system failure modes were chosen first at the system function level (versus component level) to evaluate whether system failure modes of significance to the RCS or the safety systems were possible. Systems having significant effects at the system failure level were then reanalyzed in detail at the component failure level.

Application of the system-level FMEA is a bounding technique. In choosing failure modes, emphasis was placed on ensuring that the effects of all possible combinations of component failures would be bounded. The credibility of the failure mode was not considered. The effects of the system level failure modes were evaluated by assessing their significance with respect to SG overfill, RCS overcooling, RCS undercooling (inadequate core cooling) or degrading safety system performance.

The results of the system-level FMEAs were used in two ways: First, those systems with significant failure effects were selected for component level FMEA; and second, for those systems without significant failure effects, the results of the system-level FMEA were used directly without further detailed analysis.

Component-level FMEAs were applied to develop a listing of all credible system component failures and their direct and indirect effects. The analysis begins with a complete listing of a system's major components (i.e., valves, pumps, transmitters, etc.) and the possible failure modes of each (a valve can fail completely open, completely closed, or in an "as is" or intermediate position). Three aspects of the failure mode then are evaluated and listed: possible causes of the failure, direct

and indirect effects, and possible remedial actions. Failure causes are useful in evaluating the potential for coupled failures (more than one failure mode resulting from a single initiating failure). Effects of the failure mode include both direct and indirect effects. For instance, the direct effect of a valve closure could be a complete loss of fluid flow. Indirect effects might include consequential failure of components in other systems. Remedial actions are evaluated and listed to aid in the evaluation of consequences. The availability of actions mitigating the effects of failure modes generally tend to reduce the importance of the failure mode, whereas effects that cannot be mitigated readily are of relatively greater importance.

The compiled listing of the failure modes and their effects on the systems selected for component-level FMEA typically is very large, presenting in detail all failure modes rather than just those with potential safety implications. The tabulated effects of the FMEAs must be screened to identify the failure modes of potential safety significance.

Four principal criteria were used to identify and separately list those failure effects (and their causes) having potential safety implications:

1. potential for the failure mode to initiate or contribute to SG overfill,
2. potential for the failure mode to initiate or contribute to inadequate core cooling (RCS undercooling),
3. potential for the failure mode to initiate or contribute to a continuous and uncontrolled decrease in RCS temperature in excess of technical specification rates, and
4. potential to degrade the performance of safety systems.

In addition to these criteria, the effects were evaluated to identify potentially significant effects not specifically addressed in the principal evaluation criteria.

The identification and listing of all potentially significant failure modes provides a basis for the development and evaluation of possible accident sequences incorporating these failure modes, which is discussed in Sect. 4.1.2. The results of the Calvert Cliffs control systems FMEAs are discussed in Sect. 4.2.

4.1.2 Accident Sequence Development Methodology

A particular failure mode leading directly to an unmitigated accident would be a significant result. However, in addition to this unexpected class of events, control system failures also would be considered significant to the extent that they may contribute to unmitigated accident sequences in conjunction with other postulated failures.

The evaluation of the safety significance of control system failures required the development of accident sequences and the incorporation of the control system failures in these sequences. Accident sequences were

developed using an "event tree," a representation of an initiating event, and the subsequent success or failure of required mitigating systems. An accident sequence is defined in the event tree as the initiating event and a unique combination of the operating states of the mitigating systems.

The accident sequence analysis was begun by developing a list of accident initiating events from available information such as the Calvert Cliffs FSAR and the FMEAs of the Calvert Cliffs control systems. For each initiating event, the systems required to achieve a demonstrably safe plant operating state (e.g., safe hot shutdown) were identified and an event tree constructed based on the success or failure of these systems to operate. The plant operating state resulting from each accident sequence was then evaluated to identify those sequences resulting in a safe state as defined in the FSAR accident analyses and those resulting in a potentially unsafe or undefined state.

Each event tree was then reviewed to assess the potential contribution of control system failures to unsafe or undefined plant states. Event trees involving control system actions with potential safety implications were selected based on the following criteria:

1. the existence of successful control system actions required to achieve a safe plant state (or control system failures leading to potentially unsafe or undefined plant states),
2. the existence of control system failures requiring operator action to achieve a safe plant state, and
3. the existence of "as designed" control system actions potentially leading to unsafe conditions for which no safety system mitigation is available.

The accident sequences defined by the event trees selected in the above process identify the control system failures with potential safety implications and are important results of the SICS Program.

The results of the Calvert Cliffs accident sequence analysis are discussed in Sect. 4.3, and the frequencies of the identified accident sequences and the relative contributions of control system failures are evaluated and discussed in Sect. 5. Selected accident sequences were also subjected, as required, to plant thermal-hydraulic analyses to define plant consequence states. These are discussed in Sect. 6, including the selection criteria.

4.2 IDENTIFICATION OF SIGNIFICANT CONTROL SYSTEM FAILURES

This section presents the results of the FMEAs of the Calvert Cliffs control systems at both the system and component levels. Those failure modes and effects that may contribute to accident sequences of concern are identified. For all such failure modes, potential safety significance was assessed with respect to the potential to initiate or contribute to SG overfill, RCS overcooling, RCS undercooling (inadequate

core cooling), or degradation of plant safety system performance. Section 4.2.1 presents the system-level FMEAs, and the detailed component-level FMEAs are provided in Appendix C and highlighted in Sect. 4.2.2.

4.2.1 System-Level Failure Modes and Effects Analysis (FMEA)

The systems selected for FMEA (Table 3.1) represent those plant control systems which, operating either as designed or in a degraded state, may affect RCS or safety system response to transients. System functions were reviewed to identify system function failures that could affect the specific plant-level failure modes of RC undercooling or overcooling, SG overfill, or safety system function. In this review, complete failure of the plant control systems was assumed and the subsequent impact on plant operation evaluated. If system failure did not affect the RCS or result in SG overfill, the system was not selected for a component-level FMEA.

Information used in this review included the Calvert Cliffs FSAR[10] and detailed system descriptions prepared for BG&E. The ORNL analyses assumed that operation of all plant systems was consistent with BG&E operating procedures. In those cases in which the operational configuration used deviated from the as-built capability of the system (e.g., additional capability existed but was not used), the configuration actually used was evaluated.

Of the 35 systems initially selected for analysis, this review selected 14 for component-level FMEA. Results of this review are summarized in Table 4.1. In this table each system identified in Table 3.1 is characterized according to its impact on RCS overcooling and undercooling and SG overfill. Selection status for component-level FMEA can be found in the general comments portion of the table. The more significant system level FMEA results are discussed in Sects. 4.2.1.1-20.

4.2.1.1 Auxiliary Boiler Steam System. The auxiliary boiler steam system can provide motive steam for the main and auxiliary feed pump turbines under startup, shutdown, and emergency conditions. Use of the auxiliary boiler steam system to power the feed pumps during operation is considered unlikely because it would require failure of the normal steam source for the main and auxiliary steam-driven pumps and failure of the motor-driven AFW pumps. Shutdown operations have not been considered in this analysis effort.

The auxiliary boiler steam system also heats the refueling water tank (RWT) when the ambient temperature drops below 45°F. Failure of the RWT heating below 45°F would require shutdown due to violation of technical specifications. Thus the potentially adverse effects of an auxiliary boiler failure would require extreme weather conditions for an extended period of time and a violation of the technical specifications. Even under these unlikely conditions, unprotected pipes would freeze before the large water volume of the RWT. Injection of cold water may be of

Table 4.1. Summary of system-level failure modes and effects analysis

System Name and ID		Failure Mode	Potential System Failure Effects: RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	General Comments
E06	Plant Computer	Complete Computer Failure	No	No	No	No	Not Selected. Although used to calculate core power and core power distribution required by Technical Specifications, it provides only a monitoring function and is not used to control plant components during a transient.
		Returns Erroneous Data	No	No	No	No	
P08	Auxiliary Boiler	Fails to Heat RWT	Possible	Possible	No	Possible	Not Selected. Failure to heat RWT under the most extreme conditions, may block the RWT as a source of water to the safety injection systems. Failure of plant heating would otherwise not jeopardize plant operation (see 4.2.1.1). However, little information is available to evaluate system impacts in detail.
		Fails Plant Heating	No	No	No	No	

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects: RCS Undercooling	RCS Overcooling	SG Overfill	Safety System Interface	General Comments
N09.C Electric Heat Tracing	Fails with Heating Off	No	No	No	No	Not Selected. Boron precipitation is not capable of blocking injection paths from the RWT to the RCS. Specific core safety requirements for high concentration boric acid from CVCS could not be identified (see 4.2.1.19).
	Fails with Heating On	No	No	No	No	
W01.C Solid Waste Processing	Spent Resin Processing Fails	No	No	No	No	Not Selected. Failure to process RCS purification resins would not significantly impact RCS operation in the short term.
	Low Level Waste Drumming Fails	No	No	No	No	
W01.A Waste Gas Processing	Compression of Waste Gas into Decay Tanks Fails	No	No	No	No	Not Selected. Failure would not impact the RCS or equipment required to mitigate transients.

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects				General Comments
		RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	
W09.A Hydrogen Gas	Fails to Supply Volume Control Tank	No	No	No	No	Not Selected. Failure could result in higher, long term RCS corrosion rates (assuming the plant was not shutdown and repairs made) and/or turbine trip. Most severe impact comes from the explosion danger due to the release of H_2 to the plant environment. Impacts of such a transient should be evaluated separately.
	Fails to Supply Generator Cooling	No	No	No	No	
	Releases H_2 to Auxiliary Building	No	No	No	No	
W09.B Nitrogen Gas	Fails to Pressurize SI Accumulators	No	No	No	Possible	Not Selected. SI accumulators are assumed to be pressurized prior to reactor startup (see 4.2.1.18). Failure to delay startup until accumulators are pressurized or a depressurization of accumulators (safety system failure) may impact recovery from very large LOCA's.

Table 4.1 (continued)

System Name and ID		Failure Mode	Potential System Failure Effects: RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	General Comments
P01	Main Steam	Fails to Remove Reactor Heat	Yes	No	Yes	No	Selected. Significant impact on RCS (see 4.2.1.6).
		Fails to Provide SG Overpressure Protection	No	Yes	No	No	
		SG Tube Rupture	Possible	No	Possible	No	
		Pipe or Valve Rupture	No	Yes	No	Yes	
		Fails to Maintain Pressure	No	Yes	No	No	
N09	Chemical and Volume Control	Fails to Control RCS Volume	Yes	No	No	No	Selected. Significant direct interface with the RCS (see 4.2.1.7).
		Fails to Control Boric Acid Concentration	No	No	No	No	
		Fails to Provide Safety Injection	Yes	No	No	Yes	
		Fails to Control RCS Chemistry	Possible	Possible	No	No	
N04.A	Reactor Regulating	Incorrectly Sets Pressurizer Level	Possible	No	No	No	Selected. Impact on both primary and secondary systems was basis for selection (see 4.2.1.8).
		Fails Steam Dump and Turbine Bypass	No	Yes	No	No	

Table 4.1 (continued)

System Name and ID		Failure Mode	Potential System Failure Effects: RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	General Comments
N04	Reactor Coolant	Pump Seal Failure Small LOCA	Yes	Yes	No	No	Selected. Response of RCS provides the basis for evaluating control system failures (see 4.2.1.10).
		Pressurizer PORV's Fail Open	Yes	Yes	No	No	
P07	Steam Generator Blowdown	Unisolated Blowdown to Condenser	No	Possible	No	No	Not selected. Failure of system unlikely to significantly affect the secondary system (see 4.2.1.9).
		Fails to Maintain SG Water Chemistry	Possible	Possible	No	No	
P05	Condensate and Feedwater	Fails to Correctly Maintain SG Water Level	Possible	Possible	Yes	No	Selected. Failure of system could adversely impact the operation of secondary system (see 4.2.1.11).
P05.A	Feedwater Regulating	Excessive Flow	No	Possible	Yes	No	Selected. Failure of system has an impact on core heat removal and SG overfill (see 4.2.1.12).
		Insufficient Flow	Yes	No	No	No	
P03.A	Steam Dump and Turbine Bypass Control	Fails Bypass Valves Closed	No	No	No	No	Selected. Failure of system could cause depressurization of secondary (see 4.2.1.13).
		Fails Bypass Valves Open	No	Yes	No	No	

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects				General Comments
		RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	
P02.A Turbine Generator Control	Fails to Supply Sufficient Steam Flow to Turbine	No	No	No	No	Not Selected. Failures involving steam flow result in turbine trip. Turbine trips are actuated by other instrumentation and mechanical systems and will be addressed accordingly (see 4.2.1.14).
	Supplies Excessive Steam Flow to Turbine	No	No	No	No	
P02 Turbine Generator/ Condenser	Failure to Trip Turbine	No	Yes	No	No	Not Selected. Failure of turbine to trip would be a SLB. Failure of condenser could impact RCS (see 4.2.1.17), but is similar to failure resulting from loss of feedwater and closure of turbine bypass valves. These two failures are retained as bounding events.
	Loss of Condenser Function	Possible	No	No	No	
N04.B Reactor Coolant Pressure Regulating	Pressurizer Heaters or Spray Valve Misoperated	Possible	Possible	No	No	Selected. Failures may impact RCS (see 4.2.1.15).

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects: RCS Undercooling	RCS Overcooling	SG Overfill	Safety System Interface	General Comments
N09.A Pressurizer Level Regulating	Insufficient Net Letdown Flow	Yes	No	No	No	Selected. Potential LOCA initiator (see 4.2.1.16).
	Excessive Net Makeup Flow	Yes	No	No	No	
W02 Radiation Monitoring	Spurious Closing: SG Blowdown Valves	No	No	No	No	Not Selected. System failure may cause Tech Spec non-compliance, but would not impact components ability to achieve safe shutdown.
	Spurious Closing: Isolation Valves	No	No	No	No	
	Fail to Isolate	No	Nc	No	No	
W01.B1 RC Waste Processing	Fails to Receive Letdown from RCS via CVCS	No	No	No	No	Not Selected. System failure may result in inability to recover boric acid from letdown. However, the impact of this system on plant response to transients is minimal.
	Fails to Supply Boric Acid Storage Tanks	No	No	No	No	
W01.B2 Miscellaneous Waste Processing	Fails to Process SG Blowdown	No	No	No	No	Not Selected. Failure to process SG blowdown would not impact components needed to achieve safe shutdown of the plant.

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects: RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	General Comments
W07.B Instrument Air	Fails to Supply Motive Power to Valves	Yes	No	Yes	Yes	Selected. Failure of instrument air adversely impacts feedwater regulating valves (see 4.2.1.2).
W04.B Salt Water Cooling	Fails to Cool Service and Component Cooling Water	Yes	No	Yes	Yes	Selected. Indirect failure of service and component cooling water systems could result from salt water cooling failure (see 4.2.1.3).
W03.A Component Cooling	Fails to Provide Cooling Water to Strategic Plant Components	Yes	No	No	Yes	Selected. System failure would cause small LOCA from RC Pump Seals (see 4.2.1.5).
W03.B Service Water	Fails to Provide Cooling Water to Strategic Plant Components	Yes	No	Yes	Yes	Selected. System failure could cause instrument air and safety system unavailability (see 4.2.1.4).

Table 4.1 (continued)

System Name and ID		Failure Mode	Potential System Failure Effects				General Comments
			RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	
W08	Sampling System	Fails Resulting in RCS or Secondary System Leakage	No	No	No	No	Not selected. Failures may result in primary or secondary system leakage and possibly require shutdown. However, the design limits maximum flowrates and worst case failures are not expected to have any significant impact on identified failure modes.
C03	Containment Air Recirculation and Cooling System	Fails to Adequately Cool Containment	No	No	No	No	Not Selected. System failure would result in increased containment temperatures possibly requiring plant shutdown. In the long term, in-containment equipment accuracy or operability may be affected. To some degree, the operation of the containment purge system would moderate containment temperatures.

Table 4.1 (continued)

System	Name and ID	Failure Mode	Potential System Failure Effects				General Comments
			RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	
C05	Containment Purge	Fails to Purge Containment of Hydrogen	No	No	No	No	Not Selected. System is only operated when containment is occupied. Its failure is not expected to impact equipment operability.
C08.B	Pressurizer Compartment Cooling	Fails to Inject Containment Air into Pressurizer Compartment	No	No	No	No	Not Selected. The pressurizer compartment is cooled by injection of air from the containment coolers and additional air injection from the pressurizer compartment blowers. In the event these blowers fail, compartment temperatures would be limited by the containment coolers.
X05.B1	Turbine Building Ventilation	Fails to Cool Turbine Building	No	No	No	No	Not Selected. System failure would result in an increase in turbine building temperature possibly requiring or causing plant shutdown. In the long term, turbine building equipment accuracy or operability may be affected.

Table 4.1 (continued)

System Name and ID	Failure Mode	Potential System Failure Effects				General Comments
		RCS Under-cooling	RCS Over-cooling	SG Overfill	Safety System Interface	
X05.b Auxiliary Building Ventilation	Fails to Cool Auxiliary Building	No	No	No	No	Not Selected. System failure would result in an increase in auxiliary building temperature possibly requiring or causing plant shutdown. In the long term, auxiliary building equipment accuracy or operability may be affected.
E01 500 Kv Switchyard and Unit Transformer	Fails to Provide Electric Power	Yes	No	No	Yes	Selected. System failure would challenge emergency power for auxiliary feedwater pumps and HPSI.
E02 13,000, 4160 and 480 Volt Station Power Distribution System	Fails to Provide Electric Power	Yes	No	No	Yes	Selected. System failure would challenge emergency power for auxiliary feedwater pumps, HPSI and power required to open atmospheric dump and turbine bypass valves.
E03 125 Volt DC and 120 VAC Electric Power System	Fails to Provide Electric Power	No	Possible	Yes	No	Selected. System failure will prevent the trip of steam generator feed pumps and result in atmospheric dump and turbine bypass valves closing.

some concern in some PTS sequences. However, PTS analyses performed to date have not shown RWT water temperature to be of significant concern (see ref. 5).

Because use of the auxiliary boiler steam system for a function affecting plant safety is extremely unlikely, this system was not selected for a component level FMEA.

4.2.1.2 Instrument Air System. The instrument air system provides control and operating air for the opening or closing of air-operated valves throughout the plant. Failure of the instrument air system will cause both FW regulating valves to freeze in position and both FW bypass valves to open. The net result of this failure is a potential overfill of the SGs following reactor trip.

A passive failure of the B train pneumatic tubing will result in spurious initiation of the steam-driven auxiliary feedwater system (AFS) pump and opening of the associated AFS control valves. This spurious initiation of the AFS will exacerbate SG overfill conditions.

The instrument air system was selected for component-level FMEA because of its potential for causing a SG overfill condition following reactor trip. The results of the component-level FMEA are provided in Sect. 4.6, and a description of the instrument air system is included in Appendix B-13.

4.2.1.3 Salt Water Cooling System. The salt water cooling system provides the heat sink for the service and CCW systems. The interfaces between the salt water cooling system and the service water and CCW systems are the service and CCW heat exchangers respectively. Failure of the salt water cooling system to cool these heat exchangers for an extended period could affect the function of numerous plant components. The time frame necessary for the failure of the salt water cooling system to seriously affect the service water and component cooling functions is difficult to ascertain. Clearly, the more immediate impact on the components is the complete loss of service water or CCW. The degraded operation caused by failure of the salt water cooling system to supply cooling water to the heat exchangers represents a secondary impact on plant operation, which will be addressed elsewhere. The service water and component cooling systems are also selected for component-level FMEA and can be found in Sects. 4.2.1.4 and 4.2.1.5 respectively.

4.2.1.4 Service Water System. The service water system provides cooling water service for strategic plant components including turbine generator, DGs, air compressors, and feed pumps. Failure of the service water cooling to the turbine and generator is expected to result in a turbine trip. Failure of the service water cooling to the DGs would contribute to the failure of emergency electric power. Loss of service water to the instrument air compressors could cause eventual failure of the instrument air system (Sect. 4.2.1.2). Loss of service water to the

MFW pump and condensate booster pump lube oil coolers is expected to require eventual pump trip to prevent damage. MFW pump trip will result in auxiliary feed pump actuation on low SG level.

The service water system was selected for component-level FMEA on the basis of its impact on emergency power and its ability to cause loss of the instrument air compressors.

4.2.1.5 Component Cooling Water System. The CCW system supplies cooling and seal water to numerous components throughout the plant. Specifically, it supplies the RC pump mechanical seal coolers, thermal barriers, and bearing oil coolers. It also supplies cooling water to the HPSI and LPSI pumps for the stuffing box jackets, bearing housings, and mechanical seal coolers as well as the shutdown cooling heat exchangers.

Continued operation of the RC pumps following loss of CCW could result in seal failure and a subsequent small LOCA. Operation of the HPSI and LPSI pumps for periods greater than 2 h without CCW may result in eventual pump failure.

The CCW system was selected for component-level FMEA because of its potential impact on RC undercooling. Detailed analysis of the failure modes of this system can be found in Sect. 4.2.2.

4.2.1.6 Main Steam System. For the purposes of this study, the main steam system is considered to include the SG, the main steam isolation valves, the code safety valves, the main steam stop and control valves, and the interconnecting piping. (The atmospheric steam dump and turbine bypass valves, which will be analyzed in conjunction with the main steam system, are actuated by the atmospheric steam dump and turbine bypass control system discussed in Sect. 4.2.1.13).

The SG receives water at the secondary system inlet from the condensate and FW system. The main steam system discharges high-quality steam to the turbine generator and condenser system for the conversion of thermal energy to electrical energy. It also removes reactor heat and protects the SG from overpressurization. Turbine trip transients require that the safety valves, turbine bypass valves, or atmospheric steam dump valves open to prevent overpressurization of the SG and for removal of residual heat from the RCS. On the other hand, the discharge of excessive steam to the turbine or through the relief valves potentially results in RCS overcooling. Rupture of the SG tube(s) is a small LOCA, which could potentially affect the rate of core heat removal. A pipe or valve rupture in the main steam system could also lead to RCS overcooling due to depressurization of the SG. These failure modes will be addressed in detail in the component-level FMEA of the main steam system.

The atmospheric steam dump and turbine bypass system permits the control of secondary steam pressure without requiring operation of the main

steam safety valves. Failure modes of the atmospheric steam dump and turbine bypass control system are discussed in Sect. 4.2.1.13.

The SG blowdown system interfaces with the SGs to maintain the SG water chemistry and to cool and purify the blowdown water for return to the condensate system. Failure modes of this system will be addressed in Sect. 4.2.1.9.

4.2.1.7 Chemical and Volume Control System. The chemical and volume control system (CVCS) is designed to remove, purify, and replace RC at a controlled flow rate to maintain pressurizer level during reactor operation. The system is also used to inject chemicals to control RC chemistry, collect and reinject the controlled bleed-off from the RC pump seals, and provide high-pressure injection (HPI) of concentrated boric acid following accidents.

The CVCS consists of a letdown and charging subsystem and a makeup subsystem. The letdown and charging subsystem provides RC removal and return to the RCS, while the makeup subsystem controls RCS water chemistry.

In an extreme case, failure of the letdown and charging subsystem to maintain the water volume in the RCS could inhibit RC circulation and core heat removal. This CVCS failure might result from a failure of the charging pumps and/or diversion of the letdown fluid to the liquid waste tanks. The potential for decreasing RCS coolant inventory resulted in the selection of the CVCS for component-level FMEA.

The CVCS requires instrument air and control power for valve positioning and motive power for charging pumps to function. Loss of instrument air results in closure of the letdown stop and regulating valves. Control of letdown regulating valves is provided by the pressurizer level regulating system (Sect. 4.2.1.16). Charging flow is continuously supplied by one or more charging pumps. Following loss of CCW to the letdown heat exchanger, the CVCS transfers to a recirculation mode, bypassing the ion exchangers, radiation monitor, and boronometer.

Failure of the makeup subsystem to maintain the proper water chemistry, while important, is not critical to plant operation in response to a transient. Failure to remove boron from the RCS would result in a small decrease in reactor power level with time.

4.2.1.8 Reactor Regulating System. The reactor regulating system (RRS) interfaces with the pressurizer level regulating system to provide control of the pressurizer water level. The RRS also interfaces with the atmospheric steam dump and turbine bypass system to provide adequate and controlled core heat removal in the event of a turbine trip. The potential impact of this system on the RCS is the basis for its selection for component-level FMEA.

The RSS determines the pressurizer level to be maintained by the pressurizer level regulating system. It also adjusts the position of

the atmospheric steam dump and turbine bypass valves in proportion to the energy stored in the primary coolant. Following a turbine trip, a signal is transmitted by the RRS to the steam dump and bypass control system to open the steam dump and turbine bypass valves. Failure of the RRS to position the valves sufficiently open to remove the energy in the RCS could cause safety valves to lift. Further discussion of the interface between the RRS and the atmospheric steam dump and turbine bypass system can be found in Sect. 4.2.1.13.

4.2.1.9 Steam Generator Blowdown and Recovery System. The SG blowdown and recovery system supports the main steam system by maintaining the SG water chemistry and the secondary water inventory. Secondary water leaves the SG via the bottom blowdown line and flows to the blowdown tank, which is located outside the containment building. A blowdown throttle valve controls the flow to the blowdown tank at 150 gpm.

After it is cooled and purified, blowdown water is returned to the plant condensate system. (Normal pressure in the blowdown tank is sufficient to force the flow to the condensate system.) During normal operation, the cooled and purified water is returned to the main condensers. If a high radiation level is detected in the blowdown, the return water is diverted to the miscellaneous waste processing system to prevent release of radioactive liquid to secondary systems and to the environment.

In the long term, failure of the SG blowdown and recovery system to maintain the water chemistry could result in SG tube failures due to corrosion (a small LOCA). However, because SG water chemistry is controlled by technical specification, blowdown failure is not expected to lead directly to a tube rupture.

Failure of the blowdown system to isolate or maintain isolation could lead to a continuous diversion of FW or steam. However, the 2-in.-diam water blowdown nozzle and the 1-in.-diam surface blowdown nozzle are sufficiently small relative to the FW flow inlet to significantly limit the effects on RCS temperature. The SG blowdown system was not selected for a component-level FMEA.

4.2.1.10 Reactor Coolant System. The function of the RCS is to transfer heat from the reactor core to the SGs. The RCS consists of two heat transfer loops connected in parallel across the reactor vessel. Each loop includes a SG, two RC pumps, and the primary system piping. A pressurizer connected to one of the loop hot legs maintains RCS pressure.

Two types of RCS failure were found to lead to a small LOCA: release of RC due to RC pump shaft seal failure, and failure to close or isolate the pilot-operated relief valves (PORVs) mounted on the pressurizer. The RCS interfaces either directly or indirectly with all other systems selected for component-level FMEAs, and its response to control system failures is the basis for control system analysis in this report, including those support system failure modes induced by RCS instrumentation.

Specific component failures contributing to these failure modes will be addressed in the component-level FMEA.

4.2.1.11 Condensate and Feedwater System. The condensate and FW system transfers condensate from the condenser hotwell to the SG. In conjunction with the SG blowdown and recovery system, it maintains the required chemical characteristics of the secondary water. This system interfaces directly with the main steam system at the SG and with the turbine generator condenser system at the condenser.

The principal failure mode of interest in the condensate and FW system is the excessive addition of FW to the SGs, which could also result in SG overfill. The primary component failure resulting in overcooling is failure of the MFW control valves. The failure mechanisms for the FW control valves as well as other component failures that could lead to overcooling are identified in the component-level FMEA (Sect. 4.2.2).

An undercooling failure mode of the condensate and FW system is failure to supply sufficient FW to the SGs. RCS undercooling may be caused by MFW system failure in conjunction with an AFW system failure. The contributing component failures and their causes will be addressed in the component-level FMEA.

The condensate and FW system interfaces indirectly with the FW regulating system and with the steam dump and turbine bypass system, which was discussed with the main steam system (Sect. 4.2.1.6). The extent of FW regulating system's interface with the condensate and FW system is discussed below.

4.2.1.12 Feedwater Regulating System. The FW regulating system maintains the SG downcomer level within acceptable limits by positioning the FW regulating valves. In the event of a reactor or turbine trip, FW is ramped down to 5% of full flow. This is accomplished by closing the MFW regulating valves and opening the FW bypass valves to maintain decay heat removal via the SGs.

Failure of the FW regulating system to provide sufficient FW to the SG can contribute to RCS undercooling, and failures that cause excessive FW flow to the SGs, may result in SG overfill.

The significant potential of this system to produce RCS overfill or undercooling is the basis for its inclusion in the component-level FMEA (described in Sect. 4.2.2).

4.2.1.13 Steam Dump and Turbine Bypass Control System. The steam dump and turbine bypass control system provides automatic control of the atmospheric steam dump and turbine bypass valves during both normal and emergency operation. When the main turbine trips at a reactor power level between 8 and 63%, the reactor regulating system proportionally controls the position of the steam dump and turbine bypass valves. When the main turbine trips at reactor power above 63%, the reactor regulating system supplies a quick-opening signal to the valves. Also,

the steam dump and turbine bypass control systems opens the steam dump and turbine bypass valves when the main steam pressure exceeds 895 psia without turbine trip.

Failure of the control system to open the valves would increase main steam pressure. However, the code safety valves are designed to open on high pressure, thus limiting the impact of a steam dump and turbine bypass control system failure.

Failure of the control system to close the valves, once opened, could contribute to a SG blowdown and subsequent RCS overcooling event. The impact of such failures is the basis for inclusion of this system in the component-level FMEA.

4.2.1.14 Turbine Generator Control System. The electrohydraulic (E/H) turbine generator control system is designed to control steam flow to the turbine by operating the main stop, control, and combined intermediate valves.

Failures of the turbine generator control system resulting in excess steam flow to the turbine will result in turbine trip due to an over-speed signal. Failure of the control system to pass sufficient steam to the turbine results in less than optimum turbine operation and eventual turbine trip.

Turbine trip results from numerous control system signals and failures. Turbine trip terminates transients caused by turbine generator control system failures as well as transients resulting from other control system failures. On this basis, the turbine generator control system was not selected for a component-level FMEA at this time.

4.2.1.15 Reactor Coolant Pressure Regulating System. The RC pressure regulating system maintains RCS pressure within specified limits through the use of pressurizer heaters and spray valves. High pressurizer pressure causes the pressurizer spray valves to open, thereby reducing pressure. On low pressure, the heaters are energized to increase system pressure.

Failures resulting in energizing the heaters and terminating the spray would cause a high pressure (~2400 psia), resulting in reactor trip. The high-pressure reactor trip opens both PORVs. In addition, the code safety valves are designed to open at 2500 and 2565 psia, respectively, to limit RCS pressure. The release of RC due to failure of the PORV or safety valves to close is specifically addressed in the RCS FMEA.

Failure of the RC pressure regulating system to close the spray valves could result in slow RCS depressurization. This depressurization, while it may result in reactor trip, is not considered significant.

The potential impact of RC pressure regulating system failures on PORV failure to close is the basis for its selection for acomponent-level FMEA.

4.2.1.16 Pressurizer Level Regulating System. The operating level of the pressurizer is programmed as a function of power to accommodate plant load changes and minimize RCS volume changes. The set point is generated by the reactor regulating system based on RC average temperatures. The pressurizer level regulating system regulates the letdown control valves and the charging pumps in the CVCS. Control is based on a comparison between the measured level and the programmed level.

Failures of the level regulating system can result in a net increase or decrease in RCS inventory (pressurizer level). Increases could lead to liquid discharge through the PORVs and/or safety valves, possibly resulting in valve damage, whereas decreases in level could result in the pressurizer draining following reactor trip and possibly saturating the RC (boiling in the core region). The potential impact of pressurizer level regulating system failures on the RCS inventory was the basis for its selection for further analysis.

4.2.1.17 Turbine Generator and Condenser System. The turbine generator is designed to convert steam from the SGs to electrical energy. The condenser condenses the low-pressure steam from the outlet of the low-pressure turbines and deaerates the resulting condensate.

Failure of the main turbines to trip following reactor trip would result in continued steam flow through the turbine and depressurization of the turbine header, with possible RCS overcooling. However, no failure of a single component has been found that would result in continued blowdown. Typically, failures of single inputs may fail (e.g., that from reactor trip). However, angle backup exists in trips on other parameters (e.g., turbine speed) whose set points would be exceeded following a reactor trip. A delay in turbine trip resulting from postulated failures, although such delays are believed to be constrained to relatively brief intervals, would require detailed thermal-hydraulic analysis to evaluate its effects. For this reason, the bounding complete trip failure was assumed in the sequence analysis (Sect. 4.3). Since the sequence analysis showed the consequences of this bounding failure to be mitigated by safety system response, computer analysis was not undertaken.

Failure of the condenser to condense steam from the low-pressure turbines or the turbine bypass valves would result in turbine trip, closure of the bypass valves, and trip of the MFW pumps. The consequences of this failure are substantially bounded by the transient resulting from loss of nonemergency ac power.

Based on the above, component-level FMEAs were not performed on the turbine generator and condenser systems. However, the identified bounding failures are considered in the sequence analysis.

4.2.1.18 Nitrogen Gas System. The nitrogen gas system pressurizes the SI tanks to 200 psig prior to startup. Although the SI tanks are important components in the low-pressure SI system, the system does not

depend on the nitrogen gas system during operation. Therefore, the nitrogen gas system was not selected for a component-level FMEA because its failure during plant operation would not affect the LPSI function.

4.2.1.19 Electric Heat Tracing System. Electric heat tracing is installed on all piping, valves, and pumps that contain concentrated boric acid. It is designed to maintain the components at 160°F, which is 25°F above the temperature at which a 12% boric acid solution begins to precipitate. Failure of the heat tracing system may cause precipitation of boric acid from the solution, depending on the concentration. Potential effects on the plant include (1) clogged system components and (2) failure to inject concentrated boric acid solution.

Even assuming that failure of the heat tracing would lead to isolation of all high-concentration boric acid sources, the capability of injecting lower concentration, higher capacity flow from the RWT would remain. This would maintain both core heat transfer (RCS inventory control) and the capability, in conjunction with the control elements, of achieving and maintaining a subcritical cold shutdown.

The electric heat tracing system's minimal impact on the RCS is the basis for its exclusion from the component-level FMEA.

4.2.1.20 Plant Ventilation Systems. Three major plant ventilating systems--containment, auxiliary building, and turbine building--have been selected for analysis based on their interfaces with the RCS or key support systems. These systems maintain an acceptable ambient operating environment for plant equipment and personnel. Failure of the ventilating systems could lead to severe operating environments and, potentially, to common-cause equipment failure.

Although consequential failure of fluid system equipment and/or instrumentation is possible due to ventilation system failure, the cause-effect relationships are difficult to assess. Typically, long periods of time elapse between ventilation failure and consequent equipment failure. This period, which may be hours or days, will depend on local equipment heat generation rates, natural convection flow patterns, equipment capabilities, and the responses of plant staff in this time period. In general, the effects of ventilation system failure on RCS overcooling or undercooling, SG overfill, or safety system operation cannot be assessed using FMEA techniques.

4.2.2 Component-Level FMEA

4.2.2.1 FMEA of the Reactor Coolant System. The RCS has been analyzed in detail to identify failures significant to undercooling and overcooling transients and to the operability of plant safety systems.

For this analysis, the RCS was considered to consist of the reactor vessel, the RC pumps, the pressurizer (including the PORVs and the code safety valves), and the quench tank. (A more detailed description of the

RCS as it relates to this analysis is provided in Appendix B.) Interfacing regulating systems such as pressurizer level, pressurizer pressure, and reactor regulating systems were not specifically addressed in this FMEA except when their failure could be identified as a cause of an RCS component failure. FMEAs of these systems have been performed separately.

Twenty-nine RCS failures were postulated and their effects identified. The important ones include failures that may result in LOCAs or contribute to inadequate core cooling following a postulated LOCA. The more significant failures are discussed in the following section and summarized in Table 4.2. The detailed FMEA is provided in Appendix C.

4.2.2.1.1 Significant results. The RCS FMEA identified failures that could potentially result in the following significant effects: (1) unisolable LOCAs, (2) isolable LOCAs, and (3) inadequate core cooling following a LOCA.

1. An unisolable LOCA will occur if an RC pump gross seal failure occurs, or if the pressurizer heaters fail on and result in damage to the pressurizer pressure boundary. With loss of CCW, which can be caused by a control signal or power fault as well as by operator error, a LOCA from a failed RC pump seal can result if the RC pump is not tripped. An RC pump seal failure may result from other failures internal to the RC pumps, including seal component damage from debris or wear, or integral impeller damage.

2. Isolable LOCAs include those failures that can result in the PORVs opening. These typically can be isolated with the motor-operated PORV isolation valves. The power supply for a given PORV isolation valve is separate from the power supply for its associated PORV, which provides improved isolation reliability. Failures that can lead to the PORVs lifting include those that block pressurizer spray, and thus necessitate pressure relief, particularly during a power increase, and those that directly result in the valves opening inadvertently. The PORVs can fail open inadvertently due to a control signal failure, an operator error, or failure to close after a demand to open. Normally, the PORVs are demanded to open on high pressurizer pressure on the RCS channels, which simultaneously initiates a reactor trip. If a PORV opens, the operator should immediately trip the reactor if it has not already tripped.

   Isolable LOCAs also may occur following transients involving pressurizer overfill and the subsequent discharge of saturated water through the PORVs. The liquid discharge increases the likelihood of the PORVs failing to close on demand. If a rising level transient is occurring in the pressurizer and the heaters fail to energize, pressurizer overfill is expected to occur. A pressurizer level transmitter failing low will cause both a rising level transient and no demand for the heaters. Other independent failures can also cause net gains in RCS inventory or a rising level transient (see CVCS FMEA below), which may occur simultaneously with pressurizer

Table 4.2. Reactor coolant system FMEA summary

Failure/Component	Possible Causes	Effects	Remedial Actions
1. SG Tubes Rupture	1. Adverse RCS or SG Water Chemistry 2. Tube Vibration	Reactor coolant (RC) leaks to secondary side of the SG, and to the environment atmospheric dump via SG safety or valves. Depressurization of the RCS would be similar to a LOCA of equivalent size.	Follow SG tube rupture emergency procedures.
2. Reactor Coolant Pump(s) Fail to Trip on Demand	1. Loss of Control Power 2. Operator Error 3. Faulty Trip Relays	The operator is required to trip the RCP's in the event of a LOCA. If the operator fails to trip them, more RCS inventory will be released through the hot leg breaks. The increased rate of coolant loss may be important to recovery from LOCA's depending on the break size. Also, containment isolation isolates CCW to the RCPs and an RCP seal failure may result if the pumps continue to operate. Containment isolation is initiated on high containment pressure (2/4 transmitters). The effect of this additional loss of coolant is expected to depend on break size.	Attempt to manually trip pump breakers.

Table 4.2 (continued)

Failure/Component	Possible Causes	Effects	Remedial Actions
3. RCP Seal Failure	1. Loss of CCW	Seal failure LOCA.	Trip reactor and RCPs. Follow emergency procedures for LOCA.
	2. Seal Component Damage from Debris in System or from Wear		
	3. Integral Impeller Damage (auxiliary impeller for seal water intake or seal water recirculating impeller)		
	4. Seal Area Recirculating Pump Fails (to deliver water to the integral heat exchanger)		
4. Pressurizer Backup Heaters Fail to Trip on Demand or Inadvertently Energize	1. Control Signal Failure (level transmitter fails high, pressure transmitter fails low, etc.)	High pressure results in the pressurizer. If spray is actuated, net effect will be negligible. If pressure transmitter has failed low, spray will not operate. (Heaters can still trip if lo-lo level develops in pressurizer.) Resulting high pressure would normally open PORVs and trip reactor. If reactor trips and pressurizer empties, possible	Attempt to switch heaters to "OFF" position with handswitch or restore to "AUTO" if previously "ON". Manually operate pressurizer spray as required. Manually open breakers if required.
	2. Control Handswitches Left in "ON" Position		
	3. Loss of Control Power		

Table 4.2 (continued)

Failure/Component	Possible Causes	Effects	Remedial Actions
		damage to the pressurizer could occur. If level transmitter fails high, pressurizer will empty with heaters failed on, which may initiate a failure of the pressure boundary (small LOCA).	
5. PORV(s) Fail to Open on Demand	1. Control Circuit Failure 2. Mechanical Failure 3. Loss of Electric Power Supply 4. Block Valves Closed Due to Leaking PORVs	Code safety valves will open on high pressure if the PORVs fail. However, during a LOCA, the RCS cannot be depressurized to prevent PTS conditions as required by procedure. In addition, the PORV's would be unavailable to enhance post-LOCA RCS depressurization and increase the net HPSI flowrate.	Shutdown and repair component(s).
6. PORV(s) Fail Open or Fail to Close on Demand	1. Control Signal Failure 2. Mechanical Failure of Valve	A failed open PORV is an isolatable small LOCA.	Close PORV block valves to terminate loss of coolant. Follow appropriate emergency procedures for a small LOCA.

heater failure. The heaters can be failed by loss of supply power, independent control signal failure, mechanical failure, or the control switch left in the "OFF" position.

3. The last potentially significant effect identified in the RCS FMEA is failure to trip the RC pumps following a hot-leg LOCA (i.e., if they failed to trip on demand or the operator failed to institute RC pump trip early in the LOCA). Continued operation of the pumps during a LOCA would result in greater release of RC. If they later failed or were tripped, the collapse of voids in the coolant may leave the core uncovered. Also, as discussed earlier, failure to trip the RC pumps during a LOCA may lead to an RC pump seal failure because containment isolation would cut off CCW to the RC pumps. The net effect of increasing the rate of loss of RC is unknown. Failure to trip the RC pumps could be caused by a control power failure, faulty trip relays, or operator error.

4.2.2.1.2 Other failures. Other failures identified in the RCS FMEA with notable effects are identified in Appendix C. The effects of these failures generally are not as pronounced or considered to be as significant to undercooling or overcooling transients as those already noted.

4.2.2.2 FMEA of the Chemical and Volume Control System. The CVCS has been analyzed in detail to identify system failures that may affect undercooling and overcooling transients and the operability of plant safety systems. The analysis included postulating failures of a comprehensive list of important CVCS components and evaluating the impact of their failure on system performance. Also addressed were failure of control loop components and signal failure from the interfacing pressurizer level regulating system.

A total of 83 possible failures were identified and considered. The potential effects from these failures resulted in 19 different effects at the system level (i.e., either at the CVCS system boundary or in systems other than the CVCS). These effects fall into six categories:

1. net loss in RCS inventory,
2. net gain in RCS inventory,
3. degradation of water quality in the RCS,
4. dilution of RCS boron concentration (moderator dilution),
5. degradation of SI-initiated charging capability, and
6. other effects.

The effects of most significance to undercooling and overcooling involve net losses and gains in RCS inventory, degradation of SI-initiated charging, and moderator dilution. The failure or degradation of boric acid injection capability on the safety injection/actuation system (SIAS) may be important to plant safety systems. In general, the degraded water quality effects were not considered important to undercooling and overcooling transients and the performance of plant safety systems, but they have been identified for completeness.

Failures in the CVCS generally produce slow effects due to the small capacity of the system, but because they are slow and gradual, they may be more likely to go undetected and culminate in more significant effects.

The more significant failures are discussed here, and a brief discussion of other notable failures is provided in the next section. The detailed FMEA is contained in Appendix C.

4.2.2.2.1 Significant results. The CVCS FMEA identified failures that could potentially result in the following significant effects:

1. net loss in RCS inventory,
2. net gain in RCS inventory,
3. moderator dilution (underborated makeup), and
4. degradation of safety injection flow.

1. Loss of charging flow, excess letdown flow, and instrumentation related pressurizer level drop cause net losses in RCS inventory. In general, net losses in RCS inventory may be important to undercooling transients.

   A loss of charging flow capability involves unavailability of the charging pumps or the charging pump discharge path to the RCS. The RCS impact of loss of charging flow is a drop in the pressurizer level, followed by subsequent runback of the CVCS letdown control valves to maintain RCS inventory. However, the minimum letdown control valve set point is 29 gpm (letdown isolation occurs automatically on SIAS or CVCS signal). Therefore, a net minimum RCS loss of 29 gpm results until and unless the operator isolates letdown flow. This loss rate is not catastrophic, but if it is undetected for an extended length of time, particularly at low power (when the pressurizer level set point is lower), the pressurizer may empty. Loss of charging flow can result if the charging pumps fail or if charging pump suction flow is lost.

   All three charging pumps could be affected by loss of seal and plunger flush water, which is supplied to the pumps from a single reservoir of demineralized water located several feet above the pumps. Low reservoir level is alarmed only locally. Suction flow can be failed by the failure of the volume control tank (VCT) level transmitter (LT-226). This transmitter is a common-leg transmitter to three different controllers. If the transmitter fails high, letdown flow into the VCT is stopped (by the first controller), and eventually the VCT will empty. Normal makeup to the VCT (initiated by the second controller) as well as backup makeup from the refueling water storage tank (initiated by the third controller) will fail, since these are initiated only on low level signals. Failure of the VCT outlet valve in the closed position will also fail the charging pump suction flow. The VCT level will rise, annunciating an alarm, but backup makeup from the RWT will not open automatically because its signal to open is low level. The

effect of these failures, loss of charging flow, would be overcome by an SIAS signal in most cases. However, these failures also affect pump operability and are considered common-cause failure contributors.

Letdown flow in excess of the replacement capability of the charging pumps will result in a net loss in RCS inventory. The maximum letdown flow through the letdown control valve is 128 gpm (4 gpm less than the maximum charging flow). Normally, only one of two letdown control valves is in service; if both are in service at the same time, letdown flow could be as great as 230 gpm. Even with maximum charging flow, a net RCS loss on the order of 100 gpm could occur. However, high letdown flow alarms at 135 gpm on FIA-202, so the transient may be terminated by the operator before the pressurizer level drops significantly.

A drop in pressurizer level may be accompanied by a drop in pressurizer pressure, which may initiate a reactor trip. Any RC shrinkage from the reactor trip would further exaggerate the low pressurizer level. With pressurizer backup heaters energized, high pressurizer thermal stresses will occur during subsequent refill. This can occur if the operating pressurizer level transmitter fails high. This initiates increased letdown flow, tripping of the backup charging pumps, and energizing of the pressurizer backup heaters. The actual low level will not be transmitted as is required to trip the heaters or actuate low-level alarms. Low pressurizer level will not initiate an SIAS, although low pressurizer pressure will. This failure mode is also identified in the FMEA of the pressurizer level regulating system.

2. A net gain in RCS inventory will lead to a rise in pressurizer level. Assuming that makeup to the VCT is maintained, a net gain in RCS inventory may open the PORVs and contribute to failure of the valves to close if saturated water passes through them. Those effects identified from the FMEA that represent a net gain in RCS inventory include loss of letdown flow and excess charging flow (assuming VCT makeup).

   Isolation of letdown flow will lead to a rise in pressurizer level. Backup charging pumps normally are tripped on high pressurizer level, but one charging pump normally operates continuously at a nominal rate of 44 gpm and it could pressurize the RCS. If the VCT makeup circuits are in automatic, a net RCS gain of 44 gpm could fill the pressurizer in the long term and result in PORV lift unless the operator intervenes. Letdown flow indication, pressurizer level, and decreasing VCT level should alert the operator to trip the operating charging pump. If the VCT makeup is in manual, the operating charging pump could be damaged if the VCT is allowed to drain.

   Letdown flow can be blocked by any operating letdown line valves failing closed, including the letdown isolation valve, the letdown

stop valve, the excess flow check valve, the letdown control valve, and the backpressure regulating valve. Loss of instrument air can cause all but the excess flow check valve to fail closed, including the parallel standby valves. A control signal failure can also fail all but the excess flow check valve.

The pressurizer overfill transient initiated by loss of letdown flow can be terminated if the operator trips the operating charging pump.

Other failures with effects resulting in pressurizer overfill involve inadvertent or excess charging flow caused by control malfunctions. The charging pumps can fail to trip on demand due to loss of control power on the 125-V dc buses, but only two pumps could fail on with a single control bus failure. The letdown control valve could offset any gain from two pumps failed on. However, loss of power to the pressurizer level regulating system relays or bistables would start all charging pumps and run back letdown flow, resulting in a net RCS inventory gain of 99 gpm. A 99-gpm gain would also occur if the operating pressurizer level transmitter failed low, since this would also start all charging pumps and run back letdown flow. Similarly, if the pressurizer level set-point signal from the reactor regulating system failed high, the correct pressurizer level would appear low, backup charging pumps would be started, and letdown flow would be run back. These control failures would also prevent the pressurizer heaters from energizing.

3. Those effects identified from the FMEA that represent boron dilution in the RC include failure or degradation of the boric acid injection capability on SIAS as well as underborated makeup under normal operating conditions. Moderator dilution during normal operation is easily detected by the boronometer or by increased power level. It can be important during post-trip cooldown but is not expected to have a significant effect on the transients of interest here.

   The CVCS can provide 132 gpm of concentrated boric acid to the RCS on SIAS, but the FSAR does not take credit for CVCS operation in the analysis of steam line breaks or excess load events where boric acid injection is utilized. For these events, the FSAR indicates that the RCS pressure drops rapidly (within 100 s) to the shutoff head of the HPSI pumps, 1280 psia, resulting in adequate delivery of dilute boric acid from the RWT to the RCS.

   Concentrated boric acid injection capability on SIAS can be degraded or failed by CVCS failures related to heat tracing, valve operation, or charging pump operation. Heat tracing failure in the path from the boric acid storage tank(s) to the charging pump suction can result in blocked flow from boric acid precipitation in the lines. Failure of the SIAS signal to the appropriate valves and pumps will fail the boric acid SI capability. It is noted that these failures do not affect the ability of the CVCS to inject water from the RWT in the injection mode unless the charging pumps have been failed.

4. The SI flow provided by the CVCS includes 132 gpm of concentrated boric acid solution supplied to the RCS by all three charging pumps on an SIAS. The charging pumps are not likely to fail from loss of power because they are powered by diesel-backed buses. They potentially can be failed, as previously described, by failures simultaneously affecting the operability of the three pumps.

   The more significant failures from the FMEA discussed here are presented in Table 4.3, which groups the failures according to effects and includes the possible causes, potential effects, and remedial actions available to the operators. The detailed FMEA in Appendix C presents this information for all postulated failures, grouped by CVCS subsystems.

4.2.2.3 FMEA of the Pressurizer Level Regulating System. The pressurizer level regulating system has been analyzed in detail to identify failures that could affect undercooling and overcooling transients and the operability of plant safety systems. The 24 failures postulated include vital power, nonvital instrument power, operating level transmitter, input set-point signal, operating bistables, controller, and associated relays. Some of the failures considered were also considered in the FMEA of the CVCS since a direct interface exists between the CVCS and the pressurizer level regulating system.

The more significant failures are discussed, followed by a discussion of other less significant failures identified in the FMEA. The detailed FMEA and a brief description of the pressurizer level regulating system are provided in the appendixes.

4.2.2.3.1 Significant results. Failures in the pressurizer level regulating system can potentially result in the following significant effects: (1) pressurizer overfill combined with either a high-pressure or low-pressure transient, and (2) potential overheating of the pressurizer pressure boundary (precursor to an unisolable LOCA).

1. The pressurizer overfill effect results from failures that induce the letdown control valve to close and the backup charging pumps to start. This will typically produce a net RCS gain of 99 gpm and occurs after any one of the following failures: loss of vital power from the operating bus (1Y01 or 1Y02), loss of the nonvital instrument bus (1Y10), failure of the operating level transmitter on the low side, and failure of the pressurizer level set point (from the reactor regulating system) on the high side. These failures also preclude operation of the pressurizer heaters. Thus, depending on which mechanism is controlling, a decreasing pressure transient may occur from loss of the heaters, or an increasing pressure transient may occur from operation of all three high discharge head charging pumps. A high-pressure transient could lead to lifting of the PORVs and the possibility of their failure to close due to damage from the liquid discharge.

Table 4.3. Chemical and volume control system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
Net Loss in RCS Inventory			
1. Charging Pumps Fail	1. Common cause mechanical failure (broken diaphram, inlet check valve failed etc.) 2. Loss of seal and plunger flush water from overhead supply tank 3. Blockage due to loose parts, debris or resin beads in system	Loss of charging flow to RCS. If only one pump has failed, pressurizer level will drop and initiate the second and/or third pump to resume charging flow. If charging pumps are unavailable, pressurizer level will drop and initiate runback of letdown (minimum setpoint of 29 gpm). Net RCS loss of 29 gpm.	Isolate letdown. Shutdown plant if pressurizer level has dropped too low.
2. Charging Line to Regenerative Heat Exchanger and RCS Plugs (HX Inlet Valve, HX Tubes, or FE-212 Plugs)	1. Loose parts, boron buildup, or debris in line 2. Operator error related to valve closure	Loss or reduction of charging flow to RCS. Blockage may cause high pressure at charging pump discharge, and subsequent opening of the charging pump discharge relief valves. Pressurizer level will drop and initiate runback of letdown (minimum setpoint of 29 gpm). Net RCS loss of 29 gpm.	Isolate letdown. Shutdown plant if pressurizer level has dropped too low to operate.
3. VCT Outlet Valve (CVC-501-MOV) Fails Closed	1. Inadvertant signal from makeup controller or SIAS	VCT level will rise, resulting in letdown flow getting diverted to the waste pro-	Isolate letdown and manually operate makeup valve CVC-504-MOV as required.

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
	2. Obstruction (plugged valve)	cessing system. Since, the RWT makeup valve (CVC-504-MOV) does not open automatically on high VCT level, charging flow to the RCS will be lost, causing pressurizer level to drop. Letdown will run back to its minimum setpoint of 29 gpm, but will not isolate automatically. Net RCS loss of 29 gpm.	
4. VCT Level Transmitter (LT-226) Fails High	1. Power surge fails power supply regulator 2. Internal components fail 3. Automatic control mode assumed.	Failure causes controller LC-227 to divert letdown flow from VCT to the waste processing system and causes LC-226 to fail to provide needed automatic makeup to the VCT as the VCT level drops. The failure also causes controller LC-227 to fail to initiate makeup from the RWT, when VCT level is actually low, resulting in loss of flow to the charging pumps and loss of charging flow to the RCS. The VCT could empty on the order of half hour from the transmitter failure.	Manually initiate makeup from the RWT and then realign VCT letdown inlet valve to the VCT. Failure may be hard to detect since low level indication and alarm will be failed.

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
5. Letdown Control Valves (CVC-110P -CV and CVC-110Q -CV) Fail Open	1. Mechanical failure 2. Failure of the bias control regulator on each valve 3. Erroneous control signal from pressurizer level 4. Operator puts both valves in service (in error)	Excess letdown flow, even though both backup charging pumps start on low pressurizer level. Net decrease in RCS inventory and pressurizer level (maximum letdown 230 gpm - maximum charging 132 gpm = 98 gpm). The inventory loss will be accompanied by a pressure drop in the pressurizer, which will energize the heaters. Heaters will de-energize on lo lo pressurizer level.	Close letdown stop valves. Detect failure in CVCS with high level alarm in VCT and high letdown flow.
6. Pressurizer Level Transmitter Fails High (LT110X or LT110Y)	1. Power surge fails power supply regulator 2. Capacitance bridge circuit fails or other internal components fail	Letdown control valve opens, while any operating backup charging pumps trip. VCT fills. Level in pressurizer drops. Pressurizer backup heaters energize on initial high level signal and on subsequent low pressurizer pressure accompanied by the inventory loss. Heaters would not de-energize on actual low level in pressurizer as designed due to the transmitter failure. Net loss in RCS inventory of 84 gpm. With incorrect operator response (opening other	Assume manual control of CVCS components. Failure may be harad to detect, low pressure transient may be only indication. Switch to alternate regulating system (i.e., system X if Y transmitter is failed).

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
		letdown control valve and tripping last charging pump) net letdown flow could be as high as 230 gpm.	
Net Gain in RCS Inventory			
7. Letdown Stop Valve (CVC-515-CV) or Letdown Containment Valve (CVC-516-CV) Fail Closed	1. Inadvertant or erroneous signal to close, including a. ESFAS (SIAS or CVCS isolation signal) b. High regenerative HX outlet temperature TIC-221 2. Loss of instrument air 3. Loss of control power to solenoid 4. Mechanical failure including plugging from loose parts	Letdown flow is stopped, including flow through the regenerative heat exchanger (HX), which usually heats charging flow. Pressurizer level will rise, backup charging pump will trip, but the main operating charging pump will continue to discharge to the RCS. With charging flow from the remaining pump at 44 gpm, RCS could overpressurize, causing the PORV to open.	After detecting failure, monitor pressurizer level and charging flow temperature (TE-229). Trip charging pump if level in pressurizer is too high.
8. Excess Flow Check Valve Fails Closed	1. Mechanical failure 2. Plugging	Same as above (loss of letdown flow).	Same as above.
9. Operating Letdown Control Valve (CVC-110P-CV) or CVC-100Q-CV) Fails Closed	1. Loss of instrument air 2. Loss of solenoid control power 3. Mechanical failure 4. Control signal failure	Same as above (loss of letdown flow).	For both valves failing, isolating charging flow is required. If only one of the two valves fails, place the standby valve in service (requires manual alignment of valves).

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
10. Operating Letdown Backpressure Regulating Valve (CV-201P or CV-201Q) Fails Closed	1. Loss of instrument air 2. Pressure controller or transmitter (PT-201) fails low (loss of power) 3. Mechanical failure	Same as above (loss of letdown flow).	Monitor pressurizer level and RCS pressure. Trip charging pump, if necessary.
11. Ion Exchanger(s) Plug(s) or Strainer Plugs	1. Heat damage 2. Loose parts 3. Bad resin supply 4. Resin bed support structure fails	Initial loss or reduction of letdown flow. PDIS-204 alarms at 20 psid. VCT level will decrease and initiate makeup water if in automatic. Net plant as gain in RCS inventory of 44 gpm from the operating charging pump.	Letdown flow can be switched at CVC-520-CV to bypas ion exchangers. Monitor RC chemistry and shutdown plant
12. Operating Letdown Backpressure Regulating Valve (CV-201P or CV-201Q) Fails Open (normally fail closed on loss of air)	1. Pressure controller or transmitter (PT-201) fails high 2. Mechanical failure 3. Operator error	RCS fluid downstream of letdown control valve may flash to steam due to drop in line pressure. If fluid temperature is above 145°F, TE-224 should switch flow to VCT and bypass boronometer and radiation monitor. If temperature is below 145°F, steam pockets may exist and damage monitors. High velocity flow may damage the purification filter with debris either blocking let-	Isolate letdown. Check system flows and filter pressure drop to detect filter damage. If filter is not damaged attempt throttling of manual valves associated with one of the failed regulating valves. If failure is not caused by pressure transmitter failures, place the standby regulating valve in service.

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
		down flow or eventually failing the charging pumps. Net effect on RCS inventory may be minimal if charging pumps and letdown are failed simultaneously.	
13. Loss of Non-Vital Power to Regulating System Relays (AC bus 1Y10) or Loss of Vital Power to Regulating System Bistables (bus 1Y01 or 1Y02)	1. Loss of power to bus 2. Fault on bus	Letdown control valve closes, backup charging pumps start and all pressurizer heaters de-energize. Net RCS gain of 99 gpm. Pressurizer high level transient with potential for high pressure transient from operating charging pumps or low pressure transient if loss of heaters is controlling.	Assume manual control of letdown valve and charging pump operation. If power on 1Y01 or 1Y02 failed utilize the unfailed power supply to resume pressurizer level control. Pressurizer heaters can also be turned on manually.
14. Pressurizer Level Transmitter Fails Low (LT110X or LT110Y)	1. Loss of power to transmitter (bus 1Y01 or 1Y02) 2. Internal transmitter components fail	High level transient in pressurizer. Letdown control valve closes, backup charging pumps start, and pressurizer heaters de-energize. Potential high pressure transient in pressurizer with potential to open PORV's, or low pressure transient if loss of heaters is controlling.	Switch to alternate regulating channel (i.e., channel X if Y transmitter is failed). Assume manual control of CVCS components (trip pump and isolate letdown as required).

Table 4.3 (continued)

Failure	Possible Causes	Effects	Remedial Actions
15. Pressurizer Level Setpoint (from reactor regulating system) Fails High	1. Signal fault 2. Setpoint device fault	Pressurizer overfill if VCT makeup maintained. Correct pressurizer level will appear low and extra charging pumps and runback of letdown flow will be initiated, resulting in overfill of the pressurizer. High pressurizer level will appear normal and correct control response (energize heaters, stop backup charging pumps, and increased letdown) will not occur.	Switch to alternate regulating system (X or Y) on detection of failure. Adjust RCS inventory with CVCS.
<u>Degradation of SI Initiated Charging Capability</u>			
16. Spare Charging Pumps Fail to Start on SIAS Demand	1. Power supply failure (4 KV Bus 11 or 4 KV Bus 14) 2. Mechanical failure 3. Control signal failure	Potentially only 1/3 capacity CVCS boric acid flow delivered to the RCS on SIAS demand. Reduced shutdown margins achieved.	Manually start charging pumps on detection of failure, if pumps are not failed mechanically.
17. SIAS to CVCS Components Fails on Demand	1. Control signal failure	Automatic delivery of concentrated boric acid from CVCS (132 gpm design flow) is failed.	Initiate emergency boration alignment on detection of failure. Based on analyses which demonstrate safe conditions without assuming charging injection, flow from CVCS is probably not required on SIAS, but provides a safety margin.

The relays that start the charging pumps and turn off the backup heaters in the automatic control mode deenergize to initiate these responses. Thus loss of power to the relays energizes the pumps and deenergizes the heaters. The letdown control valve closes on loss of power as well. Loss of vital bus 1Y01 or 1Y02 (redundant power supplies with one selected) results in no output from the level transmitter, which is interpreted as low level and a demand to close. Loss of nonvital bus 1Y10 results in no signal from the limiter to the letdown valve, which is also interpreted as a demand to close. Failure of the level set-point signal on the high side (from the reactor regulating system) leads to the same response, because the correct pressurizer level will be interpreted as too low.

The overfill transient resulting from these failures can be terminated by manually tripping the charging pumps. The pressurizer heaters can also be switched from their failed state in "AUTO" to "ON" or "OFF" as required to restore pressurizer pressure.

2. A low-level transient in the pressurizer in combination with the pressurizer heaters energized is a potential cause of damage to the pressurizer pressure boundary on refill. The low level with heaters energized can result from failure of the operating pressurizer level transmitter on the high side. The system will respond to the high-level signal by emptying the pressurizer and energizing the backup pressure heaters. With the transmitter failed high, no low-low level signal will develop and the heaters will not deenergize as they normally would on low-low level.

   Similarly, with the level set-point signal from the reactor regulating system failed low, the correct pressurizer level will appear too high and the system will respond by emptying the pressurizer and energizing the backup pressurizer heaters. But, because the low-low level set point that switches the heaters off is independent of the set point programmed from the reactor regulating system, this failure will not by itself lead to pressure boundary damage.

   There are two component failures associated with the low-low set-point control that could be precursors to an unisolable LOCA if a low-level transient were to develop in the pressurizer. These are failures of the low-low bistable LC-110XL (or LC-110YL) in the closed position, and failure of the associated relays (63XA/LC-110L or 63XB/LC-110L) to open on demand. Either of these failures will prevent the pressurizer heaters from deenergizing on low-low level demand. The bistable and the relays (in series) are normally energized closed and open when deenergized to deenergize the heaters. If the bistable fails closed, the relay circuit remains energized and the heaters will remain energized. Although the heaters can be deenergized on high pressure, high pressure is not expected to exist during a low-level transient. In any case, the heaters can be deenergized manually by switching the heater control from "AUTO" to "OFF."

3. Pressurizer heater control failure can also result in a low-pressure transient. If the bistable or the relays associated with the low-low level set point fail in their "fail-safe" deenergized state, the heaters will deenergize. This would occur if the operating bistable (LC-110XL or YL) or the relays (63XA/LC-110L and/or 63XB/LC-110L) failed open. Loss of power or electric power circuit component failures can cause this.

   The more significant failures discussed here are presented in Table 4.4 in the format in which the detailed FMEA was developed (see Appendix C). This format identifies postulated failures, possible causes, potential effects, and remedial actions available to the operator. A complete listing of pressure regulating system failure modes and their effects is provided in Appendix C.

4.2.2.4 FMEA of the Reactor Coolant Pressure Regulating System. A FMEA of the RC pressure regulating system was performed to identify the impact of component failures on RCS undercooling and overcooling and on the operability of standby safety systems. The 13 failures postulated included failure of vital power, nonvital instrument power, pressure transmitter, controllers, and associated bistables. Failure of relays that interface with the system from the pressurizer level regulating system was covered in the FMEA for the level regulating system. Both regulating systems provide control of the pressurizer backup heaters. Descriptions of both systems are contained in Appendix B.

The results of the detailed FMEA for the RC pressure regulating system are highlighted in this section. The detailed FMEA can be found in Appendix C.

4.2.2.4.1 Significant results. Failures in the RC pressure regulating system do not result in effects significant to undercooling, overcooling, or the operability of standby safety systems. The most noteworthy effects would lead to a high-pressure transient, which may open the PORVs, or to a low-pressure transient, which would be followed by a thermal margin/low-pressure reactor trip. At lower pressures, SIAS would initiate. Since the operators trip two RC pumps on SIAS, low-pressure transients caused by uncontrolled pressurizer spray may be terminated. Even if the operator failed to trip the pumps and saturation conditions were reached in the core, the condition would not be significant.

A PORV lift in itself would not contribute to inadequate core cooling or an uncontrolled decrease in RCS temperature. In this event, the PORVs operate as designed to control the transient. Unless the PORVs failed to close due to an independent failure mechanism, the pressure regulating system failure did not lead to effects of concern.

The RC pressure regulating system failures that do result in a low-pressure transient involve either the pressurizer heaters in a deenergized state or inadvertent actuation of the pressurizer spray flow. Loss of power on Instrument Bus 1Y09 will cause both the proportional

Table 4.4. Pressurizer level regulating system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
Pressurizer Overfill			
1. Loss of Non-Vital Power to Regulating System Relays (AC bus 1Y10)	1. Loss of power to bus 2. Fault on bus	Letdown control valve closes, backup charging pumps start and all pressurizer heaters de-energize. Pressurizer high level transient with potential for high pressure transient from operating charging pumps or low pressure transient if loss of heaters is controlling.	Trip charging pumps as required. Turn on pressurizer heaters manually as required to increase pressure. Manual control on letdown valve is lost. If bus is not faulted, manually align backup bus 1Y09.
2. Loss of Vital Power to Regulating System Bistables (bus 1Y01 or 1Y02)	1. Loss of power to bus 2. Fault on bus	Same as above.	Assume manual control of letdown valve and charging pump operation. If power on 1Y01 or 1Y02 failed utilize the unfailed power supply to resume pressurizer level control. Backup for 1Y01 and 1Y02 is also available from bus 1Y11. Pressurizer heaters can also be turned on manually.
3. Pressurizer Level Transmitter Fails Low (LT110X or LT110Y)	1. Loss of power to transmitter 2. Internal transmitter components fail	High level transient in pressurizer. Letdown control valve closes, backup charging pumps start, and heaters de-energize. Potential high pressure transient from operating charging	Switch to alternate regulating channel (i.e., channel X if Y transmitter is failed). Assume manual control of CVCS components (trip pump and isolate letdown as required).

Table 4.4 (continued)

Failure	Possible Causes	Effects	Remedial Actions
		pumps or low pressure transient if loss of heaters is controlling.	
4. Pressurizer Level Setpoint (from reactor regulating system) Fails High	1. Signal fault 2. Setpoint device fault	Pressurizer overfill if VCT inventory maintained. Correct pressurizer level will appear normal and runback of letdown flow will be initiated, resulting in overfill of the pressurizer. High pressurizer level will appear normal and correct control response (energize heaters, stop charging pumps and increase letdown) will not occur. May not overfill pressurizer, but on power increase, significant expansion of coolant may lead to overfill.	Switch to alternate regulating channel (X or Y) on detection of failure. Adjust RCS inventory with CVCS.
Potential Precursor to Pressurizer Damage			
5. Pressurizer Level Transmitter Fails High (LT110X or LT110Y)	1. Power surge fails power supply regulator 2. Capacitance bridge circuit fails or other internal components fail	Letdown control valve opens, while any operating backup charging pumps trip. Level in pressurizer drops. Pressurizer backup heaters energize on initial high level signal. Heaters would not de-energize on actual low	Assume manual control of CVCS components. Failure may be hard to detect, volume control tank high level may be only indication. Switch to alternate regulating channel (i.e., channel X if Y transmitter is failed).

Table 4.4 (continued)

Failure	Possible Causes	Effects	Remedial Actions
		level in pressurizer if redundant transmitter also failed. Net loss in RCS inventory of 84 gpm. With incorrect operator response (opening other letdown control valve and tripping last charging pump) net letdown flow (RCS loss) could be as high as 256 gpm.	
6. Lo-Lo Bistable (LC-110XL or LC-110YL) Contacts Fail Closed (assumed normally energized closed)	1. Contact short or arcing caused by corrosion, aging, moisture, swell, etc.	On low low level, heaters will not de-energize. Charging pumps will still energize and letdown control valve will close on demand. Potential damage from dry heater operation if low low level exists. Lo-lo level alarm may also be failed, but low level alarm will be operable.	Switch to alternate regulating channel (X or Y) to utilize redundant operable bistable. Switch manual heater control from "AUTO" to "OFF".
7. Relays (LC-110L) Fail to Open On Demand (when de-energized and when lo lo level exists)	1. Contact short or arcing caused by corrosion, moisture, aging, etc.	Heaters will not automatically de-energize on lo lo level.	Manually switch heaters off on lo lo level alarm.

Table 4.4 (continued)

Failure	Possible Causes	Effects	Remedial Actions
Low Pressure Transient			
8. Relays (LC-110L) Fail Open (normally energized closed)	1. Loss of power 2. Failure of electric power circuit components	Heaters would fail to energize on demand. Could lead to low pressure transient in RCS. Also degraded level control on high level in pressurizer.	Monitor RCS pressure. Manually control heaters as required.
9. Lo-Lo Bistable (LC-110XL or LC-110YL) Contacts Fail Open (assumed normally energized closed)	1. Loss of power resulting in failure to deenergized position 2. Failure of electric power circuit components	Even if level was not low, or if pressure was low, pressurizer heaters would de-energize, resulting in slow pressure decrease in the pressurizer.	Switch to alternate regulating channel (X or Y) to utilize redundant operable bistable.

and backup heaters to deenergize, initiating a slow decrease in pressure. Full capacity spray flow can be actuated inadvertently by (1) failure of the operating pressure transmitter on the high side, (2) failure of the proportional controller on the high side, or (3) failure of the actual spray controller on the high side. Heat input capacity from the pressurizer heaters is not enough to offset the cooling provided by full pressurizer spray flow; thus a pressure decrease would occur.

A high-pressure transient can develop from the operating pressure transmitter failing low. This will close the spray valves, energize the pressurizer heaters, and annunciate a low-pressure alarm. Without operator intervention, the pressure will cause the PORVs to lift and the reactor to trip on high pressure.

Inadvertent pressure alarms (high or low) may induce the operator to mistakenly adjust the pressure in the wrong direction via manual control of the heaters and spray valves. The pressure effects, though, would be bounded by either a high- or low-pressure reactor trip. Other identified possible failures would be countered by automatic system response, or their effects would be bounded by high- or low-pressure reactor trip.

Table 4.5 contains a selection of the more significant RC pressure regulating system failures taken from the complete FMEA in Appendix C.

4.2.2.5 FMEA of the Reactor Regulating System. The RRS has been analyzed in detail to identify failures that would affect undercooling and overcooling transients and the operability of plant safety systems. The system was analyzed based on the configuration in use at Calvert Cliffs. As originally designed, it was intended to serve as a reactor power controlling system. It was to have automatic control element drive capabilities, along with a coupled variable pressurizer liquid volume change signal to the pressurizer level control system and an RCS temperature signal to actuate the atmospheric dump and turbine bypass valves' control circuits following turbine trip.

Although the automatic control element assembly (CEA) control feature has been removed, the RRS continues to provide pressurizer level and steam dump valve automatic control signals and alarm signals. The RRS processes RCS temperature and turbine pressure signals to generate these control and alarm signals.

4.2.2.5.1 Significant results. During power operation, failures of RRS components or inputs were found to have minimal effect. Failure can result in a modified pressurizer level set point and spurious alarms that may result in the operator manually changing reactor and turbine power level. However, reactor or turbine trip is not expected as a consequent effect.

Failure in the steam dump demand circuits or their RCS temperature inputs can generate a signal that would open the atmospheric dump and turbine bypass valves following turbine trip (the signal is blocked

Table 4.5. Reactor coolant pressure regulating system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
1. Pressure Transmitter (PT-100Y or PT-100X) Fails Low	1. Loss of power on operating vital bus (1Y01 or 1Y02) 2. Loss of power to transmitter (faulted wires, etc.) 3. Internal transmitter components fail	A zero current demand signal will be produced indicating a low pressure condition. Pressurizer spray valves will close, all pressurizer heaters will energize and a low pressure alarm will annunciate. Actual pressure will increase due to heater operation, which will cause the PORVs to lift. If fault is loss of vital power and pressurizer level regulating system is on same bus, all heaters will de-energize on a false lo-lo level signal. The spray valves will still be closed and a low pressure alarm will still annunciate, but no transient will develop. If a high pressure transient did develop, manual response would be required to open spray valves. If low pressure existed, the heaters could not be energized as required, even manually. A decrease in pressure would occur with an eventual	Switch to alternate regulating channel (X or Y) to utilize operable alternate transmitter. Also utilize manual control of heaters and/or spray, as required.

Table 4.5 (continued)

Failure	Possible Causes	Effects	Remedial Actions
		thermal margin/low pressure reactor trip.	
2. Pressure Transmitter (PT-100Y or PT-100X) Fails High	1. Power supply regulator fails due to power surge 2. Internal transmitter components fail	Spray valves will open fully, all heaters will de-energize, and high pressure alarm will annunciate. Actual pressure will decrease due to 375 gpm spray flow at 548°F. Reactor trip will have occurred by 1750 psia from thermal margin/low pressure trip (assume RT pressure transmitters are separate from regulating system transmitter).	Switch to alternate regulating channel (X or Y) to utilize operable alternate transmitter. Isolate spray with manual controller and manually energize heaters as required.
3. Proportional Controller (P1C-100Y or P1C-100X) Fails High	1. Power surge 2. Component short or arcing or other internal component failure	Pressurizer spray valves are opened and proportional heaters are de-energized. Pressure decrease in pressurizer, which cannot be offset by backup heaters. Low pressure alarm will annunciate. Eventual thermal margin/low pressure reactor trip. Pressure may continue to drop. At 1600 psia safety injection signal will actuate.	Isolate spray with manual control. Utilize alternate regulating channel for continued operation.

Table 4.5 (continued)

Failure	Possible Causes	Effects	Remedial Actions
4. Spray Valve Controller (1Y09) Fails High	1. Power surge 2. Component short or arcing or other internal component fault	Pressurizer spray fails on (375 gpm max). Pressure decrease in pressurizer which cannot be offset by heaters. Low pressure alarm will annunciate. Eventual thermal margin/ low pressure reactor trip will occur. Pressure may continue to drop. At 1600 psia safety injection signal will actuate.	Isolate spray with manual control.
5. Loss of Non-Vital Power on Bus 1Y09	1. Loss of power to bus 2. Fault on bus	Pressurizer spray valves will close and backup heaters will de-energize. Proportional heaters will also fail off. Low pressure transient will develop. May get low pressure alarm.	Energize backup heaters manually (with handswitch) as required to restore pressure.

unless the turbine is in a tripped state). Thus, if a RCS high T_{avg} was generated due to an RRS failure and the turbine subsequently tripped, an overcooling transient equivalent to a small steam line break would occur.

Specific failures of the RRS and their effects are listed in Table 4.6.

4.2.2.6 FMEA of the Condensate and Main Feedwater System. A FMEA of the condensate and MFW system was performed to identify the impact of component failures on RCS undercooling and overcooling, SG overfill, and operation of standby safety systems. The FMEA identified component failures that would affect SG overfill and RCS undercooling. Specific major failures leading to SG overfill and RCS undercooling are identified in Table 4.7, which is a summary of the FMEA performed for the condensate and MFW system. The detailed FMEA of this system can be found in the Appendix C. Each major SG overfill and RCS undercooling failure identified is discussed in the following section, and a simplified description of the condensate and MFW system can be found in Appendix B.

4.2.2.6.1 Significant results. The FMEA performed on the condensate and MFW system identified five important failure modes, three of which involve potential overfill of the SG. The other two failure modes involve potential RCS undercooling resulting from failure to provide adequate FW to the SGs.

Steam generator overfeeding will occur if the FW regulating valve fails open, or if the FW regulating valve fails to close following a reduction in FW demand (e.g., reactor trip). SG overfill will also occur if the operator fails to override the bypass valve for an extended period following turbine trip. Failing the control valve open would be expected to have a greater impact at lower reactor power levels, while failure to close would be more severe at higher reactor power levels. Below 15% power, the smaller diameter bypass FW regulating valve automatically controls FW flow to maintain SG level. The impact of bypass valve failure in the open position is not expected to result in a rapid overfill transient because the relatively slow transient gives the operator more time to take manual remedial actions.

Failure of either FW regulating valve in the open position could occur due to:

1. mechanical failure of valve or operator,
2. controller failure opens valve, or
3. erroneous inputs to the controller.

If one of the MFW regulating valves fails open, the operator may be able to manually control the main valve or close the motor-operated isolation valve and isolate the affected SG. The operator may also trip the MFW pumps, which would result in automatic actuation of the AFW system on

Table 4.6. Reactor regulating system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
1. Quick Opening Bistable Failures High or Tav Error ($T_{av}-T_{ref}$) Fails High	1. Bistable fails high	Places the turbine bypass valves and the atmospheric steam dump valves in a failed state such that following turbine trip the valves would be opened and would remove more heat than required by the RCS conditions.	Manually close or isolate open valves.

Table 4.7. Main feedwater and condensate FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
Steam Generator Overfill			
1. Feedwater Regulating Valve (FW 1111 or 1121) Fails Open	1. Mechanical Failure of Valve or Operator 2. Controller Failure (FC 1111) Opens Valve 3. Erroneous Controller Inputs	SG level increases initiating turbine and reactor trip. Prior to turbine trip, overfill of the SG may result in carryover of moisture into the main turbine, causing turbine blade erosion and/or failure. Following turbine trip, the regulating valve will be signaled to close and the bypass opened. SG overfill potential exists if the valve remains open. Substantial injection of water into steam lines could jeopardize steam line integrity.	Operator should attempt to throttle the valve manually if possible and, if required, trip the main feedwater pumps manually to prevent SG overfill. Confirm subsequent automatic initiation of auxiliary feedwater. Operator should manually override the controller if it is the problem. Operator also may attempt to isolate or control flow using the motor operated isolation valve.
2. Feedwater Regulating Valve (FW 1111 or 1121) Fails to Close Following Turbine Trip	1. Mechanical Failure of Valve or Operator 2. Loss of Pneumatic Supply While Valve is Open a. Loss of Instrument Air Supply	Following reactor trip, SG level will increase. Unless controlled, the SG overfeed will result in injection of water into the steam lines. Extensive injection could jeopardize steam line integrity.	Operator should attempt to throttle the valve manually and, if required, trip the main feedwater pumps prior to overfilling SG. Confirm the subsequent automatic initiation of auxiliary feedwater.

Table 4.7 (continued)

Failure	Possible Causes	Effects	Remedial Actions
	b. Isolation of Pneumatic Supply Due to Solenoid Valve Failure or Failure of 120 VAC Buses Y09 or Y10		
	3. Controller (FC 1111, 1121) Fails to Close Valve		
3. Feedwater Regulating Bypass Valve (FW 1105, 1106) Remains Open Following Reactor/Turbine Trip	1. Control Room Operator Fails to Throttle Bypass Valve Manually Following Reactor Trip 2. Mechanical Failure of Valve or Operator 3. Controller (LIC 1105, 1106) Fails	Following reactor trip, the main feedwater regulating valves close and the bypass open to maintain 5% flow. As the residual heat generated in the core decreases, the SG level will begin to increase slowly. The control room operator is required to throttle the bypass valves manually to maintain SG level. If the valves are not throttled, SG overfill could occur.	Operator should throttle bypass valve manually if possible. If required, isolate flow path or trip main feedwater pumps prior to SG overfill.

Table 4.7 (continued)

Failure	Possible Causes	Effects	Remedial Actions
RCS Undercooling			
4. Degraded Feedwater Flow to Steam Generator	1. Loss of 13 kV Service Bus 11 Coupled With Loss of Diesel Generator Power	Trips Condensate and Condensate Booster pump resulting in the loss of main feedwater flow. It also trips motor driven auxiliary feedwater pump. Steam driven auxiliary feedwater pump is not impacted.	Restore bus.
5. Degraded Feedwater Flow to Steam Generator	1. Loss of 4 kV Bus 11 Resulting in Isolation of the 13 kV Service Bus 11 From the 500 kV Bus	Trips Condensate and Condensate Booster pump resulting in the loss of main feedwater flow. It also fails to power motor driven auxiliary feedwater pump. Steam driven auxiliary feedwater pump is not impacted.	Restore bus.

low SG level. If the operator fails to trip the MFW pumps, no automatic trip of the FW pump turbines upon high SG level would occur.

It should be noted that failure of the FW bypass valve (above 15% power) in the open position would cause SG overfill only if the FW regulating valve controller failed to compensate as designed.

Following turbine trip, the FW regulating valve is signalled to close. Failure of either FW regulating valve to close could occur due to

1. mechanical failure of valve or operator,
2. loss of pneumatic supply while valve is open, or
3. failure of the controller to close the valve.

Loss of instrument air or failure of 120-V ac control power will result in closure of the pneumatic supply and discharge valves on the regulating valve operators. The main and bypass FW regulating valves would then fail in the "as is" position. The operator has the option of manually controlling the FW regulating valves or tripping the FW pumps. If necessary to control SG level, the operator may trip the MFW pumps and verify the initiation and control of AFW.

When the turbine trips, the FW regulating valves are closed and the bypass valves are opened by the trip set controller to permit 5% of total FW flow to the SGs. This action permits decay heat removal from the core. If the bypass valve remains open for an extended period, SG overfill may result. The valve could remain open due to

1. operator failure to throttle the bypass valve,
2. mechanical failure of valve or operator, or
3. failure of trip set controller (FC 1211, 1221).

The operator should periodically observe the SG level following turbine trip. As the residual heat generated in the core decreases, the SG level will slowly increase. As the SG level rises, the operator should manually override the trip set controller and throttle the bypass valve to prevent SG overfill.

The specific effects of a SG overfill include damage to main steam safety and turbine bypass valves and increased stresses on the main steam lines and their supports. Although the effects of increased stresses, intensified by the opening and closing of turbine bypass or safety valves, have not been analyzed in detail, the conditional probability of consequential steam line failure would be increased. Moisture carryover to the turbine can adversely affect turbine life due to turbine blade erosion, but in most cases the turbine stop valves will protect the turbine from moisture carryover.

The operator is an important component in control of the condensate and FW system. Operator action or failure to take action can influence the severity and course of a transient. The following paragraphs summarize the actions the operator should take following important failures.

In the case of SG overfill, the operator should suspect a potential overfill when high SG level is annunciated. The operator should determine the cause of the rising level and take appropriate action including

1. manually closing the FW regulating valve,
2. tripping the SG FW pump, or
3. closing the MFW isolation valve.

If the level continues to rise, the operator should trip or verify the automatic trip of the main turbine. Each SG has a two-out-of-four logic device that automatically trips the turbine when the high level limit on two of four sensors is exceeded. This device transmits a signal to a single OR gate that actuates a single relay, which in turn trips the turbine. If either of these devices, the OR gate or the relay, is in the undetected failed state, the turbine trip signal will not be generated.

In the case of loss of MFW RCS undercooling, the operator should diagnose a failure in the condensate and MFW system upon low SG level annunciation. The operator should determine the cause of the falling level and take appropriate action including

1. manually opening the FW regulating valve;
2. restarting tripped pumps, if possible; or
3. verifying automatic actuation or manually actuating AFW.

If the operator's actions to restore MFW flow are unsuccessful, the operator should actuate or verify automatic actuation of the AFW flow.

Two power failures have been identified that result in failure to supply FW to the SGs, which in turn may contribute to RCS undercooling. The loss of electric power to the condensate or the condensate booster pumps will result in failure of the condensate flow and subsequent MFW pump trip on low suction pressure. The loss of electric power to the motor-driven AFW pump will degrade the flow of AFW to the SGs. In order to fail the MFW flow and degrade the AFW flow, the following power failures must occur:

1. failure of 13-kV Service Bus 11 coupled with loss of DG 4-kV power generation, or
2. failure of 4-kV Bus 11, resulting in isolation of 13-kV Service Bus 11 from the 500-kV bus.

The operator's remedial actions are to verify the operability of the steam-driven AFW pump and associated valves, restore the failed bus, or, if required, cross-connect AFW from Unit 2.

It should be noted that the steam-driven AFW pumps and control valves would not be affected by these failures. The AFW control valves are air operated (accumulator backed) and controlled by 125-V dc solenoid valves. These valves fail open on loss of air, permitting flow of AFW to the SGs.

Other failures affecting RCS undercooling in the condensate and MFW system have been identified. Although these failures affect water flow, AFW flow remains available. A failure that curtails the supply of MFW to the SG, will cause the level in the SG to drop until the AFW pumps can begin the refill. The reactor is also tripped upon low SG level. Emergency Operating Procedure EOP-3, Loss of Main Feedwater,[11] was reviewed and found to be consistent with the information described here regarding failure modes and operator remedial action. Detailed FMEA results for the condensate and FW system are included in Appendix C.

4.2.2.7 FMEA of the Feedwater Regulating System

4.2.2.7.1 Significant results. The principal failures in the FW regulating system involve the potential for overfeeding the SGs. Four specific failures leading to SG overfill are identified in Table 4.8, which is a summary of the FMEA for the FW regulating system. It should be noted that some components in the FW regulating system such as the square root extractors, lead-lag units, and comparators are not expected to fail at frequencies as high as those of other components in the system. A simplified description of the FW regulating system can be found in Appendix B.

The failure of the FW regulating controller was addressed generally in the MFW and condensate FMEA (Sect. 4.2.2.6). Specific failures of the FW regulating system are addressed in detail in this section.

Steam generator overfeeding may occur if the FW regulating system should fail the MFW regulating valve in the open position. Again, failing the control valve open would be expected to have a greater impact on RCS overcooling at lower reactor power levels, while the failure to close would be more severe at higher reactor power levels. Below 15% power, the smaller diameter bypass valves are controlling FW flow, so the impact of regulating system failure in the open position is not as immediate because the operator has more time to respond. Also, SG "shrink" and "swell" effects are less likely below 15% power, permitting clearer diagnosis of the problem by the operator. If the operator fails to reduce the FW flow, the turbine will trip on high SG level.

During power operation, failure of one of the two MFW control valves in the open position by the regulating system could occur due to

1. steam flow transmitter failing high,
2. FW flow transmitter failing low,
3. downcomer level transmitter failing low, and
4. FW controller opening the regulating valve.

If one of the FW regulating systems fails the MFW regulating valve open, the operator can take manual control of the valve. If the operator cannot adequately control the flow of FW to the SG, the turbine should be tripped to preclude turbine blade damage. In addition to protecting the turbine, turbine trip also blocks signals from a majority of the FW regulating system circuits including steam and FW flow and SG

Table 4.8. Feedwater regulating system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
1. Feedwater Controller (FC1111, 1121 or (FC105, 1106) Failure Opens Valve	1. Loss of Control Power (Y01 and Y09, Y02 and Y10) Valve Open 2. Electronic Failure	Valve supplies excessive feedwater flow to steam generator possibly resulting in SG overfill. Potential for carryover to turbine causing turbine erosion exists prior to turbine trip.	Operator should attempt manual control or trip the main feedwater pumps to prevent SG overfill.

downcomer level input signals. Due to the automatic turbine trip on high SG level and the subsequent automatic closure of the MFW regulating valves, failures in the steam and FW flow and downcomer level circuits are not of significant concern.

Failures in the FW controller or associated manual control station can open the MFW regulating valve or prevent its closure. These failures are not necessarily blocked by turbine trip and are therefore of greater significance. As indicated in Table 4.8, manual control of the valve is possible for some failures. However, if SG level cannot be controlled in this way, the operator must trip the MFW pumps or close the FW isolation valve to prevent SG overfill.

Although SG level transmitter LT1111 (1121) is routinely used by the regulating system during three-element control (above 15% power), an alternate level transmitter, LT1105 (1106), normally used for single element control, may be used in the event of a failure of the primary transmitter. This provides some redundancy for the FW regulating system.

Failure of one of the two bypass control valves in the open position by the regulating system could occur if (1) the downcomer level transmitter fails low, or (2) the FW bypass valve controller fails the valve open.

If one of the regulating systems fails the bypass valve open, the operator should manually control the valve if possible. If adequate control of the FW flow cannot be maintained, the operator should trip the turbine and the SG feed pumps to prevent SG overfill. Failure of the bypass valve open by the regulating system, while the main valve is open, may not result in SG overfill and RCS overcooling if the MFW valve can modulate closed and limit the flow rate to the SG.

Although level transmitter LT1105 (1106) is normally used by the regulating system during single element control (below 15% power), an alternate transmitter, LT1111 (1121) may be used in the event of a failure of the primary transmitter. Again, this provides some redundancy for the FW regulating system.

The principal effect of failures in the FW regulating system on RCS undercooling is the potential for failing to feed the SGs. Following a failure that reduces the supply of MFW to the SG, the level in the SG will drop until the AFW pumps can begin a refill. The reactor is also tripped on low SG level indication. Specific FW regulating system failures can result in terminating the supply of FW to the SG. However, these failures do not affect AFW flow and, therefore, are of smaller significance. Detailed results of the component level FMEA of the FW regulating system are included in Appendix C.

4.2.2.8 FMEA of the Main Steam System and Atmospheric Steam Dump Turbine Bypass Control System. A FMEA of the main steam system was performed to identify the impact of component failures on RCS undercooling and overcooling, SG overfill, and operation of standby

safety systems. The FMEA identified component failures that would impact standby safety systems and RCS overcooling. A third category of component failures involving significant equipment damage was also identified by the FMEA. Specific failures leading to RCS overcooling are identified in Table 4.9, which is a summary of the main steam system FMEA. (The detailed FMEA can be found in Appendix C.) The major RCS overcooling failures identified by the FMEA are discussed in this section, and a simplified description of the main steam system can be found in Appendix B.

The atmospheric steam dump and turbine bypass control system interfaces with the main steam system to provide the signal to open the turbine bypass and atmospheric steam dump valves. These systems are closely related, and their failure modes have been analyzed together.

4.2.2.8.1 Significant results. The significant failures identified are those which result in RCS overcooling due to failure to close turbine bypass valves. The four turbine bypass and two atmospheric steam dump valves are normally closed, but are opened to relieve excess main steam line pressure and provide capability for RCS cooldown. The turbine bypass valves have a total capacity of 40% of main steam flow (10% each), and the atmospheric dump valves have 5% (2.5% each).

Failure to close these valves once they are opened following turbine trip can result in excessive depressurization of the main steam system. Depressurization of the main steam system due to failure of the turbine bypass valves to close results in an initially uncontrolled blowdown of the SG inventory (assuming the turbine has tripped). The effect of the blowdown on the RCS is a rapid drop in RCS pressure and temperature. The drop in RCS temperature results in a positive reactivity insertion in the reactor core, which is controlled by reactor trip. Unless manually terminated, the depressurization of the SGs will result in automatic closure of the main steam isolation valves (MSIV) which isolates the turbine bypass valves.

Similar effects result if the turbine bypass valves inadvertently open during power operation. The increased steam flow is expected to result in a reactor and turbine trip. Once the turbine trips, a depressurization of the main steam system similar to that described previously would occur.

The turbine bypass valves can fail open or fail to close as a result of the following:

1. mechanical failure of valve;
2. solenoid valve fails to close, preventing isolation of high-pressure instrument air;
3. control circuit failures; or
4. T_{avg} error following turbine trip or pressure signal failure.

Table 4.9. Main steam, atmospheric dump, and turbine by-pass systems FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
1. Turbine Bypass Valves (MS-3940, 3942, 3944, 3946) Fail to Close	1. Mechanical failure 2. Solenoid valves (MS-3941, 3943, 3945, 3947) fail to close preventing isolation of instrument air 3. Tav error or pressure signal failure 4. I/P converter failure 5. Control circuit failure	Substantial depressurization of steam generator could result in initial RCS overcooling. Each turbine bypass valve is able to pass 10% of full power steam flow. If depressurization continues, MSIV's will automatically close isolating the bypass valves.	Manually close valve, if possible. Close isolation valves or manually initiate MSIV closure.
2. Turbine Bypass Valves (MS-3940, 3942, 3944, 3946) Open Inadvertently	1. Mechanical failure 2. Spurious Tav error or pressure signal 3. I/P converter failure 4. Control circuit failure	Substantial depressurization of steam generator could result in initial RCS overcooling. Each turbine bypass valve is able to pass 10% of full power steam flow. If depressurization continues, MSIV's will automatically close isolating the bypass valves.	Manually close valve, if possible. Take necessary procedures to control and reduce depressurization including manually closing isolation valves.
3. Turbine Bypass Valves (MS-3940, 3942, 3944, 3946) Fail to Open	1. Mechanical failure 2. Fails to receive signal from SG outlet pressure and reactor regulating system 3. I/P converter failure 4. Loss of dc bus 11 5. Pressure transmitter fails	Significant failure if it becomes necessary for Turbine Bypass Valves to open in response to a small LOCA. RCS could not be depressurized.	Manually open valve, if possible.

Table 4.9 (continued)

Failure	Possible Causes	Effects	Remedial Actions
	6. Signal auctioneering circuit (PY-4056) fails		
4. Atmospheric Steam Dump Valves (MS 3938, 3939) Fails to Open	1. Mechanical failure 2. Fails to receive signal from reactor regulating system 3. I/P converter failure 4. Loss of dc bus 11	Significant failure if it becomes necessary for the Steam Dump Valves to open in response to a small LOCA. RCS could not be depressurized.	Manually open valve, if possible.
5. Combination of Turbine Bypass and Atmospheric Steam Dump Valves Fail to Open	1. Mechanical failure 2. Fails to receive signal from SG outlet pressure and reactor regulating system 3. I/P converter failure 4. Loss of dc bus 11 5. Pressure transmitter fails 6. Signal auctioneering circuit (PY-4056) fails	Significant failure if it becomes necessary for these valves to open in response to a small LOCA. RCS could not be depressurized.	Manually open valve, if possible.

The atmospheric steam dump valves are subject to much the same types of failures as the turbine bypass valves. The primary difference between the two types of valves, in addition to capacity, is the absence of an actuation signal to the dump valves from the steam generation pressure transmitter. Failure of the atmospheric steam dump valves to close was not considered significant to this analysis because of the limited steam flow capacity of each valve. Each valve is capable of passing only 2.5% of the total steam flow. If the failure occurred during operation, a reactor and turbine trip could be prevented by throttling the turbine. If the turbine did trip, this failure would result in a very slow depressurization of the SGs. However, the atmospheric dump valves are not isolated by MSIV closure.

A potential RCS overcooling failure not considered in the FMEA is steam line rupture. This failure mode was not included because it represents a passive failure of equipment. The failure rate for steam line rupture is lower than other failures, hence its elimination from the FMEA. However, Emergency Operating Procedure EOP-4, Steam Line Rupture,[12] was reviewed to determine remedial action that might be taken if steam relief valves fail open. Both failures have a similar impact on the main steam system (i.e., depressurization).

The RCS undercooling failure identified as significant in the main steam system FMEA involves failure of the atmospheric dump and/or turbine bypass valves to open on demand. Following reactor and turbine trip, a hot shutdown can be maintained by the main steam safety valves even if the steam relief valves fail to open. However, following a small break LOCA, RCS cooldown is required by procedure. Thus, failure of the valve to depressurize the SGs could degrade recovery from the small LOCA.

Continual use of the larger capacity turbine bypass valves would require special operator actions under these conditions. As the SGs depressurized, the MSIVs would close automatically unless the operator manually blocked the steam line isolation signals from the ESFAS.

4.2.2.9 FMEA of the Component Cooling System. A FMEA of the component cooling system was performed to identify the impact of component failures on RCS undercooling and overcooling, SG overfill, and operation of standby safety systems. Failures that would affect RCS undercooling and safety system operation are identified in Table 4.10, which is a summary of the FMEA. The detailed FMEA of the system can be found in Appendix C. Each major failure of this system affecting safety system performance and RCS undercooling is discussed in the following section. A simplified description of the component cooling system can be found in Appendix B.

4.2.2.9.1 Significant results. The FMEA determined that failures in the component cooling system result in loss of CCW to the RC pump seals and potentially lead to seal failure. The RC pumps require seal water and motor bearing lube oil cooling. The operator is instructed to turn off the pumps if one of the following conditions exists:

Table 4.10. Component cooling system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
RCS Undercooling			
1. Loss of Component Cooling Water to Reactor Coolant Pump Seals		Upon detection of high RC pump seal controlled bleed-off temperatures, which would occur after a loss of component cooling water to the pump seals, the operator is instructed to trip the pumps. Failure to trip the pumps under these conditions is assumed to result in failure of the pump seals. Rupture of the pump seals constitutes a small loss of coolant accident (LOCA). Safety systems including HPSI and LPSI will be challenged. RCS undercooling may result due to the LOCA.	Re-open component cooling system valves to restore flow if possible. If component cooling water flow cannot be restored, trip RC pump prior to exceeding temperature limits of pump seals. If the seals fail, follow procedure for a small LOCA.
a. All four pumps	1. CC-283 closes 2. CC-284 closes 3. CV-3832 closes 4. CV-3833 closes 5. Loss of control power to SV-3832 or 3833 6. Loss of pneumatic supply to SV-3832 or 3833 7. SV-3832 closes 8. SV-3833 closes		
b. On one Pump:	Operator fails to trip pump after one of the following:		
Pump 11A	CC-170 or 171 closes		
Pump 11B	CC-173 or 174 closes		
Pump 12A	CC-176 or 177 closes		
Pump 12B	CC-179 or 180 closes		

Table 4.10 (continued)

Failure	Possible Causes	Effects	Remedial Actions
Safety System Impact			
2. Loss of Component Cooling Water to HPSI and LPSI Pumps		Pumps are designed to operate for two hours without component cooling water. Loss of component water for periods greater than two hours is assumed to fail HPSI and LPSI. HPSI and LPSI are safety systems designed to provide core heat removal during emergency operation.	Re-open valves if possible. If safety injection is required and cooling water flow cannot be restored, attempt to rotate the pumps in operation.
a. All HPSI and LPSI pumps affected	Mechanical failure CC-258 closes		
b. HPSI 11 and 12 and LPSI 11 affected	Mechanical failure CC-270 closes		
c. HPSI 13 and LPSI 12 affected	Mechanical failure CC-242 closes		

1. CCW is lost for more than 10 min,
2. seal cavity temperature reaches 200°F, or
3. thrust bearing temperature reaches 195°F.

From a plant safety standpoint, the failure of interest involves the loss of seal water cooling. If the pump continues to run without seal water cooling for a period exceeding 10 min, the pump seals may fail and result in a small LOCA. Plant safety systems (including HPSI and LPSI) will be challenged to provide adequate core cooling during this transient.

The cooling water flow to the pump seals can be lost due to the following general groups of failures:

1. any pump seal water supply or return valves close, or
2. multiple pump and/or valve failures.

The pump/header failure group includes failure of pumps, main header supply, and return valves. The design of the component cooling system makes this unlikely; the two cross-connected trains of CCW (normal and standby) served by three pumps and two-heat exchangers should provide redundancy.

Pump seal water supply or return valve closure represents a more significant failure mode in the component cooling system. Failure of one of these valves may result in the loss of cooling water to one or all four RC pumps.

Each RC pump has one normally open gate valve for supply, and one normally open globe valve for return, of CCW. Failure of the supply or return valves (CC 170, 171, 173, 174, 176, 177, 179, 180) resulting in closure will fail the cooling water flow to that pump.

In addition to each pump's supply and return valves, the containment isolation valves (CV 3832, 3833) control the supply and return of cooling water for the header, which serves all four pumps, the support coolers, and the control element drive mechanism (CEDM) coolers. These valves isolate containment upon receipt of a containment isolation signal. They are air operated, with a solenoid valve controlling the air supply to the valve operator. Loss of electric power or pneumatic supply to the solenoid valve will result in control valve closure. Failure of the solenoid valve will also close the control valve. If either supply or return valve closes, the CCW flow to all four RC pumps will be isolated. If the operator fails to trip the RC pumps upon loss of CCW flow, a pump seal failure LOCA will result.

Two normally open gate valves (CC 283, 284) are provided to permit isolation of this supply header from the rest of the system. These valves are assumed to be manual valves that are closed only during maintenance. Although closure of these valves would isolate the supply of cooling water to the pumps, the failure mode is very unlikely because these valves would be closed only during cold shutdown. If one or more

were not reopened, the loss of cooling water (or possible failure of the affected RC pump seals) would be detected prior to resuming power operation.

It should be noted that CCW failure to the CEDM coolers is not considered a significant failure. Air cooling to the CEDM coils is sufficient to permit continued coil operation; the cooling water is provided to extend coil life. Loss of all cooling to the coils would eventually result in coil failure, causing the control rods to drop into the core.

Loss of CCW can also adversely affect the operation of standby safety systems including HPSI and LPSI. The CCW system provides cooling to the high-pressure (3) and low-pressure (2) SI pumps. These pumps are designed to operate 2 h without CCW, which considerably reduces the impact of short-term failures.

Although the SI pumps are not operating, CCW is supplied to them during normal operation to provide immediate cooling to the pumps should sudden SI be required.

Cooling water flow to the pumps can be lost due to the following general groups of failures:

1. pump supply or return valves close, or
2. multiple pump and/or distribution valve failures.

The pump and distribution valve failure group is similar to that described for the RC pumps. Again, the redundant design of the component cooling system makes such failures unlikely.

Pump supply or return valves may close, resulting in loss of cooling water. The most significant failure in this group is closure of return valve CC 258. This failure would result in loss of cooling to all HPSI and LPSI pumps. The second most important failure in this group is closure of supply valve CC 270. This failure results in loss of cooling water to two HPSI pumps (11 and 12) and one LPSI pump (11). The last important failure in this group is closure of supply valve CC 242, which results in loss of cooling water to one HPSI pump (13) and one LPSI pump (12). Failure of each pump's supply and return valves is not considered significant because other pumps are available to provide HPSI and LPSI.

The failure rate of the supply and return valves discussed previously is not considered significant because they are normally open manually controlled valves. The most likely failure mode for these valves is a postulated maintenance failure (closure of the valve for maintenance and failure to reopen).

4.2.2.10 FMEA of the Service Water System. A FMEA of the service water system (SRW) was performed to evaluate the impact of component failures on RCS undercooling and overcooling, SG overfill, and operation of standby safety systems. Failures that might cause RCS undercooling and

therefore affect safety system performance are identified in Table 4.11, which is a summary of the FMEA. The detailed FMEA of the system can be found in Appendix C. Each major failure of this system affecting safety system performance and RCS undercooling is discussed in the following section. A simplified description of the SRW can be found in Appendix B.

4.2.2.10.1 Significant results. The FMEA determined that RCS undercooling and degraded safety system operation may occur if failures in the service water system result in loss of cooling water to the emergency power DGs. The DGs provide a backup electric power supply to important safety systems necessary for the mitigation of transients, including

1. the HPSI system,
2. the motor-driven AFW pump, and
3. the CCW system.

The DGs require lube oil, diesel jacket water, and diesel air cooling. Service water is supplied to the tube sides of three heat exchangers for each DG. Service water is also provided to the aftercooler of the diesel starting air compressor.

Failures resulting in complete loss of service water to all three DGs are not considered likely due to the redundancy of the SRW design. The three diesels are served by four separate service water headers (two headers for each unit): Diesel 11 may be provided with service water from Unit 1 header 11 or Unit 2 header 21, Diesel 12 may be provided with service water from all four headers, and Diesel 13 may be provided with service water from Unit 1 header 12 and Unit 2 header 22. One diesel operating at its design rating is capable of bringing one unit to safe shutdown conditions. Hence the complete failure of emergency diesel power due to loss of service water is remote.

Another significant failure of the SRW system involves the loss of service water cooling to the containment air coolers. This system is one of the engineered safety features providing containment air cooling during normal and emergency conditions. The loss of service water to more than one containment cooler would degrade post-accident heat removal from the containment building.

Substantial redundancy has been designed into the SRW system interface with the containment cooling system to reduce the likelihood of complete system failure. Only three of four containment air coolers are necessary for heat removal following a LOCA. The service water outlet from each cooler is equipped with three parallel lines, each with a valve: one line satisfies normal operation cooling requirements, the second is opened upon containment isolation, and the third has a manual valve should the second valve fail to open. Manual valves in the supply piping permit service water flow to any cooler from either subsystem header.

Table 4.11. Service water system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
Service Water Header Failures			
1. Service Water Pumps 11, 12, 13 Trip	1. Mechanical Failure 2. Loss of Electric Power from 4 kV Bus 11 for Pump 11, 4 kV Bus 14 for Pump 12, and both 4 kV Buses 11 and 14 for Pump 13 3. Supply or Return Valves Fail Closed	Significant failure because it degrades heat removal from important plant components including the diesel generators and the containment air coolers. Two pumps are required to operate so one pump is placed in standby. The redundancy incorporated into the design permits operation of pump 13 from either bus. It is likely that two pumps would fail simultaneously.	Verify automatic start of standby pump. If pump 13 does not start, align contacts to other bus.
2. Service Water Heat Exchanger 11, 12 Fails	1. Mechanical Failure 2. Salt Water System Header Failure 3. Inlet or Outlet Valves Fail Closed	Significant failure because it degrades heat removal from important plant components. Plant may be temporarily operated with just one heat exchanger during normal operation. During an emergency some loads would be isolated, permitting temporary operation with only one heat exchanger.	Re-open valves or repair heat exchanger if possible.

Table 4.11 (continued)

Failure	Possible Causes	Effects	Remedial Actions
Loss of Cooling Water to System Loads			
3. Loss of Service Water to Emergency Diesel Generator:		Loss of service water to an operating emergency diesel generator will result in diesel generator failure. The two Calvert Cliffs units share 3 diesels. Supply header 11 can supply service water to either diesel 11 or 12. Supply header 12 can supply diesel 12 or 21. Supply header 21 can supply diesel 11 and 12. Supply header 22 can supply diesel 21 and 12. This redundancy reduces the probability of loss of diesel power due to service water failures.	If one supply header to a particular diesel is unavailable, operator should open valves to supply diesel with an alternate source of cooling water.
No. 11 Diesel	1. 1-CV-1587 Fails to Open a. Mechanical Failure b. Diesel Start Signal Not Received Due to Circuitry Failure c. Controller PDIC-1587 Closes Valve		
	2. One of Two Manual Valves Fail Closed		
	3. Service Water Header Failures		
No. 21 Diesel	1. 2-CV-1587 Fails to Open a. Mechanical Failure b. Diesel Start Signal Not Received Due to Circuitry Failure c. Controller PDIC-1587 Closes Valve		
	2. One of Two Manual Valves Fail Closed		

Table 4.11 (continued)

Failure	Possible Causes	Effects	Remedial Actions
	3. Service Water Header Failures		
No. 12 Diesel	1. 1 and 2-CV-1645 Fail to Open a. Mechanical Failure b. Pressure Sensors 1/2 PS-1645 Fail		
	2. 1 and 2-CV-1645 Fail to Open a. Mechanical Failure b. Pressure Sensors Prevent Valve from Opening		
	3. 1-CV-1588 Fails to Open a. Mechanical Failure b. Diesel Start Signal Not Received Due to Circuitry Failure c. Controller PDIC-1588 Closes Valve		
	4. Both Manual Supply or Both Return Valves Fail Closed Simultaneously		
	5. Service Water Header Failures		

Table 4.11 (continued)

Failure	Possible Causes	Effects	Remedial Actions
4. Loss of Service Water to Compressed Air System Components:		Loss of service water cooling to the compressors or aftercoolers will result in eventual compressor or aftercooler failure. This is a significant failure because pneumatic components must be continuously supplied with instrument air to maintain safe and reliable operation of the plant. Some redundancy is provided in the compressed air system in the event of component failures. Two instrument air compressors are available, although one is usually all that is required. The Unit 1 plant air compressor is backed up by the Unit 2 plant air compressor. Plant air is also important because it provides breathing air for respirator operation inside containment. Plant air is backed-up by breathing air tanks inside containment.	Reopen service water supply or return valves if possible.
All Instrument Air and Compressed Air Compressors	1. SRW-181 Fails Closed 2. SRW-183 Fails Closed 3. PCV-1628 Fails Closed 4. CV-1637 Fails Closed 5. CV-1639 Fails Closed 6. Service Water Pump 11 Trips 7. Loss of 125 VDC Bus 11 Closes CV-1637 8. Loss of 125 VDC Bus 21 Closes CV-1639		
Plant Compressor 11	1. SRW-197 Fails Closed 2. SV-1636 Fails Closed 3. TCV-1636 Fails Closed		Verify that backup compressors are started when line pressure drops below low limit.

Table 4.11 (continued)

Failure	Possible Causes	Effects	Remedial Actions
Plant Compressor 11 Aftercooler	1. SRW-199 Fails Closed		
	2. SV-1635 Fails Closed		
	3. SRW-200 Fails Closed		
Instrument Air Compressor 11	1. SRW-189 Fails Closed		
	2. TCV-1630 Fails Closed		
	3. SV-1630 Fails Closed		
Instrument Air Compressor 11 Aftercooler	1. SRW-191 Fails Closed		
	2. SV-1629 Fails Closed		
	3. SRW-192 Fails Closed		
Instrument Air Compressor 12	1. SRW-193 Fails Closed		
	2. SV-1634 Fails Closed		
	3. TCV-1634 Fails Closed		
Instrument Air Compressor 12 Aftercooler	1. SRW-195 Fails Closed		
	2. SV-1633 Fails Closed		
	3. SRW-196 Fails Closed		

Table 4.11 (continued)

Failure	Possible Causes	Effects	Remedial Actions
5. Loss of Service Water to Containment Coolers:	Service Water Header Failures	Significant failure if more than one cooler were to fail at one time. However, this represents an unlikely event. These coolers provide post-accident heat removal from the containment. Significant redundancy is available in this system because either header can be used to supply any cooler. Only 3 coolers are necessary for heat removal following a LOCA.	Re-open valves if possible or open other header supply valve to the affected cooler.
11, 12	1. CV-1581, 1583 Fails Closed		
	2. CV-1584, 1586 Fails Closed		
	3. Supply Header 11 Failure		
	4. Manual Valves Fail Closed		
13, 14	1. CV-1589, 1592 Fails Closed		
	2. CV-1591, 1594 Fails Closed		
	3. Supply Header 12 Failure		
	4. Manual Valves Fail Closed		

Loss of service water cooling to the instrument air compressors and aftercoolers was determined to be a significant failure of the SRW system. Loss of instrument air results in isolation of CCW flow to the RC pump seals. Failure to trip the pumps on loss of seal water cooling will result in seal failure and a small LOCA. Loss of instrument air will also prevent the FW regulating valves from closing which could initiate a SG overfeed transient following reactor trip.

Three service water system component failures can result in the loss of cooling water to all air compressors. These failures include the following:

1. service water pump 11 trips,
2. control valve CV-1637 fails closed, and
3. control valve CV-1639 fails closed.

For the purpose of this analysis, loss of service water cooling is assumed to eventually fail the instrument air compressors. Under actual operating conditions, some time would elapse between loss of service water and failure of the air compressors. The operator may be able to extend this period by alternating between the two compressors. Additional discussion of instrument air system failure modes may be found in Sect. 4.6.

4.2.2.11 FMEA of the Salt Water Cooling System. A FMEA of the salt water system was performed to identify the potential effects of component failures on RCS undercooling and overcooling, SG overfill, and operation of standby safety systems. Specific failures identified in Table 4.12 were found to affect RCS overcooling and standby safety systems. This table summarizes the significant results from the detailed FMEA, which can be found in Appendix C. A simplified description of the salt water system is included in Appendix B.

4.2.2.11.1 Significant results. The results identified for the salt water system are second-order effects compared to the near-term results from the failure of other systems. Failures in the salt water system eventually will degrade the heat removal capability of the service water and CCW systems, which in turn may impact RCS undercooling and standby safety systems.

The loss of one of the salt water cooling trains to a CCW heat exchanger will cause the CCW to rise in temperature, and the loads supplied by the CCW may be affected as the temperature rises. The RC pump seals are the components of interest from a RCS undercooling standpoint. Loss of CCW to the RC pump seals will result in seal failure and a small LOCA.

The loss of salt water cooling to one of the service water heat exchangers will also cause the affected service water train to heat up. The loads supplied by the service water system eventually may fail as the temperature rises. The loads of interest for the service water system are the DGs and the compressed air system compressors. Diesel generators are standby safety components and would fail shortly after losing service water cooling.

Table 4.12. Salt water system FMEA summary

Failure	Possible Causes	Effects	Remedial Actions
BCS Undercooling			
1. Loss of Salt Water Cooling to Component Cooling Water HX 11, 12	1. SW 5160, 5162 CV Closes 2. SW 5206, 5208, or 5163 Closes 3. Salt Water Pump Trip	Substantial impact on Component Cooling System due to loss of cooling to the component cooling heat exchanger. Time-to-failure for components serviced by the component cooling system is expected to be long (tens of of minutes or hours) but can not be determined using FMEA techniques.	If salt water cooling is lost to only one component cooling HX, the operator should verify that the operating component cooling HX has adequate cooling water. If cooling RCP pump seals is lost, trip pumps.
Safety System Impacts			
2. Loss of Salt Water Cooling to Service Water Heat Exchanger 11, 12	1. Valve Failure 2. Salt Water System Header Failure	Substantial impact on Service Water System due to the loss of cooling to the service water heat exchanger. Time-to-failure for components serviced by the Service Water System is expected to be long (tens of minutes or hours) but can not be determined using FMEA techniques.	If salt water cooling is lost to only one service water system heat exchanger, the operator should verify that the operating service water system has adequate cooling water.

4.3 ACCIDENT SEQUENCE DEVELOPMENT

The results of FMEAs of the Calvert Cliffs control systems have been presented in Sect. 4.2. These postulated failures, while they may initiate a transient or accident, are not necessarily of safety significance. The extent to which such failures are mitigated by safety system action affects their significance to plant safety. However, if control systems were required to mitigate the initiated transient without a backup safety system available, the identified control system actions would have safety significance and would represent a significant result of the SICS study.

The evaluation of control system failures in the context of developed accident sequences is discussed in Sect. 4.3. In this analysis, sequences of accident-initiating events and the operating or failed states of control and safety systems are developed. For purposes of the accident sequence analysis, the ultimate plant state for each sequence is postulated based on available information or engineering judgment. These plant states are corroborated, to the extent required, by thermal-hydraulic analyses (see Sect. 6).

Accident sequences resulting in an adverse plant safety state caused by failure of a control system are identified as significant results of the SICS Program. The sequence frequencies and the relative contributions of control system failures to these frequencies are estimated as discussed in Sect. 5.

The accident sequences identified as significant are summarized in Sect. 4.3.1, and the development and evaluation of accident sequences are discussed in Sect. 4.3.2.

4.3.1 Summary of Significant Accident Sequences

The potential effects of control system failures on plant safety have been evaluated by accident sequence analysis as summarized in Sect. 4.3 and discussed in detail in Sect. 4.3.2. The results of this analysis show that for most accident-initiating events, the action of safety systems will prevent adverse safety consequences to the plant regardless of the operating state of control systems. Only two accident-initiating events, a small-break LOCA and a SG overfeed, were found to require the successful operation of control systems to achieve plant recovery.

Although not corroborated by thermal-hydraulic analysis, operation of atmospheric steam dump valves, PORVs, and possibly turbine bypass valves are believed to be required to recover from a small-break LOCA. This is principally because of the relatively low shutoff head of the HPSI pumps (1275 psia). The relatively low RCS pressure at which the SI tanks and the LPSI system begin to operate (200 psi) also contributes to dependence on the control systems for depressurization.

Small-break LOCA sequences have been identified as significant for the following reasons:

1. small-break LOCAs can be initiated by control system failures as well as by passive failures such as SG tube rupture,
2. small-break LOCAs may require the operation of control systems for recovery,
3. required control system actions must be manually initiated and regulated by the operator, and
4. LOCA emergency procedures do not explicitly define the equipment that should be used for cool down and depressurization (i.e., the control system equipment).

Accident sequences resulting in injection of FW into the main steam lines (SG overfill) also were identified as significant. As with LOCA sequences, SG overfeed sequences are initiated by control system failures and, in some cases of importance, must be manually terminated by the operator to prevent injecting high-temperature water into the steam lines.

4.3.2 Development and Evaluation of Accident Sequences

Development of accident sequences consists of identifying accident-initiating events, identifying the system functions required to mitigate the initiating event, and developing a logical structure describing sequences of the initiating event and subsequent successful or failed operating states of the mitigating functions, and, for each sequence, the resulting plant state. Of particular significance to the SICS Program are the following plant states, which may result from an accident sequence with a failed control system or a safety system failure resulting from a control system failure.

1. Uncontrolled overfilling of a SG (SG overfill).
2. A significant and continuous decrease in RCS temperature, including PTS (RCS overcooling).
3. Inadequate core cooling, leading to potential core damage (RCS undercooling).

The identification of accident-initiating events is discussed in Sect. 4.3.2.1, and the development and evaluation of the accident sequences resulting from these initiating events are discussed individually in Sects. 4.3.2.2 through 4.3.2.8.

4.3.2.1 Accident Sequence Initiators. The initial step in the development of accident sequences is the identification of accident-initiating events. Two principal sources of such events have been used in the SICS Program: Chapter 14 of the Calvert Cliffs FSAR,[10] the accident analysis section of the Calvert Cliffs FSAR,[10] and the results of the FMEAs of the Calvert Cliffs control systems (Appendix C). The accident-initiating events described in the FSAR are listed in Table 4.13.

Control system failures identified in Sect. 4.2 as potential accident-initiating events were compared to the events listed in Table 4.13. In general, control system failures could be included as part of one of the

Table 4.13. Summary of FSAR Chapter 14 initiating events

Event	Description
1. CEA Withdrawal	Withdrawal from the reactor core of one (or more) control element assemblies.
2. Boron Dilution	Reduction of the concentration of boric acid in the reactor coolant.
3. Excess Load	Rapid increase in the load placed on the plant electric generator by the electric grid.
4. Loss of Load	Rapid decrease or loss of the load placed on the plant electric generator by the electric grid.
5. Loss of Feedwater	Failure of the main feedwater system to deliver a flowrate required to remove reactor core decay heat.
6. Loss of FW Heaters	Failure of the main feedwater heaters resulting in a significant decrease in temperature of the feedwater delivered to the system generators.
7. Loss of Coolant Accident (LOCA) (includes PORV opening, SG tube rupture, and CEA ejection accidents)	Continuous loss of reactor coolant from the RCS in excess of makeup capability.
8. Loss of Coolant Flow (includes RC pump coast down and seizure)	Failure of one or more of the RC pumps to maintain forced circulation of reactor coolant.
9. Loss of Non-Emergency AC Power	Deenergizing one or more 13 KVAC electric power buses.
10. CEA Drop	Insertion (or drop) of one or more CEA's.
11. Asymmetric SG Event (includes SG overfill, loss of main feedwater, or main steam isolation of one steam generator)	Accident affecting the flow of feedwater to or the flow of steam from one of the two steam generators.
12. Steam Line Break (SLB)	Uncontrolled release of steam from one or both steam generators.
13. Non-Reactor Incidents	Failures in plant systems not affecting RCS performance such as spent fuel or waste disposal system incidents.

FSAR initiating events. (As initiating events, the failures were included in the FSAR. However, the accident sequences discussed in the FSAR do not necessarily include those developed from the control system initiated or postulated initiating failures.)

One initiating event was added to Table 4.13 for completeness: a reactor trip of unspecified cause. Although a reactor trip is a safety action, various control system actions are required to achieve a safe, stable shutdown. The sequence has been identified to the extent that a reactor trip, in conjunction with an independent or coupled control system failure, could lead to an accident sequence of concern.

One group of events listed in Table 4.13, Non-reactor incidents, was not included in the sequence development. These events, which by definition do not affect RCS performance, are not considered initiators of RCS accident sequences.

4.3.2.2 Reactor Trip Sequences. A reactor trip at power has the initial effect of rapidly reducing the heat generation rate of the reactor core. Following trip, the core will be in a stable subcritical state, generating heat at core decay heat rates. However, several control systems are required to function following reactor trip in order to achieve a stable hot shutdown plant operating state. Should one or more of these control systems fail, an accident sequence could occur.

An unspecified reactor trip initiator is a composite event that includes release and insertion of the CEAs. The trip may occur due to an RCS perturbation or may be spurious. With respect to accident sequence development, whether the trip precedes a control system failure or occurs in response to a control system failure is not considered significant.

Following a reactor trip, control system operations are required to achieve a stable hot shutdown state. These systems include

1. turbine trip equipment,
2. RCS (pressurizer) pressure control equipment,
3. RCS (pressurizer) inventory control equipment,
4. SG pressure control equipment, and
5. condensate and MFW equipment.

A reactor trip combined with failure of one or more of the above control systems will produce a plant transient of potentially greater severity than the normal trip transient. Combinations of the possible successful and failed operating states of the five systems listed can be depicted in an event tree format. The event tree for the reactor trip initiating event is shown in Fig. 4.1. Beginning with the assumed reactor trip, the tree is developed by branching each system function in sequence to consider the possible proper operation or failed operation of the system (more than two operating states of a system may be depicted at a branch if required).

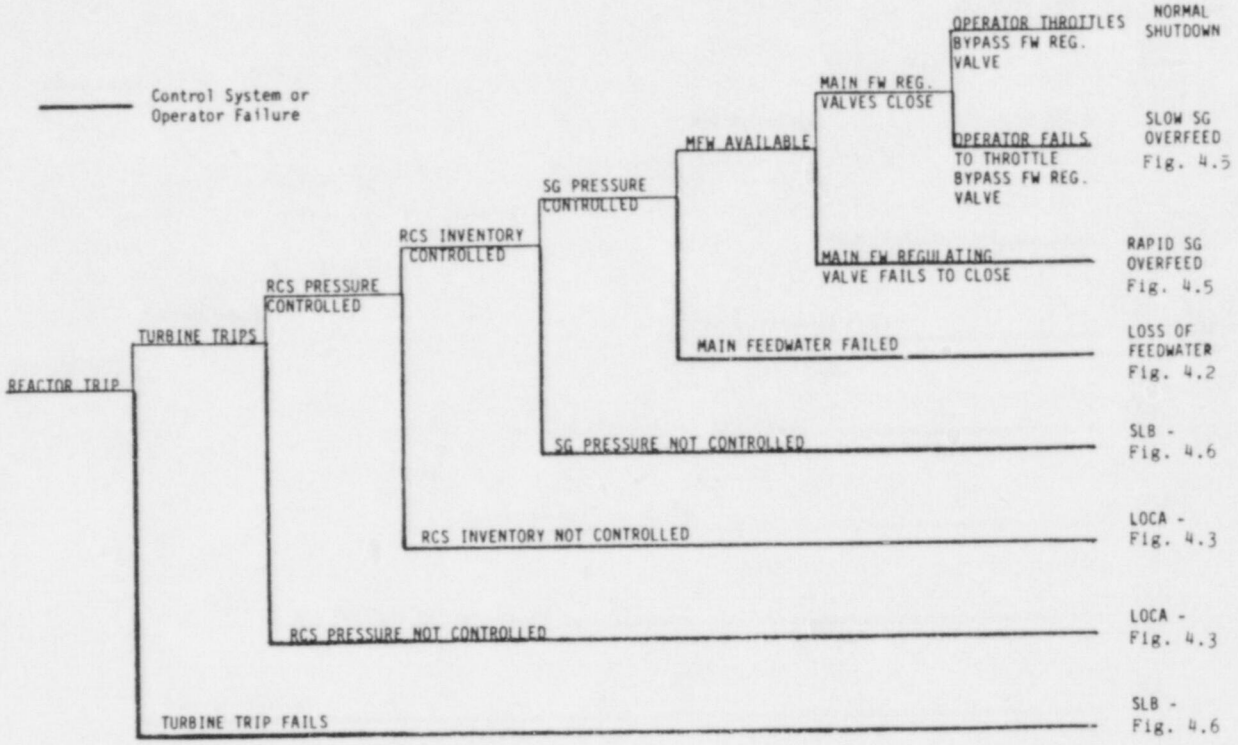

Fig. 4.1. Reactor trip event tree.

The first function considered in Fig. 4.1 is operation of the turbine trip function. The top branch depicts a successful turbine trip and termination of steam flow to the high-pressure turbine by closure of the turbine stop and/or throttle valve. Given reactor trip and turbine trip, operation of the next function is considered. The lower branch considers a reactor trip with turbine trip failure--a failure of the turbine stop and throttle valves to close, resulting in a continuous flow of steam from the SGs. This transient is a control system failure initiator equivalent to a steam line break (SLB), one of the identified initiating events listed in Table 4.13. This transient is further developed in the SLB event tree, Fig. 4.2.

Similarly, the operating states of other systems, given reactor trip and turbine trip failure, could be considered (resulting in 128 end states). However, these control system functions need not be considered because of the automatic operation of safety systems following a SLB (e.g., MFW isolation valve closure prevents SG overfeed regardless of the operation of the MFW regulating valves). To the extent required, control system failures combined with turbine trip failure are considered in the SLB event tree.

Given successful turbine trip, the next function considered is RCS pressure control. Two failure types can be postulated: failures resulting

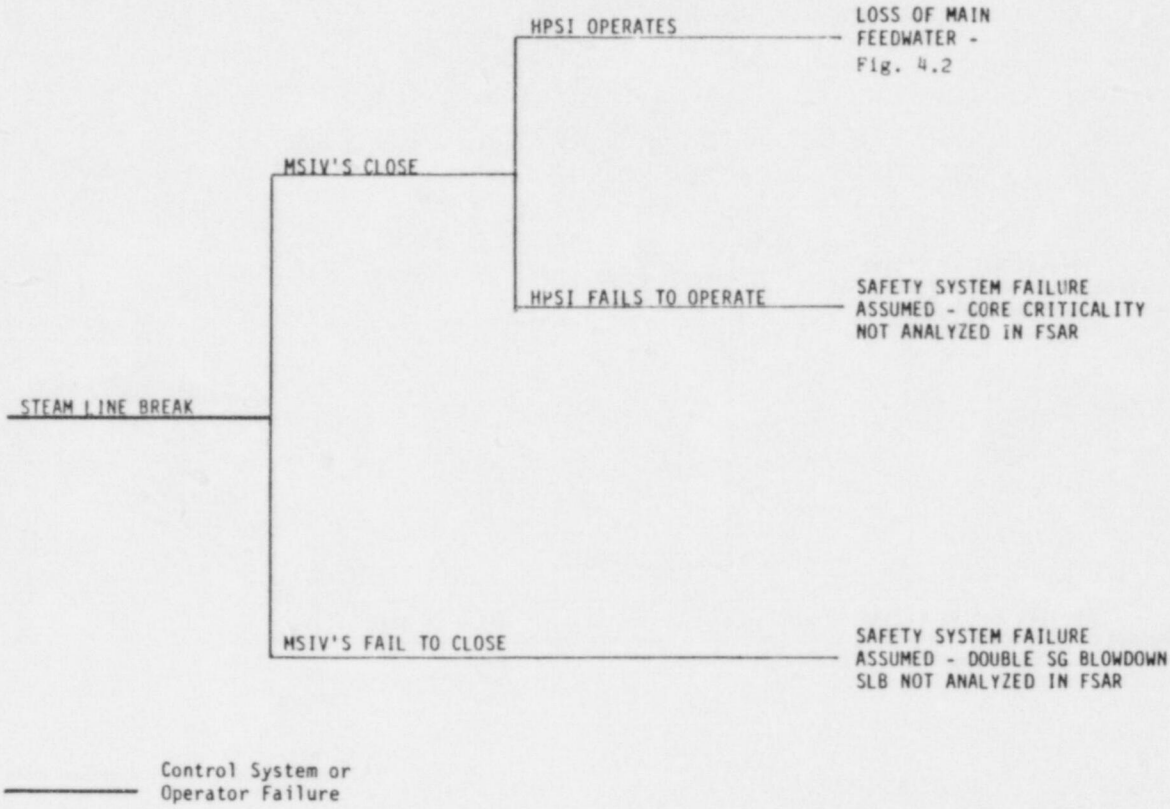

Fig. 4.2. Steam line break event tree.

in high RCS pressure or failures resulting in low RCS pressure. High-pressure failures are controlled automatically by the pressurizer safety valves. Should the safety valves or relief valves (PORVs) fail open as a result of the transient, a small LOCA would result. The small-break LOCA event tree is shown in Fig. 4.3.

Low pressure failures could result from failed open PORVs (or safety valves) or a failed open pressurizer spray valve. A failed open PORV is a LOCA. A failed open spray valve will result in RCS depressurization; however, no case was found in which this slow transient could have safety implications. The most likely scenario, beyond the operator manually terminating spray flow, would be a low RCS pressure SI signal and a procedurally required manual trip of two RC pumps, which may terminate spray flow.

RCS inventory control is accomplished by regulating the letdown flow rate and controlling the number of charging pumps in operation to maintain a constant pressurizer level. This equipment can fail, resulting in excessive or insufficient RCS inventory (increasing or decreasing pressurizer level). Excessive net charging flow can result in slowly filling the pressurizer and, assuming that volume control tank

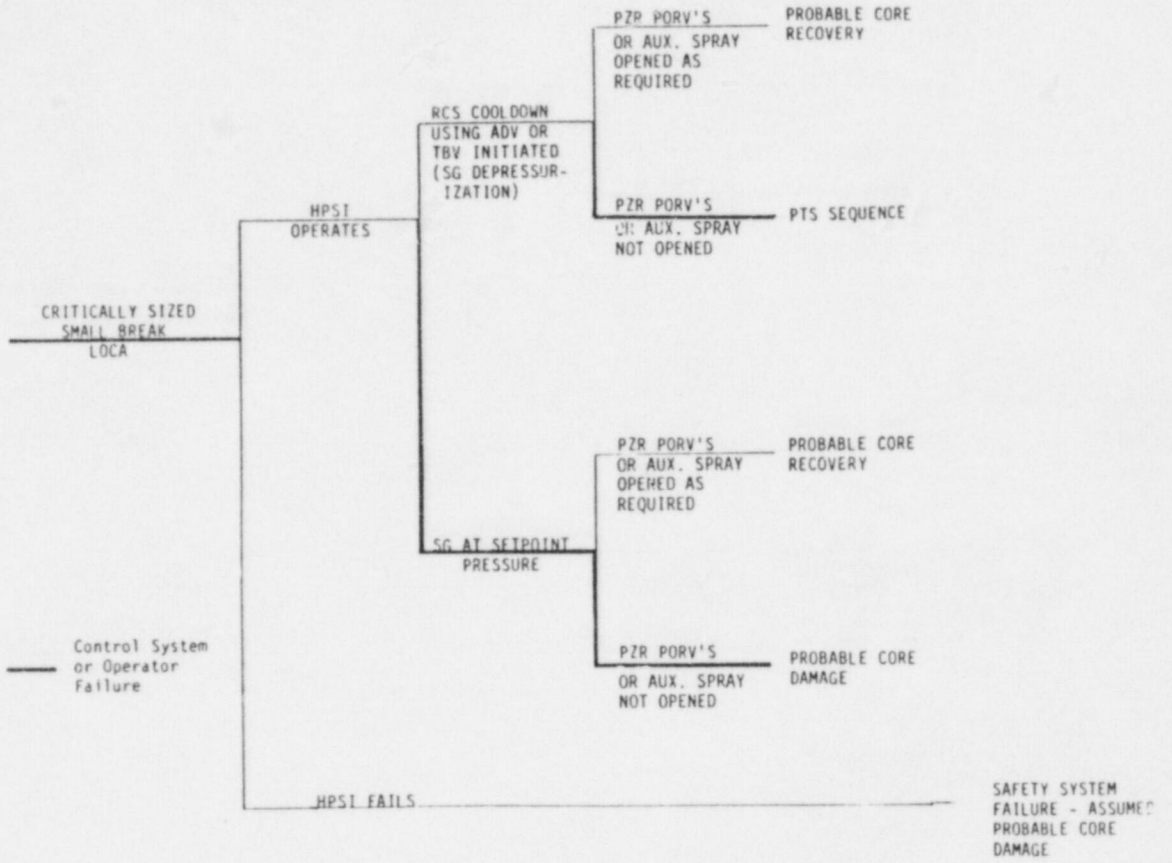

Fig. 4.3. Small-break LOCA event tree.

(VCT) inventory is maintained, possibly damaging the pressurizer relief or safety valves by liquid discharge. This could result in a small LOCA as indicated on the event tree. Insufficient net charging flow, due either to excessive letdown or inadequate charging flow or both, will result eventually in draining the pressurizer and losing the pressurizer heater control function. Unless manually isolated or controlled, continued loss of RCS inventory would result in a LPSI signal and probable isolation of letdown, which terminates the transient.

Following turbine trip, the atmospheric (steam) dump valves and turbine bypass valves open to limit and control SG pressure. If these valves failed to open, the pressure would be controlled by the main steam code safety valves. If one or more atmospheric dump or turbine bypass valves failed to close, a small SLB (equivalent) would be initiated. The SLB event tree is shown in Fig. 4.2.

The final control system function considered for the reactor trip initiating event is FW control. Following reactor trip, FW flow must be maintained at a low flow rate for continual removal of core decay heat.

Failures in the FW or condensate system can cause a loss of FW injection capability and initiate a loss of FW transient. The loss of MFW event tree is shown in Fig. 4.4.

Considering FW pumping capacity, the flow rate must be limited to prevent overfeeding the SGs. This is accomplished by automatically closing the MFW regulating valves and opening the bypass FW regulating valves to control the flow rate at ~5% of the full power FW flow rate. If either MFW regulating valve fails to close, a SG overfeed transient will occur. However, even if the system operates as designed, the operator is required to manually throttle the bypass regulating valve as the core decay heat generation rate decreases with time. If the operator fails to perform this function (or if the bypass regulating valve fails open), a slow SG overfeed transient results. As indicated, the SG overfeed transients are developed in the SG overfeed event tree, Fig. 4.5.

As shown in Fig. 4.1, the operation of control systems following a reactor trip will result in a normal safe shutdown if all systems operate properly. This sequence is shown in the event tree as the upper branch of each function. However, failures of the control system can result in SG overfeed, loss of FW, or SLB or LOCA transients as indicated in Fig. 4.1. It is noted that the initiation of a transient is not an RCS "end state." In each case these transients are mitigated by the subsequent operation of control and safety systems. The operating states of these mitigating systems are considered in the transient-specific event trees.

4.3.2.3 Transients Terminated by Reactor Trip. The transient-initiating events listed in Table 4.13 were found to fall into two categories: transients terminated by reactor trip and transients requiring operation of additional safety systems. Transients terminated by reactor trip may be described by a reactor trip event tree (Fig. 4.1). These transients are discussed below.

CEA malfunctions: CEA withdrawal and CEA drop transients will result in a perturbation of the core power level and core power distribution. To the extent that these transients result in RCS parameters exceeding set-point values, they will result in a reactor trip. Once the reactor is tripped and the control elements are released from their drive mechanisms, the transient will proceed as shown in Fig. 4.1.

Boric acid concentration control malfunctions: Failures of CVCS equipment or the manual control of this equipment during planned changes in RC boric acid concentration could result in excessive or inadequate concentrations. Excessive concentration of boric acid will decrease reactor power slowly and may cause a reactor trip, depending on manual control of the turbine generator and/or CEAs. Although the boric acid concentration will continue to increase until manually controlled, no adverse safety consequences result.

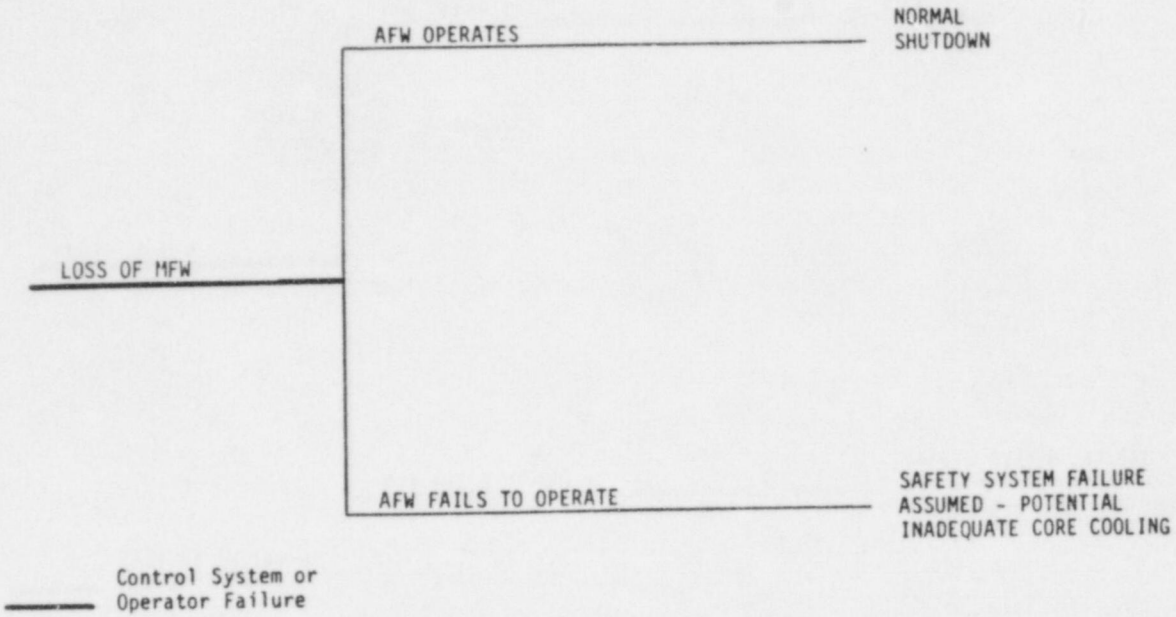

Fig. 4.4. Loss of MFW event tree.

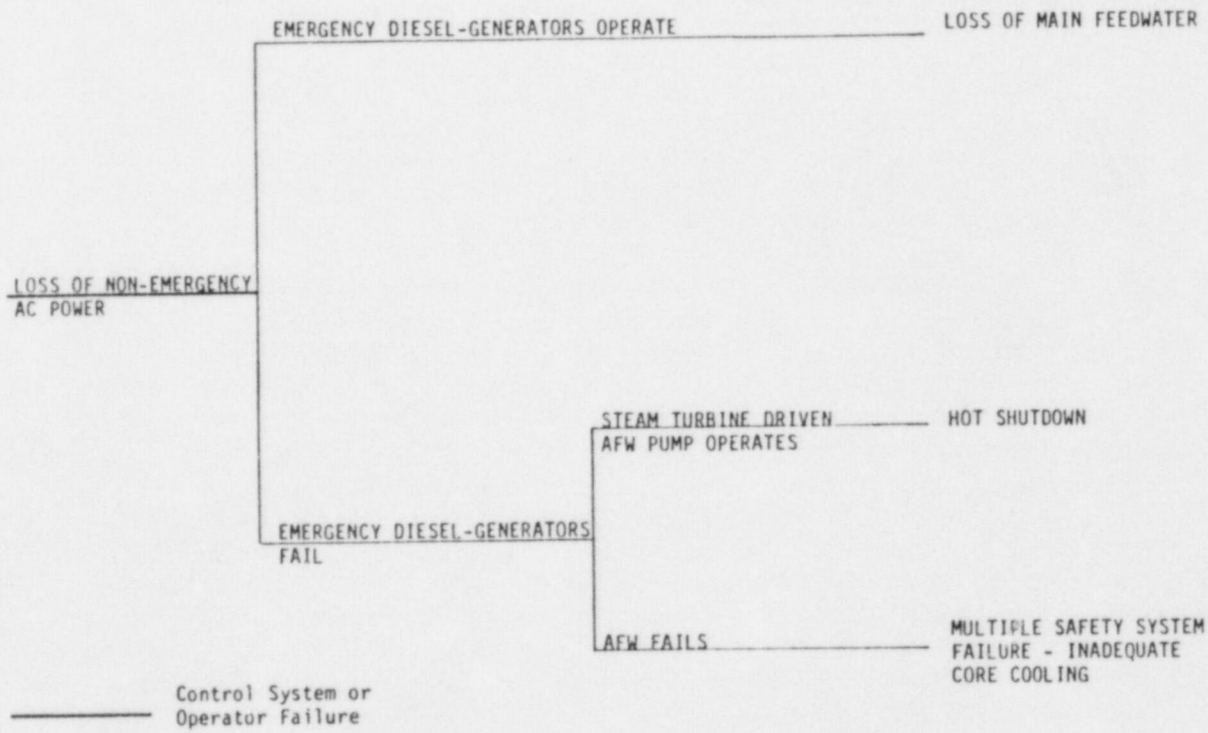

Fig. 4.5. Loss of non-emergency ac power event tree.

Inadequate boric acid concentration, a boron dilution transient, will result in increased core power and, unless manually controlled, will result in reactor trip. Once the reactor is tripped, the dilution will continue until manually controlled. If, as indicated in Fig. 4.1, an additional transient is initiated following reactor trip, the RCS response may be marginally more severe. However, for overcooling type transients, the resulting SI signals would terminate the boron dilution transient through initiation of borated SI and concentrated boric acid from the CVCS.

Electric generator load malfunctions: Rapid increases or decreases in the electrical load placed on the plant generator can result in an upset condition possibly resulting in turbine and reactor trip, which will result in terminating the transient.

Loss of FW heaters: Loss of the steam supply to the MFW or condensate heater will result in a decrease in FW temperature and an increase in heat removal from the RCS. The more severe transients of this type (loss of high-pressure heaters) would result in a reactor trip. Once the reactor is tripped, the transient is terminated.

Loss of RC flow: Failures resulting in the coastdown or seizure of the RC pumps at power will have a significant initial effect on core heat transfer. These transients result in a rapid reactor trip to limit temperature increase of the fuel and fuel cladding. Once the reactor is tripped, however, stable shutdown conditions can be achieved with the RCS in a natural circulation mode adequate to remove the decay heat generated in the core.

4.3.2.4 Loss of Main Feedwater. A loss or significant decrease in the MFW flow rate at power to one or both SGs will result in a reactor trip. To the extent the indicated level in either SG is reduced to its low level set-point value, the safety qualified AFW system will be initiated. These sequences of events are shown in the loss of MFW event tree, Fig. 4.4.

If the AFW operates as designed, a normal shutdown will occur. It is noted that the AFW flow rate is preset and requires manual throttling similar to the MFW bypass regulating valve.

Failure of the AFW is an assumed failure of a safety system and thus beyond the scope of this analysis. However, this sequence results in a complete loss of heat removal capability through the SGs. In this condition the core will be cooled by boiling, with RC discharged through the pressurizer PORVs and/or safety valves. However, at high RCS pressure, the RCS inventory of RC will continue to decrease unless the RCS can be depressurized to allow injection of coolant from the HPSI system. Failure to inject coolant at adequate rates or to restore SG cooling will result in core failure.

4.3.2.5 Loss of Coolant Accidents. Recovery from a breach of the RCS pressure boundary resulting in an uncontrolled loss of RC is

accomplished by injecting RC into the RCS at rates exceeding the loss of RC prior to the onset of core damage (inadequate core cooling). For break sizes equivalent in size to two open pressurizer PORVs or larger, RCS pressure decreases rapidly and an adequate rate of injection is achieved.[10] However, for break sizes large enough to represent a significant loss of coolant but not large enough to provide a rapid pressure drop ($0.0005\ ft^2$ <break size <$0.02\ ft^2$), the slower rate of decrease in RCS pressure can have an adverse affect on the injection capability of the HPSI system.[13] Under these conditions, proper operation of control systems apparently is required.

The event tree for a small-break LOCA is shown in Fig. 4.3. A LOCA may result from control system failure, as discussed, or result from a postulated breach of the pressure boundary. As indicated in Table 4.13, the general class of small-break LOCAs includes CEA ejection accidents and SG tube ruptures in addition to simple LOCAs.

Although it is recognized that the operation of the safety and control systems required for recovery depends on the break size, inadequate information is available to specify critical sizes without detailed thermal-hydraulic analyses. However, the range of sizes of interest is bound at the upper end at a break size of $0.02\ ft^2$ and at the lower end by a break size of $0.0005\ ft^2$.[13]

One post-LOCA recovery action, manual trip of the RC pumps, is not shown on the event tree. Trip of the RC pumps is not believed to be of concern for LOCA break sizes less than $0.1\ ft^2$.

As shown in the event tree, the HPSI is assumed to be critical to the recovery from a LOCA. Although the failure of this safety system is beyond the scope of the SICS program, a complete postulated failure of the HPSI is assumed to result in core failure. However, assuming the HPSI operates as designed, control system action is still required to maintain the RCS pressure below the shutoff head of the HPSI pumps and allow an adequate injection of fluid.

Two operator actions specified in the LOCA emergency procedures tend to facilitate RCS depressurization:

1. the operator is instructed to initiate an RCS cooldown, and
2. upon indication of relatively low RCS cold-leg temperatures and relatively high RCS pressures, the operator is cautioned to depressurize the RCS to avoid exceeding reactor vessel reference temperature for nil ductility transition (RTNDT)

RCS cooldown is initiated by manually opening the atmospheric dump and/or turbine bypass valves to reduce SG saturation pressure and temperature. The reduction in SG saturation temperature increases the RCS to SG heat transfer rate and, in conjunction with the postulated LOCA, promotes RCS depressurization. Failure of the operator to manually open the valves or failure of the valves to open will result in the SGs remaining at their hot shutdown pressure set point and corresponding saturation temperature.

The minimum pressure relief required to achieve an adequate cooldown rate can be provided by opening both of the atmospheric during dump values (~5% steam flow) or any one of the turbine bypass values (~10% steam flow). However, if the turbine bypass valves are used, the operator must bypass the SG isolation instrumentation to prevent closure of the main steam isolation valves (MSIVs) on low SG pressure. This action is not specified in the LOCA emergency procedures. Following closure of the MSIVs (or closure of the turbine bypass valves after they are initially opened), the operator must open both atmospheric dump valves to continue adequate cooldown.

Assuming the SGs are not depressurized at an adequate rate, heat transfer to the SGs eventually will be lost. (This failure event is indicated on the event tree as "SG at set-point pressure") Given a loss of SG heat transfer, another means of augmenting RCS depressurization is required to prevent core failure. One possible operation would be to open one or both PORVs. However, due to the high SG temperature, the RCS cold-leg temperatures are expected to remain relatively high. As a result, manually opening the PORVs is not specified in the LOCA emergency procedures. If the operator fails to open the PORVs in this sequence, the possibility of core failure is assumed. If the RCS depressurization is augmented by opening the PORVs, core recovery is considered probable.

Operation of the CVCS in these sequences would have a small, positive effect on core recovery for a specific range of break sizes. However, the major impact of the additional 132-gpm injection rate is to scale the range of break sizes of interest upward by 132 gpm (or the existing capacity of the CVCS).

Assuming adequate SG depressurization, the subsequent effects of PORV operation on core recovery are considered in the upper branches of the event tree. Depressurization of the SGs and the procedurally required trip of the RC pumps will significantly reduce RCS cold-leg temperatures. Under these conditions, the operator may be required to depressurize the RCS by opening the PORVs if the ductility limits for the reactor vessel are threatened. If the operator fails to manually open the PORVs or the PORVs fail to open on demand, the only hazard would be PTS, which may jeopardize reactor vessel integrity. However, the likelihood of vessel failure under these conditions is expected to be small. The effects of PTS on the Calvert Cliffs reactor vessel have been analyzed and the results presented.[5]

In summary, sequences of events following a small-break LOCA have been developed and discussed. Due principally to the relatively low shutoff head of the HPSI system, operation and manual control of the atmospheric dump valves, turbine bypass valves, or pressurizer PORVs have been assumed to be required for core recovery and/or protection of reactor vessel integrity. The following are considered to be significant results of the SICS analysis.

1. Small-break LOCAs can be initiated by one or more of several identified control system failures.

2. Operation of the atmospheric dump valves, turbine bypass valves, and/or PORVs are presently procedurally required to ensure recovery.
3. Operation of these control elements in these sequences requires manual initiation and regulation.
4. The SB-LOCA emergency procedure does not explicitly specify the equipment to be initiated and regulated.

In addition, the relatively low RCS pressure (200 psi) at which the SI tanks and the LPSI system begin to inject coolant increases potential dependency on control system actions.

4.3.2.6 Loss of Non-Emergency ac Power. During normal operation, Calvert Cliffs plant electrical loads are fed from two 500-kV ac buses through a series of transformers to lower voltage buses. The RC pump motors are fed from 13-kV ac buses, and other plant loads are fed from 4-kV ac buses. Buses 11 and 14 in Unit 1 are designated 1E safety-qualified buses and, upon being deenergized, are fed from on-site emergency DGs.

A loss of non-emergency ac power is defined as deenergizing all 13-kV ac buses simultaneously. This transient results in a reactor trip, a loss of MFW flow, and coastdown of the RC pumps. The event tree illustrating the accident sequences initiated by this loss of power is shown in Fig. 4.5.

The principal mitigating equipment consists of the emergency on-site DGs and associated circuitry. If 1E kV ac buses 11 and 14 are energized by the DGs, the transient event tree would be similar to the loss of MFW transient sequences described in Sect. 4.3.2.4 (see Fig. 4.4). In addition to the loss of FW, the RC pumps would be stopped and RC flow maintained in the RCS by natural circulation.

In the event the DGs failed to energize either 4-kV ac bus, the plant could be maintained in a hot shutdown condition by operation of the steam turbine-driven AFW pump and associated control valves. This equipment can be initiated and maintained in operation by the dc power system including battery-backed 120-V ac buses.

4.3.2.7 SG Overfeed Transients. As discussed in Sect. 4.3.2.2, the MFW flow rate must be controlled following a reactor trip to prevent overfeeding the SGs. The event tree describing SG overfeed sequences is shown in Fig. 4.6.

Following reactor trip, the MFW regulating valves are signaled to close and the bypass regulating valve is opened and controlled to maintain 5% of the full FW flow rate. If either of the two main regulating valves fail to close, the SG level in the affected SG will begin to increase rapidly.

Once this overfeed transient is initiated, it can be terminated only by operator action. The actions considered most likely are manual trip of the MFW pumps or manual closure of the MFW isolation valves. If the

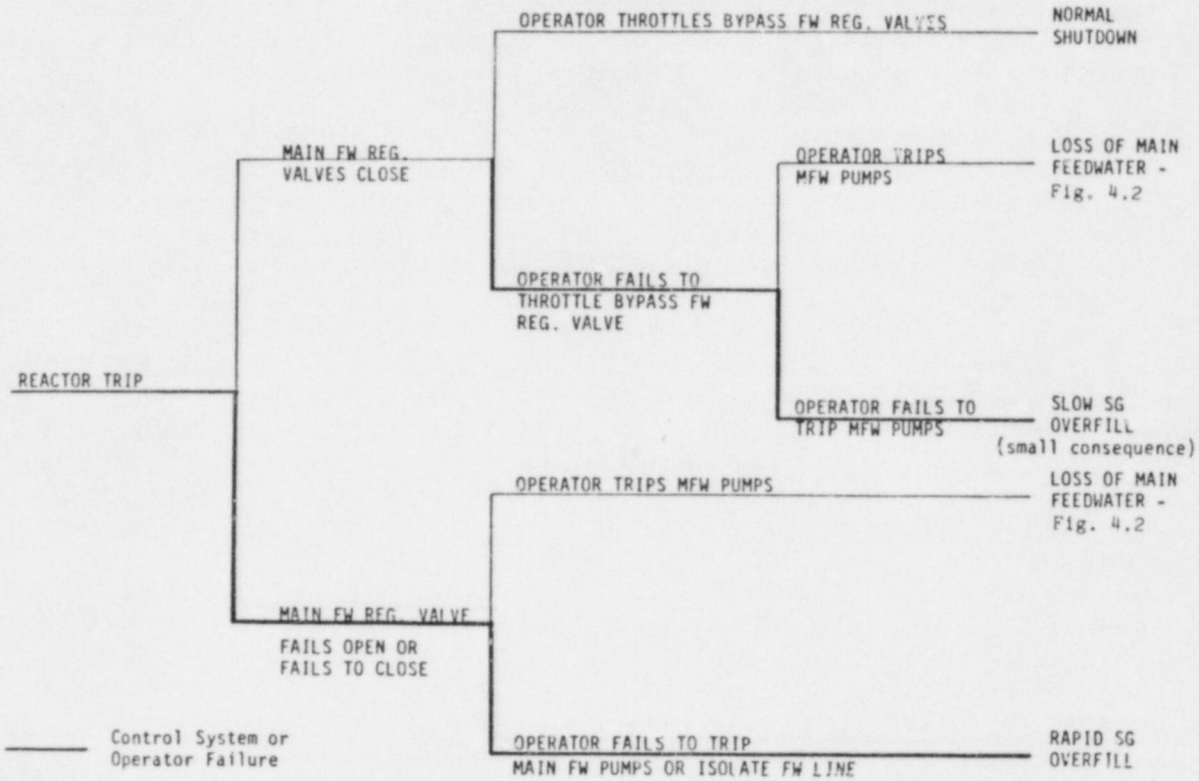

Fig. 4.6. SG overfeed event tree (excess FW flow).

operator recognizes the overfeed and trips the pumps or closes the isolation valves, the overfeed will be terminated and the transient will proceed as depicted in the loss of MFW event tree (Fig. 4.4). However, if the operator fails to terminate the overfeed, the SGs will overfill and high-temperature water will be injected into the main steam lines.

A similar transient can occur if one of the MFW regulating valves fails open at power. In this case, the turbine and reactor will trip on a high SG level, and the overfeed transient will proceed as noted or be terminated automatically depending on the particular failure. A number of failures can occur that initially could open the regulating valve but would be blocked by the "turbine tripped" signal, resulting in regulating valve closure. Other failures can be postulated that open a regulating valve but are not blocked by the turbine tripped signal.

A special overfeed transient has been identified following closure of the MFW regulating valves. It is an unusual sequence in that a slow overfeed is initiated (assuming that all equipment operates as designed). Following reactor trip, the bypass FW regulating valves are automatically controlled to maintain 5% flow. However, SG level is not controlled automatically. As core-generated decay heat decreases, the SG level will

begin to increase. Unless the MFW flow rate is manually controlled or terminated, the SGs will overfill and water will be injected into the steam lines. Although failure to manually control FW flow and SG level following reactor trip is considered highly unlikely, the initiating event (reactor trip) frequency is high. Thus, the overfill sequence frequency due to failure to manually throttle the bypass control valves may be comparable to more rapid overfill sequences involving equipment failure. However, the extremely slow rate of fill, even assuming that overfill occurs, is not expected to have significant consequences (i.e., this transient is not expected to jeopardize steam line integrity).

The rapid overfill sequences identified in Fig. 4.6 are considered significant results of the SICS analysis. The frequency of these sequences (which include only those not automatically terminated by a turbine tripped signal) are expected to be relatively high due to the lack of an automatic means of terminating the transient independently of the regulating valves (e.g., automatically tripping the MFW pumps on high SG level).

The consequences of rapidly injecting FW into the steam lines are unanalyzed and not well defined. The principal concern is that the injection of water will result in dynamic loads on the steam lines or their supports, which could jeopardize their integrity. Failure of the steam lines under these conditions would result in a severe RCS overcooling transient and could jeopardize other equipment due to pipe whip, jet impingement, or flooding.

4.3.2.8 Steam Line Break. An uncontrolled release of steam from the main steam lines, due either to a control system failure as shown in Fig. 4.1 or a postulated pipe break, will result in a severe RCS overcooling transient. The sequences resulting from the SLB or equivalent are shown in the event tree in Fig. 4.2.

The systems mitigating a SLB are safety systems. As the SGs are depressurized following the SLB, the main steam isolation valves (MSIV) and MFW isolation valves are closed automatically. This action terminates the transient for all breaks downstream of the MSIV and limits the steam release for breaks upstream of the MSIV. The MSIVs will isolate all control system failure-initiated steam line break equivalents except failed open atmospheric dump valves. Although these two valves can release a total of 5% of full main steam flow, even a failure of both valves to close would be a self-limited transient with negligible safety consequences.

4.4 IDENTIFICATION OF OPERATOR EFFECTS

The effects of the possible range of operator actions (i.e., correct actions, delayed correct actions, incorrect actions, or inaction) are summarized briefly in this section. Discussions of operator action are also included in some descriptions of specific scenarios of interest.

In general, we have found that the effects of operator action or misaction are more significant in the case of Calvert Cliffs than in the companion Oconee study because many more of the plant control functions at Calvert Cliffs are performed by operators.

The ground rules of the SICS study state that an operator is assumed to take the correct action on time if (1) the symptoms of the problem are clear; (2) the appropriate responses are included in the written procedures, and the procedures are clear and unambiguous; (3) the means are available to take the correct action (e.g., instrument air is available to power an actuator); and (4) sufficient time is available for the response. In cases where operator action is critical to the successful termination of a transient, the maximum (safe) time allowed for operator response is to be noted.

However, judgments are clearly difficult to make as to whether symptoms of any given problem would be clear to an operator, and whether sufficient time would in fact be available for the appropriate response. Based on studies of actual operator response, a considerable range of uncertainty of performance could be factored into these studies. This would depend not only on the symptoms available (instrument readings) and the time within which actions must be taken, but also on more subjective factors such as individual operator capabilities and training, time of day, and distractions. Hence, in the assignment of mumeric values to the probability of an operator responding correctly, it should be understood that plant- and operator-dependent error bands are very large, corresponding roughly to the scatter in the data in one of the better reports currently available on operator response.[14] Because no specific database is available on Calvert Cliffs operator performance, the current SICS study does not attempt to distinguish between or make judgments about their predicted performance or compare them to those reported in ref. 14 or elsewhere.

Perhaps because operator response is so difficult to quantify and the response time requirements for different accidents vary widely, the NRC guidelines are typically not specific on how much time is generally allowed for appropriate operator action. For example, in the case of the operator manually tripping the primary circulating pumps during certain classes of SB-LOCAs, it was assumed that proper operator action could not be counted on in less than 2 min.[15] A "commonly accepted" (but, to our knowledge, undocumented) NRC limitation is that a plant must be able to survive any transient without any operator action for at least 10 min. The corresponding limit imposed on the British Advanced Gas Reactors is 30 min.[16]

As part of an ORNL subcontract with UCLA, a new tool for dealing with operator response, known as the "confusion matrix" technique, is being evaluated for possible application to SICS. (The results of the UCLA study were not available for inclusion in this report; they will be published separately.) Confusion matrices are two-dimensional arrays quantifying the probability of confusion between any of the events listed on the horizontal axis (actual events or transients) with those

listed on the vertical axis (operator diagnosis). The probabilities for misdiagnosis, which appear as nonzero off-diagonal elements, are a function of how much time the operator has to figure out what happened; therefore, confusion matrices typically are presented in sets representing several different times (e.g., 15 min and 1 h). The probabilities assigned to each of the elements in the matrix are subject to a wide variety of opinions and, in fact (as previously indicated), would be very dependent on the particular operator and his or her experience and state of alertness, the plant instrumentation display, the effectiveness of training programs and drills, and the number of other distractions present. Confusion matrices were applied to two probabilistic risk assessments (PRAs), one at Oconee-3 and the other at Seabrook.[17,18] Input data for the matrices developed in these studies were derived from interviews with simulator training staff, operators, systems analysts, and psychologists. Of the two studies, only ref. 17 presented numerical probability estimates (in the Seabrook PRA, nonnegligible probabilities for confusion were given only as high, medium, or low). The applicability of these studies to the Calvert Cliffs SICS analysis is tenuous at best because of the obvious reactor and site dependency of the data derived. The results are of general interest, however, in that they do show some of the possible areas of misdiagnosis in the major sequences of interest to SICS. For the Oconee PRA, the total probability for misdiagnosis of an SB-LOCA within 15 min of the break was about 0.05, dropping to 0.007 after the operator has had 1 h to react. The corresponding probabilities for excessive FW flow (SG overfeed) were 0.03 and 0.002 respectively. The Seabrook PRA rates the confusion level for a SB-LOCA (in the first 5 to 15 min) as "low," while there were two "high" confusion level entries for the SG overfeed category (SG tube rupture and small steam line/feed line break) as well as low confusion level items in several other categories listed.

In summary, the two PRA studies indicate that chances for misdiagnosis (and, therefore, improper response) to the two major sequences of interest are about 1 in 20 to 1 in 30 in the short term, and about 1 in 100 to 1 in 500 in the long term.

4.5 ELECTRICAL FAILURES THAT COULD CONTRIBUTE TO SIGNIFICANT ACCIDENT SEQUENCES

The plant electrical system was treated separately in the FMEA because the electrical system is common to many systems throughout a nuclear power plant. However, the charter for USI A-47 was to determine how the electrical system could cause control systems to fail with safety implications.

The plant electrical system is an auxiliary system that can impact reactor core cooling indirectly by affecting core cooling systems. Therefore, electrical system FMEAs were directed toward those events determined to be of importance based on safety implications of control systems failures. That is, for the events determined to be significant, electrical system failures that could contribute to the events were

examined. Events for which control system failures would have the more significant safety implications were SG overfill and a critical size break in the primary system boundary that would not depressurize the primary system rapidly enough to obtain adequate HPSI flow. These events are summarized in Sect. 4.3.1.

For purposes of the FMEA, the Calvert Cliffs-1 electrical system was separated into (1) power supplies to the reactor regulating systems, (2) the bulk ac distribution system, and (3) the dc distribution system. The regulating systems included in the analyses were reactor regulating system; RC pressure regulating system; pressurizer level regulating system; FW regulating system; atmospheric steam dump and turbine bypass system, and turbine generator control system. Some of these systems are powered by non-Class 1E instrument buses and some by Class 1E vital buses. Failure of these control systems caused by power supply failure is presented in detail in Appendix D, including a design description of each of the regulating systems and a description of how they fail on loss of power. Appendix D includes an analysis of the effects of failure of a single motor control center (MCC), instrument bus, vital bus, or dc bus that provides power to any of the control systems. Appendix D also includes an analysis of the effect of failing two buses simultaneously. No electrical failures identified would, independent of other failures, have a significant safety implication. However, Appendix D contains some recommendations which, if implemented, may help avoid some undesirable failure modes.

The bulk ac distribution system was evaluated for failure modes that could contribute to important events caused by control system misoperation. The ac distribution system buses reviewed included the 500-kV switchyard, 13-kV service buses, 4160-V unit buses, 480-V unit buses, 480-V MCCs, and 120-V instrument buses. Loss of all ac power was not included as part of this program because that issue is being addressed in a program to resolve USI A-44, "Station Blackout." Single-bus failures that could contribute to the events of interest were evaluated, and failure modes that could affect multiple buses were examined.

The 125-V dc system interacts with the ac distribution system, plant regulating systems, and plant safety systems. Dc bus failures were examined to determine how such failures could affect other systems that contribute to events of interest.

Summarized here are control system power supplies and ac and dc power supply failures that could contribute to SG overfill or to loss of the capability to reduce primary system pressure. A single instrument bus failure can cause FW to a SG to fail "as is," and the same instrument bus failure could lead to a trip of the reactor if an operator does not respond properly. After a reactor trip one SG would be overfed, and if the operator does not trip the FW pump, that SG would overfill. A sequence of events for this scenario is discussed in Sect. 4.3. Other effects caused by instrument bus failures that are undesirable, although not serious relative to safety implications, are discussed in Appendix D.

4.5.1 Electrical System Failures that Affect the Capability to Reduce Primary System Pressure

Because of the low pressure rating of the HPSI pumps at Calvert Cliffs, it is necessary to reduce primary coolant system pressure below its normal operating value in order for the HPSI pumps to add water to the reactor vessel. The event tree for a small-break LOCA (Fig. 4.3) and shows that at least two control systems will affect the sequence of events: SG pressure control systems and the PORVs on the pressurizer.

4.5.1.1 Electrical Failures of the PORV. The PORVs and PORV isolation valves are supplied by Class 1E 480-V MCCs 104R and 114R (see Fig. 4.7). Control power for the auxiliary relay that operates a PORV is supplied from a 480/120-V transformer connected to MCC 104R or 114R. Likewise, control power for operation of the motor-operated isolation valve is supplied from a separate 480/120-V transformer connected to MCC 104R or 114R. The PORVs may be operated manually or automatically. They open automatically on a 2-of-4 high-pressure (2385 psig) signal from the reactor protection system (RPS), the set point that would also trip the reactor. An auxiliary relay powered from 125-V dc bus 11 is energized to open both PORVs when the pressurizer pressure exceeds 2385 psig. The PORV isolation valves are manually operated and do not require control power other than from the associated 480-V MCC. An unusual feature of the PORVs and the isolation valves is that a PORV and its isolation valve are not powered from the same 480-V MCC. MCC 104R powers a PORV and MCC 114R powers its associated isolation valve.

For the sequence of interest, failure of both PORVs to open is an undesirable failure that may lead to core damage as described in Sect. 5.2.1. Both PORVs would fail closed if power from MCCs 104R and 114R failed, but these MCCs are Class 1E and are in different divisions. Failure of both buses simultaneously with a small-break LOCA is not likely. Another failure mode for which both valves would not open could occur if a PORV were isolated at the time a small-break LOCA occurred followed by failure of MCC 104R or 114R. Prior to the LOCA the PORV could have been isolated because of a leak. If the MCC that powers the functional PORV failed, it would also fail the power to the closed isolation valve. Until power was restored, one PORV could not be opened and the second PORV would remain isolated. If power failed because of a fault on the MCC, the MCC would have to be repaired before power could be restored. However, if the power source failed, MCCs 104R and 114R are connected through two normally open breakers that are also key-locked to prevent connecting the two division sources together. This interconnection could be used to restore power to the failed MCC.

4.5.1.2 Electrical Failures Affecting SG Pressure Control. A second control system failure that can affect the capability to depressurize the primary system during a small-break LOCA is the turbine bypass and steam dump system. Operation of the turbine bypass and steam dump controller is described in Appendix D. Atmospheric steam dump is controlled automatically by primary coolant T_{avg} error, but the atmospheric dump valves can also be controlled manually from the control room or from the

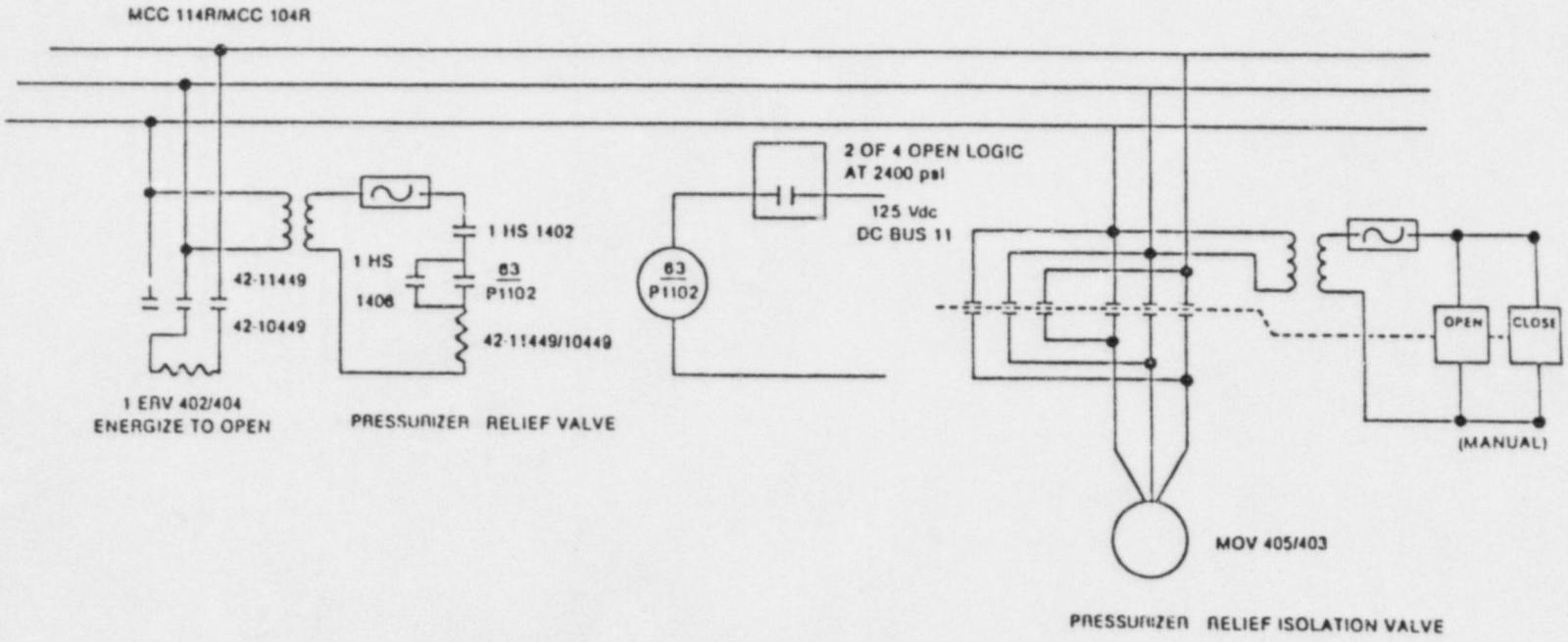

Fig. 4.7. Functional block diagram of pressurizer relief valve control.

emergency shutdown panel. The turbine bypass is controlled automatically by a T_{avg} error signal or by a 900-psia set point to a pressure controller as described in Appendix D.

For the operator to have the capability to reduce SG pressure from the control room, nonvital control power 1Y09 must be available. However, the operator can position two 3-way pneumatic hand valves to transfer atmospheric dump valve control to the auxiliary shutdown panel. At the auxiliary shutdown panel there are two hand controllers, one for each of the atmospheric dump valves. One of these hand controllers is powered by vital bus 1Y01 and the other by vital bus 1Y02. Therefore, a complete loss of auxiliary shutdown panel control of the atmospheric dump valves because of electrical failures would require failure of two vital buses normally powered from different dc sources.

The turbine bypass valves are pneumatic valves operated by current-to-pneumatic (I/P) converters and by solenoids for quick action. Control power for the turbine bypass instrumentation is supplied by Instrument Bus 1Y09 and dc Bus 11. Failure of either of these supplies will cause the turbine bypass valves to fail closed.

4.5.1.3 Summary of Electrical Failures Affecting Primary System Pressure Control. No single failures in the electrical system would result in both PORVs becoming nonfunctional simultaneously with loss of the atmospheric dump and turbine bypass control system. Loss of power to MCC 114R would fail power to one PORV and cause loss of power to Instrument Bus 1Y09. Failure of 1Y09 would cause loss of automatic control of the turbine bypass valves and loss in the control room of manual control of the atmospheric dump valves. However, manual control of the atmospheric dump valves could be transferred to the auxiliary shutdown panel by positioning two manual, pneumatic, three-way valves--one for each dump valve. For this failure the operator could reduce primary pressure with one remaining functional PORV and with two atmospheric dump valves manually controlled from the auxiliary shutdown panel.

If power cannot be restored to MCC 114R through its normal feeder, a connection to MCC 104R could be used. Likewise, Instrument Bus 1Y09 can be connected to Instrument Bus 1Y10 if power cannot be restored to 1Y09 through its normal feed from MCC 114R. The time period from initiation of the event until possible core uncovery needs further analysis because the transients may be slow enough for restoration of ac power to be a significant factor in the progression of the transient.

4.5.2 Electrical System Failures That Affect SG Overfill.

SG overfill can result from failure to control the MFW or AFW pumps, failure to regulate the FW flow regulating valves, or a combination of the two. The AFW is not considered in this section because it is a standby safety system. An AFW false start while the MFW pumps are operating would result in SG level increase until the main feed flow

regulating valve reduced MFW flow to maintain level in the SG. Some electrical failures could cause SG overfeed and overfill unless terminated by operator intervention.

4.5.2.1 Electrical Failure of the SG FW Control System. The normal electrical feed to the FW control system is a Class 1E 120-V ac vital instrument bus from an essential safety features (ESF) inverter. Upon failure of this circuit, the level system is automatically transferred to a non-Class 1E 120-V ac instrument bus. (This FW regulating system is described in Appendix D, Sect. 3.5.) Each SG has a MFW regulating valve controlled by its associated FW control system. There are no redundant FW control systems; however, to prevent loss of FW to a SG, each SG control system has redundant power sources that are transferred automatically. Each of the two FW regulating valves receives control power from a different instrument bus, and loss of an instrument bus will cause the associated regulating valve to fail as is. Failure of Instrument Bus 1Y09 will also cause the MFW pump turbine to fail as is (described in Sect. 4.5.2.2). This will not cause a plant transient by itself, but if the plant trips--which could occur on loss of instrument power--one SG would be overfed and an operator would have to decrease FW flow to prevent SG overfill.

4.5.2.2 Electrical Failure of the FW Pump Turbine Control System. FW turbines require steam, lubricating oil, and electrical power for orderly operation. Steam to the MFW pump turbine is supplied from main steam, reheat steam, or the auxiliary SG. Lube oil is supplied by the main oil pump, which is powered from 480-V MCC 106, by the auxiliary oil pump (powered from 480-V MCC 116), or by the emergency oil pump (connected to 250-V dc bus 13), which will start automatically on low oil pressure. Electrical power to the turbine speed control circuits is supplied by 120-V ac instrument power 1Y09 and 125-V dc power from an ESF battery.

Automatic speed control is derived from the pressure differential (dP) across the MFW regulating valve. The controller varies the speed of both pumps based on a low value dP signal from the FW regulating valves. The main purpose of this control loop is to maintain efficient pump operation rather than to control flow. The low signal selector forces the pumps to run at the same speed, with the SG level controls modulating the control valves. Failure of 1Y09 or components fed from it will cause the automatic control action to cease with the turbine speed as is.

With no automatic control action, the operator may control turbine speed by use of the motor speed changer, which is powered from a dc bus. This action can regulate the speed only below the as-is failed speed setting because of the hydraulic low-value selector gate. If a SG is being overfed because of failure of an instrument bus, the motor-driven speed changer would still give the operators manual control of the FW turbine.

If 1Y09 is energized and loss of dc power occurs after the motor speed changer control has reached the high speed stop limit, automatic control

will have no effect unless the automatic action requires speeds of less than 2000 rpm. The loss of dc power would cause the MFW turbine trips to fail because they are energized to trip. The dc power loss is annunciated.

4.5.2.3 Summary of Electrical Failures Affecting SG Overfill. Failure of one instrument bus can cause SG overfeed, but no single failure of an electrical system will cause an overfill condition, although prompt, decisive operator action may be required to prevent overfill. There is some redundancy in the level control but not in the FW turbine control. There exist ways of reestablishing failed buses through alternate feeds by manual operations, which could be a short-term solution if the failure indeed occurred at the bus.

4.5.3 Quantitative Analysis of Electrical Failure

Electrical failure probabilities were estimated to show how they contribute to SICS failure. Electrical failures that could cause both pressurizer PORVs to fail closed were examined to determine the probability that both PORVs would fail to open. There are no single-element cutsets other than common-cause failures that can cause both PORVs to fail to open simultaneously. The basic events are discussed in Sect. 4.5.1.1, and estimates of their probabilities or frequencies of failure are as follows:

1. Independent failure of a single 480-V MCC (104R or 114R): 3.5E-2/ry (ref. 19)

2. Common-cause failure of two 480-V MCCs: 3.5E-3/ry.

3. Unavailability of a single PORV (isolated for maintenance by a motor-operated valve): 2E-2.

The frequency per reactor year that both PORVs would be unavailable simultaneously is

$$P_{TE} = (3.5E\text{-}2)(3.5E\text{-}2) + 3.5E\text{-}3 + 2(2E\text{-}2)(3.5E\text{-}2) = 6E\text{-}3/ry.$$

However, unavailability of both PORVs is of no consequence unless there is also an accident. The probability of a critical size LOCA occurring simultaneously with failure of both PORVs is small because there is no identified coupling of those events other than a possibility of the operator isolating the PORVs in error or failing to open them. Assuming that both PORVs are unavailable for 24 h following their simultaneous failure, the probability that they would be unavailable when requested is (3E-3)(5E-3/ry) = 2E-5/ry.

Failure of electrical systems also affects the sequence in which the atmospheric steam dump and turbine bypass valves are needed to control primary system pressure by dumping steam from the secondary. The probability of loss of secondary-side atmospheric steam dump and turbine bypass controls involves failure of Instrument Bus 1Y09 and failure of

an operator to transfer control of the atmospheric steam dump valves (ADVs) to vital buses 1Y01 and 1Y02. Transfer of the ADVs from 1Y09 to 1Y10 is accomplished by manually positioning a three-way pneumatic valve for each dump valve. Repositioning these valves transfers control of the ADVs to alternate controllers in the auxiliary shutdown panel. These controllers are powered by 1Y01 and 1Y02. The probability of simultaneous occurrence of a critical size LOCA and loss of the instrument bus is small, but the instrument bus is occasionally out of service for repair. If the SB-LOCA occurred when 1Y09 was unavailable, secondary-side pressure control would not be functional. It is estimated that it would take a maximum of one day to repair 1Y09 when it fails. Therefore, unavailability of 1Y09 would be (1 d/365 d) (3.5E-2/ry) = 1E-4/ry, assuming it has the same probability of failure as a 480-V MCC. The probability of operator failure to transfer to 1Y01 or 1Y02 was estimated to be 0.1. The probability of a small-break LOCA would be multiplied times the unavailability of the secondary steam dump systems.

Electrical failures that may contribute to SG overfill involve failure of a FW turbine speed control system. Failure of one of two instrument buses will cause one of the MFW regulating valves to fail as is, and it would also cause the FW turbine speed control to fail as is. If the instrument bus failure caused a plant trip, one of the SGs would be overfed and the operator would have to decrease FW flow to prevent overfill. The probability of an instrument bus failure is 3.5E-2, and the probability of operator error is discussed in Sect. 4.4. The probability of overfeeding at least one SG equals the probability that one of two instrument buses will trip times the probability that it would cause a plant trip. After an instrument bus failure, an operator would have time to transfer regulating systems to the remaining bus. We have estimated that the operators would have a 0.5 probability of avoiding a reactor trip. Therefore the probability of SG overfeed is (2)(3.5E-2)(0.5) = 3.5E-2. The probability of SG overfill is discussed in a later section.

4.6 INSTRUMENT AIR FAILURES THAT COULD CONTRIBUTE TO SIGNIFICANT ACCIDENT SEQUENCES

A FMEA of the instrument air (IA) system was performed to determine the impact of major component failures within that system on the Calvert Cliffs nuclear units. A brief description of the IA system can be found in Appendix B of this report, and the detailed FMEA of the IA system is contained in Appendix C.

The IA system FMEA disclosed that many of the failures considered did not result in substantial disturbances to the IA system because of the design of the Calvert Cliffs system. This was due in large measure to the thoughtful design of the IA system and the use of redundant components. The analysis disclosed, however, that several failures have

the potential to cause loss of adequate air pressure for the valves, instruments, and controllers throughout the plant. These failures include the following:

1. Failure open of pressure relief valves on the air receivers and the IA compressor aftercooler/moisture separators.

2. Failure closed of manual isolation valves on the IA prefilters, air dryer, and afterfilters.

3. Rupture of the IA service header downstream of the afterfilters. (This type failure is not a control system failure but has occurred on operating nuclear plants and is, therefore, considered in this report.)

4. Failure closed of branch isolation valves in the IA service header downstream of the afterfilters.

For all of the above failures except actual rupture of the service header, the loss of air event can be reversed (terminated) simply by opening (closing) the appropriate valves in the IA system. For example, the event that results from failure open of air receiver pressure relief valves can be terminated by closing the inlet and outlet isolation valves of the affected receiver. This means that, for most of the failures considered, it is reasonable to assume that operations/maintenance personnel can take effective action to terminate the loss of air event given a reasonable amount of time in which to diagnose the problem.

The IA system provides compressed air for operating valves, instruments, and controllers throughout the Calvert Cliffs plant. Equipment, systems, and plant areas utilizing IA include the following:

1. DGs 11 and 12
2. RWT heat exchanger room
3. West penetration room
4. Letdown heat exchanger
5. Spent fuel pool cooling room
6. Valve compartment
7. CVCS ion exchanger
8. Component cooling room
9. ECCS pump room Nos. 11 and 12
10. VCT and east rooms
11. Charging pump room
12. Miscellaneous waste receiver tank room
13. Cryogenics room
14. RCW pump room
15. Auxiliary Building HV ac areas
16. Service water pump room
17. East piping penetration room
25. Access control HV ac
24. I&C shop
25. Plant computer
26. Blowdown tank area
27. RCW Waste evaporator
28. Miscellaneous waste evaporator
29. Upender
30. Caustic storage tank
31. Makeup demineralizer
32. Condensate polishers
33. Turbine deck, east and west
34. Auxiliary boilers
35. Deaerator
36. Condenser area ring
37. Sewage treatment
38. Intake circulating water pumps
39. Condensate precoat filters
40. Turbine lube oil coolers

18. East electrical penetration room
19. Service water heat tank area
20. Main plant area
21. Battery vent area
22. Component cooling head tank
41. FW Heaters 14A, 14B, 15A, 15B, 16A, and 16B
42. AFW pumps
43. Condenser area west
44. Moisture separator reheaters 11 and 12

From the above list it can be seen that the IA system serves a large number of loads throughout the plant, and that consequently the loss of air could result in very complicated operational problem scenarios. This situation is mitigated somewhat by the fact that, while all of the systems listed use instrument air for routine plant operations, most of the plant systems can be satisfactorily operated in a manual mode should valves and instruments misoperate as a result of instrument air failures. Further, not all of the systems listed have a direct effect on plant response, and therefore are not necessary to control or mitigate abnormal plant transients or to bring the plant to a safe shutdown condition.

In a loss-of-IA casualty, a piping rupture or other failure of the IA system causes air to be released at a rate faster than it can be supplied by the operating compressors. IA pressure therefore decreases below the normal 93- to 100-psig operating range, and the following sequence of actions automatically occurs:

1. The automatic (standby) IA compressor starts at 90 psig.
2. At 88 psig, an IA low-pressure alarm alerts the operator.
3. The plant air (PA) to the IA cross-connect valve opens at 85 psig IA pressure. As the PA system supplies air to the IA system, the PA system pressure decreases below the normal 93- to 100-psig operating range.
4. The other unit's PA compressor starts at 90 psig PA pressure and supplies air to the affected PA system and the PA tieline.
5. The PA service header isolation valves shut at 85 psig PA pressure, causing the two PA compressors to discharge only to the affected IA system.
6. The PA low-pressure alarm actuates at 80 psig.
7. The containment IA control valve closes at 75 psig IA pressure.

In Emergency Operating Procedure EOP-14, "Loss of Instrument Air," (recently changed to AOP-7D)[20] remedial actions are specified for two classes of IA loss. IA is defined as completely lost when IA system pressure drops below 50 psig or when pressure is decreasing so rapidly that leak detection and isolation is not possible. A partial loss of instrument air is considered to exist when IA system pressure is above 50 psig and is decreasing slowly enough to allow time for leak detection and isolation.

Conditions characteristic of a complete loss of instrument air are

- IA system pressure less than 50 psig and decreasing,
- IA low-pressure alarm,

- IA compressors both running or both off,
- PA-to-IA cross-connect valve open,
- IA compressor trouble alarm,
- both IA dryer towers regenerating, and
- switching failure alarm at IA dryer.

Once a complete loss of instrument air is suspected, the procedure calls for both reactor and turbine trip as well as other supplementary actions that will bring the plant to a cold shutdown condition in a controlled manner. In a partial loss of instrument air, the rate of pressure decrease is low enough to allow operators to search for the cause of the air loss. Once the problem is identified, the affected component is isolated. The preferred method of leak isolation is to close the root stop valve associated with the leaking component. Isolating the leak by closing a branch header isolation valve may cause serious control problems in unaffected systems supplied by that branch header. If the IA pressure drops below 50 psig prior to finding and/or isolating the leak, the event must be treated as a complete loss of instrument air, and appropriate actions must be carried out.

The 50-psig pressure value that separates a complete from a partial loss of IA has been determined to be the minimum system pressure necessary to ensure proper operation of the electropneumatic converters used to control the components of various systems. Below ~50 psig, system controls can be seriously affected, finally failing in the state designed for a loss of instrument air.

From the preceding discussion it can be seen that the detailed effects of a loss of IA event are quite difficult to predict. There are a number of reasons for this difficulty, including the large number of components that depend upon IA and the various scenarios that can be proposed for creating a loss-of-air casualty. Table 4.14 summarizes the general effect of the loss of IA event on various plant control systems and components required to bring the plant to shutdown. From this table it can be seen that loss of IA will have the following general effects on the operator's ability to control important plant systems and components:

1. The RC pumps must be tripped because adequate cooling water cannot be maintained. This necessitates natural circulation cooling, which is not an unexpected or unusual requirement.
2. RC pressure must be maintained using manual control for the pressurizer heater banks along with control of the auxiliary spray valves.
3. Pressurizer level must be maintained using manual control of the charging pumps.
4. The MFW system cannot be relied upon for a control-label supply of FW, and by procedure the MFW pumps are stopped.
5. The AFW system is relied upon to provide inventory to the SG following loss of IA. In a complete loss of IA event, the two steam-driven AFW pumps will operate at maximum speed; however, this is not expected to be a problem. AFW flow control valves are air

Table 4.14. Summary of instrument air failure impact on key reactor systems and components

1. REACTOR COOLANT SYSTEM
   Reactor vessel: N/A
   Steam generators: N/A
   RC pumps: Loss of instrument air may lead to pump trip due to loss of cooling water to RCP seals.
   PORV: N/A, electric operators.
   Code safety valves: N/A, electric operators.
   Quench tank: Fill valve from demineralized water storage tank, gas collector header relief valve, and tank drain valve fail closed.

2. CHEMICAL AND VOLUME CONTROL SYSTEM
   Letdown control and stop valves fail closed, causing pressurizer level to increase. Operator must control level by manually operating the charging pumps.

3. PRESSURIZER LEVEL REGULATING SYSTEM
   The electronics of this regulating system are not affected by IA failure; however, it will be ineffective because letdown valves close on loss of instrument air. Pressurizer level must be controlled by manually operating the charging pumps.

4. REACTOR COOLANT PRESSURE REGULATING SYSTEMS
   The electronics of the regulating system are not dependent upon instrument air; however, pressurizer spray valves fail closed on loss of air and RC pressure control is affected. Operators must control pressure by operating the heater banks manually and using the auxiliary spray valves. The auxiliary spray valves are quite reliable since they are backed up with IA by the salt water system air compressors and accumulators.

5. REACTOR POWER REGULATION
   N/A

6. MAIN FEEDWATER, CONDENSATE, AND HEATER DRAIN SYSTEMS
   MFW regulating valves: Loss of IA causes these valves to fail as is, possibly causing SG overfeed.
   MFW bypass valves: Loss of IA causes these valves to fail open.
   MFW pump turbine steam supplies: N/A
   Heater drain system valves: Failure of these vales is expected to cause substantial upsets in the MFW system, possibly culminating in a trip of the condensate booster and MFW pumps. The operator is instructed by EOP-14 to stop heater drain pumps on loss of IA.

Table 4.14 (continued)

7. MAIN STEAM SYSTEM AND ATMOSPHERIC STEAM DUMP AND TURBINE BYPASS CONTROL SYSTEMS

Atmospheric dump valves: These valves fail closed on loss of IA: however, the IA supply to the operators of these valves is backed up by an accumulator and salt water compressors 11 and 12, and loss of air is considered a low probability event. Valves can be operated manually if necessary.

Turbine bypass valves: These valves fail closed on loss of IA.

Main steam isolation valves: N/A, electric operators.

Main steam safety valves: N/A, mechanical operators.

8. AUXILIARY FW SYSTEM

Auxiliary FW motor-driven pump: N/A

Auxiliary FW steam-driven pump: The AFW pump turbine steam isolation valves and governor valves are air operated and fail open on loss of IA, which will cause the pumps to go to the high-speed stop. These valves are supplied with air from separate accumulators that can be supplied from either the salt water air system or the IA system. This redundant accumulator-backed arrangement increases the reliability of the control air required by these valves.

Auxiliary FW control valves: These valves fail open on loss of air. Also, each of the control valves is provided with redundant I/P converters fed from separate air accumulators. This arrangement increases the reliability of the valve air supply and provides a reservoir of control air to assure good AFW control after loss of IA.

9. COMPONENT COOLING SYSTEMS

Loss of IA causes RC pump seal cooling water valves to close; however, they can be opened manually. Upon isolation of RC pump seal cooling water, RC pumps must be tripped within 10 min.

10. SERVICE WATER SYSTEM

Loss of IA will cause the valve controlling the flow of service water to the IA and PA compressors to fail closed, thus causing the compressors to eventually trip on high temperature. Air will be supplied automatically by the other unit's PA compressor, and that compressor is cooled by service water from the sister unit. This makes loss of air due to a service water failure very unlikely.

11. SALT WATER COOLING SYSTEM

Loss of IA has no significant effect on the salt water cooling system.

Table 4.14 (continued)

12.	DIESEL GENERATORS 11, 12, AND 21 Loss of air will not affect the ability of the diesel generators to start and function. Each diesel unit contains its own air compressor and redundant air receivers to assure that the diesel air start system can function independently of the IA system.

operated but are backed up by an air accumulator arrangement that is charged by either the IA system or the salt water air system. In the unlikely event the air accumulator arrangement fails, flow control valves fail open on loss of air, and SG inventory can be maintained by starting and stopping the AFW pumps.

6. Main steam pressure must be controlled by use of the atmospheric dump valves following a loss-of-IA event. These valves are air operated from a highly reliable air accumulator arrangement maintained charged either by the IA system or by the salt water air system. The atmospheric dump valves are therefore expected to be available for steam pressure control following loss of IA; however, even if air is not available to operate these valves, they can be operated manually by operations personnel.
7. A number of other systems of lesser importance must also be controlled manually. In some cases this will require the operator's presence at locations away from the control room.

The purpose of the emergency procedure is to provide the operator with general guidance for performing those actions that may be needed during loss of IA transients; however, from this discussion it should be apparent that loss of IA can create situations requiring prompt operator actions that would be difficult to anticipate. Our review indicates that the current emergency procedures do not provide the operator with sufficiently detailed instructions. It is imperative that operators be well trained and properly guided by EOPs to respond to loss of IA events.

4.7 GENERIC IMPLICATIONS OF CALVERT CLIFFS-1 SCENARIOS

4.7.1 Background

While the failure scenarios at Calvert Cliffs-1 have necessarily been examined from a plant-specific point of view, the ultimate objective is a generic resolution of the impacts of control upon safety. To extend our results to other plants of C-E design, we must determine how broadly representative are the design features that have proven of interest in our investigation. The following section describes other C-E plants in terms of their resources for countering a small-break LOCA through depressurization and subsequent water injection at lower than operating pressure.

4.7.2 Water Injection and Pressurizer Pressure Relief Features in Other C-E Plants

In a plant having the same water injection and pressurizer PORV features as Calvert Cliffs, small-break LOCA scenarios developed for Calvert Cliffs can be expected to have similar resolutions. Plants with HPSI systems of higher pressure than Calvert Cliffs will be less dependent on depressurization in the critical range of break sizes. Plants lacking PORVs for depressurizing, and having HPSI systems incapable of providing

water until the pressure is well below the operating point, may have potential dryout problems more severe than those at Calvert Cliffs.

Several C-E plants have features similar to Calvert Cliffs-1 and -2. These designs include HPSI at about 1275 psia, CVCS charging with three positive displacement pumps of 44 gpm each, and 2 pressurizer PORVs. These plants are Ft. Calhoun, Millstone Point 2 [which counts one charging pump as an emergency core cooling system (ECCS)], Palisades, and St. Lucie 1 and 2.

The following C-E plants have about 1500-psia HPSI systems with no PORVs: San Onofre 2 and 3, Arkansas 2 (which has one 3-in. pressure relief line with two manually actuated motor-driven valves in series), and Waterford 3.

Maine Yankee has pressure reduction and water injection systems similar to those in Westinghouse plants. It has a 2700-psia HPSI system and two PORVs, and there are three charging pumps: one positive displacement and two centrifugal.

Palo Verde 1, 2, 3 (not yet on line) provide 1950-psia HPSI systems and no PORVs.

4.7.3 Combinations of Identified Failures with Generic Implications

Essentially all of the broad and augmented FMEAs we have performed for Calvert Cliffs have involved single failures or enhanced-probability multiple failures. (Enhanced-probability multiple failures can be simultaneous failures with a common mode, or may arise from multiple failures with one or more system elements in an undetected failed state prior to the final initiating failure of something else.)

There are two reasons for excluding from consideration the multiple simultaneous failures of many independent control elements: (1) failures of vanishingly low probability are of no interest to the program; and (2) an examination of all combinations of (say) a hundred control elements would be a task of unmanageable magnitude. However, there is some interest in examining a limited number of low-probability simultaneous failures in order to extend Calvert Cliffs results to generic conclusions concerning other nuclear plants of C-E.

4.7.3.1 Rationale for Examination of Multiple Failures. Producing generic conclusions from plant-specific studies requires two extrapolations:

1. Are such problems as may be discovered in the plant-specific study applicable to all plants of the same class? This is the easier of the two extrapolations to make, and requires specific inquiry as to the extent to which the design weaknesses responsible for the identified failures are present in other plants.

2. Do other plants of the same class have failure modes not possible in the sample plant because of some accidental or engineered superiority in the sample plant's design? This is not easy to determine in a plant-specific study.

One approach to help determine whether "I'm all right, but you aren't" is to examine the effects of a multitude of independent failures upon the sample plant (in this case Calvert Cliffs). In the sample plant these failures may have no conceivable common cause, no mechanism for undetected prior failure of one or more of them, and no common elements of any kind. Suppose that, despite the demonstrable near-zero probability of their simultaneous failure, we examine the consequences of failure in four control elements deliberately chosen for the (adjudged) undesirability of their simultaneous outage.

Two possibilities exist: the consequences are either acceptable or they are not. If the consequences for several such "worst-case" multiple failures are benign, the judgment can be made that even if a sister plant somewhere has controls interconnections not present in Calvert Cliffs, such interconnections will permit no multiple failures of safety significance. However, this approach to generic extension fails if the consequence of such an impossible-in-Calvert-Cliffs combination of failures is unacceptable. It would at that point be necessary to demonstrate that system isolation existed in other plants to the same degree as in Calvert Cliffs. The information to do this might or might not be available.

4.7.3.2 Catastrophic Common Cause for Multiple Failures. Unacceptable consequences due to multiple simultaneous failures may be of vanishingly small probability if the failures are truly independent. However, certain catastrophic events, though themselves having very low rates of occurrence, may provide common causes for the otherwise independent failures. Earthquakes, fires, and floods are all potential initiators. Investigations of "worst-case" multiple failures as discussed in the preceding section may also provide a preview of results to be expected from, for instance, a seismic vulnerability investigation. Should results of such test cases be benign, the consequences of seismically induced multiple control failures may be predicted to be of low concern. Should results be unacceptable, probabilities of the precipitating catastrophic event would require evaluation, as would recommendations for hardening the systems at risk.

4.7.3.3 Multiple Failures Examined. Several classes of events involving multiple independent failures have been simulated, and the results are described in Sect. 6.1. An example is the class of multiple failure events that lead to dryout. If one SG level indicator is failed high, and the low-level and low-low-level trips are both failed, a dryout event in one SG can be initiated. Again, three independent failures are required, as well as inattention on the part of the operator, making this of trivial probability in Calvert Cliffs. Should these events have a potential common cause in another plant, the

consequences involve dryout of only one SG, and hence this sequence has acceptable safety consequences on a generic as well as a plant-specific basis.

5. QUANTIFICATION OF SEQUENCE FREQUENCY

In Sect. 4, two transients--a class of small-break LOCAs and rapid SG overfeeds--were found to be of principal interest to the SICS Program. In each case, these transients were found to lead to consequences of concern, potential core damage, PTS, or SG overfill due to control system failures. The transient sequences resulting from these control system failures were not automatically terminated by safety system action.

In Sect. 5, the frequencies of the transient sequences of concern are evaluated. The results of sequence frequency evaluation are summarized in Sect. 5.1, and the bases of the transient frequency quantifications for the small-break LOCAs and SG overfill sequences are discussed in Sects. 5.2 and 5.3 respectively. Section 5.4 discusses operating experience at the Calvert Cliffs station and other Combustion Engineering-designed plants.

5.1 SUMMARY OF FREQUENCY QUANTIFICATION RESULTS

In Sect. 5, the frequencies of significant sequences identified in Sect. 4.3 are estimated. The small-break LOCA event tree (Fig. 4.3,) identified two sequences of potential concern: one potentially leading to insufficient core cooling caused by failure to initiate RCS cooling or depressurization, and the other an overcooling (PTS) sequence. The frequencies of these sequences were estimated to be as follows:

Transient	Estimated frequency (events/reactor year)
Small-break LOCA Insufficient core cooling	8E-6
Small-break LOCA Overcooling (PTS precursor)	1.5E-6

As indicated in Sect. 5.2.2, the PTS sequence frequency does not include the conditional probability of vessel failure. Based on the vessel failure analysis of ref. 5, the sequence frequency of vessel failure events would decrease to ~10^{-8}/ry or less when the conditional probability of vessel failure is included.

The relatively high estimated frequency of insufficient core cooling following a small-break LOCA was due principally to the following factors:

1. Coupling of the LOCA to loss of instrument air due to automatic isolation of service water to the instrument air compressors,
2. Lack of a specific procedural step directing the operator to transfer ADV control to the auxiliary shutdown panel, and

3. Lack of a procedural step directing the operator to open the PORVs or initiate auxiliary spray in the event RCS cooling failed.

The frequency of this LOCA sequence could be reduced significantly by providing more explicit direction in the existing LOCA emergency procedure[21] or the draft emergency procedure.[22]

The frequency of the rapid SG overfill sequence, shown in the overfill event tree (Fig. 4.6, as discussed in Sect. 5.3) was estimated at 9E-3/ry. The frequency of the SG overfill sequence was based on an estimated frequency of overfeed events (not terminated by turbine trip) of 9E-2/ry and an estimated probability of 0.1 failures per demand that the operator fails to terminate the overfeed in the three or more minutes available.

The estimated overfill frequency is in reasonable agreement with the one observed SG overfill in 19 ry (Calvert Cliffs Units 1 and 2). In this event, the SG reached its maximum indicated level 2 min after reactor trip, and the operators isolated the FW pump ~4.5 min after reactor trip. No damage to the steam lines or supports was reported, although one of the TBVs failed to close (which may have been unrelated to the overfill).[23]

5.2 QUANTIFICATION OF SMALL-BREAK LOCA SEQUENCES

The small-break LOCA event tree (Fig. 4.3) described several event sequences initiated by a small-break LOCA. In addition to the sequence involving safety system failure (HPSI), two sequences were found to be of interest. Failure to initiate and maintain an RCS cooldown via the SGs coupled with a failure to depressurize the RCS via the PORVs or auxiliary spray could lead to core damage. Also, assuming that RCS/SG cooldown was initiated, a subsequent failure to depressurize the RCS (assuming that reactor vessel RTNDT limits were exceeded) would be a PTS sequence.[5]

The frequencies of these two sequences involve the frequency of a small-break LOCA in a size range of concern and the conditional probabilities that subsequent electromechanical or operator failures will prevent the successful performance of necessary mitigating functions. Because of the functional differences between these failure modes, each is discussed separately in Sects. 5.2.1 and 5.2.2.

5.2.1 Small-Break LOCA Sequences Involving Insufficient Core Cooling

As shown in Fig. 4.3, one sequence was found that may result in core damage caused by insufficient core cooling. This sequence requires a specific size of small-break LOCA, a failure to initiate RCS cooldown via the SGs, and a failure to depressurize the RCS via the pressurizer PORVs or the auxiliary spray. The frequency of this sequence may be estimated by combining the frequency of the initiating LOCA and the conditional

probabilities of the two function failures. This process is depicted in a fault tree format in Fig. 5.1. The frequencies and conditional failure probabilities used in this fault tree are discussed below.

The estimated frequency of a small-break LOCA in the size range of interest was developed based on the Calvert Cliffs PTS analysis.[5] The size range used was <0.016 ft^2, which includes single unisolated PORVs, RC pump seal failures, and SG tube ruptures. The estimated frequency for this event was 1.5E-2/ry, which is believed to be conservative since PORV failure and break sizes of less than 0.0005 ft^2 have not been found to produce the core damage sequences described. SG tube failures and pump seal failures do contribute significantly to this frequency and could be expected to initiate break sizes of interest. To account for break sizes covered by the 1.5E-2/ry frequency that are not expected to lead to core damage, the referenced frequency was quantitatively reduced by an order of magnitude. The small-break LOCA initiating event frequency for insufficient core cooling sequences is 1.5E-3/ry.

Following initiation of the LOCA, the success of either of two mitigating functions--RCS cooldown via the SGs or RCS depressurization via the pressurizer PORVs or auxiliary spray--would lead to successful mitigation of the transient. The contributing failures that could lead to a simultaneous failure of these functions are depicted on the fault tree.

RCS cooldown is initiated by the operator opening both ADVs and/or any of the turbine bypass valves (TBVs) in accordance with Step 11 of the LOCA emergency procedure[21] or step F(3) of the draft procedure.[22] Failure of this function could be caused by operator error or by electromechanical failures of the valves or associated support systems.

The ADV and TBV are automatically controlled to limit RC average temperature and steam line pressure. In order to initiate an RCS cooldown, however, the operator must place these valves in manual control and open them. This action is routine, and sufficient time (1 h) exists to perform the function. Although the operator will be under a stressed condition due to the LOCA, this action is expected to be performed with very high reliability. Consequently, the probability that the operator will fail to initially open the valves is estimated to be 0.001 based on the data of ref. 14. This probability assumes that the control room staff is not confronted by complicating factors such as a loss of instrument air when performing this function.

The principal mode of initiating the RCS cooldown is assumed to be manual operation of the TBV. This action will result in reducing the pressure in the steam lines and, unless the operator bypasses the steam generator isolation system (SGIS), will result in the MSIVs being closed at a steam line pressure of 653 psia (T_{sat} = 495°F). MSIV closure would isolate the TBV and, unless the operator subsequently opened both ADVs, would terminate the RCS cooldown.

As mentioned, this action is considered routine, with the understanding that the operators will be under the added stress of the LOCA sequence.

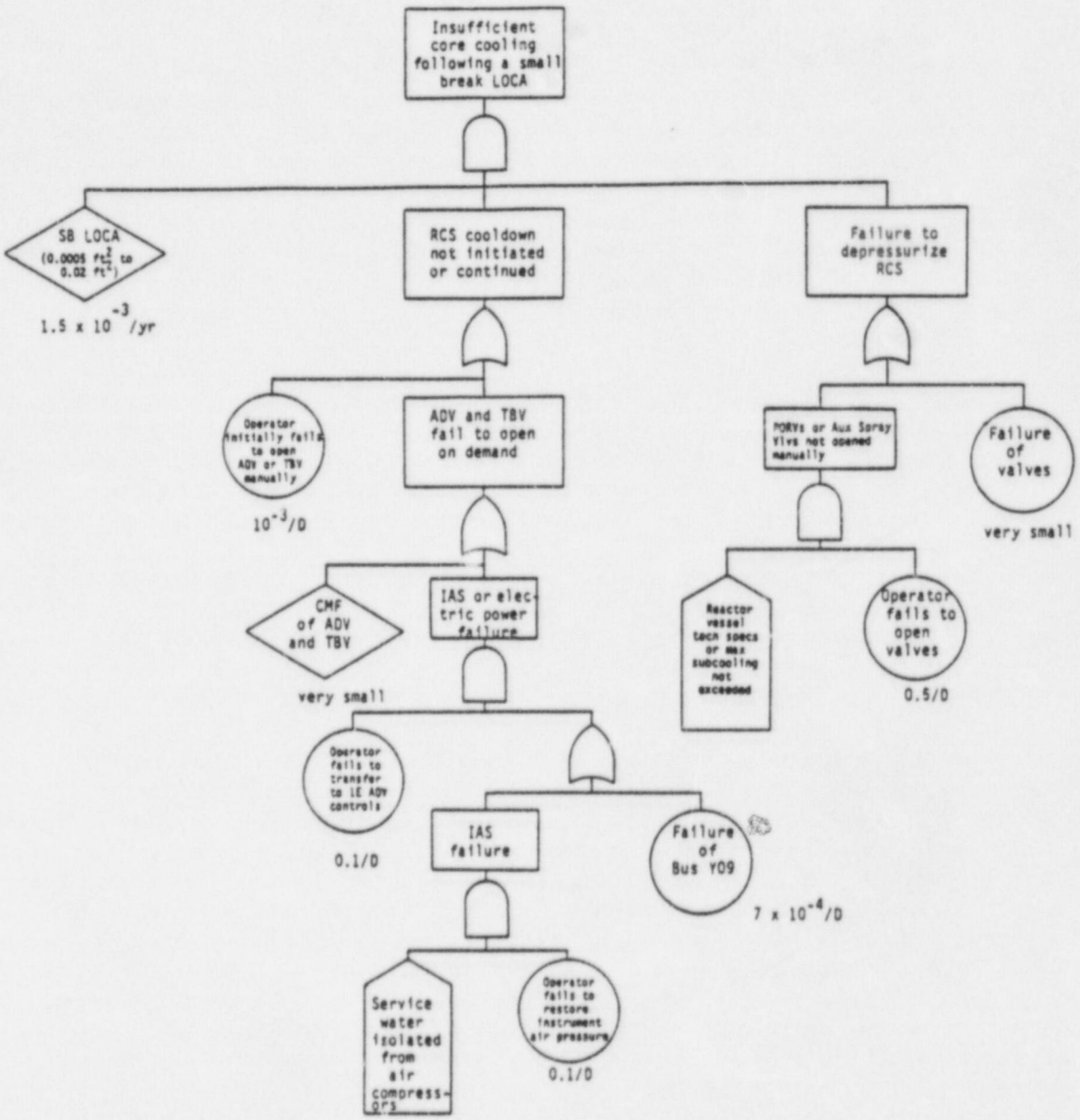

Fig. 5.1. Insufficient core cooling LOCA sequence fault tree.

The probability that the MSIVs will be allowed to close and the ADVs not opened has not been estimated separately. Although not specified in the emergency procedures, the contribution of failure of this action is included in the estimated 0.001 failures per demand discussed previously.

Electromechanical failures that could cause the ADV and the TBV to fail to open or remain open on demand consist principally of a loss of Instrument Bus Y09 or a loss of instrument air pressure. A postulated common-mode failure of all ADVs and TBVs is considered to have an insignificant probability. In the event of either failure, the operator has the option of manually transferring control of the ADV to the auxiliary shutdown panel, which consists of independent 1E controls and an instrument air supply from the salt water air compressors.

Nonvital instrument buses such as Y09 have been estimated to fail with a frequency of 3.5E-2/ry (ref. 5). However, even assuming a 24-h outage time per failure, the probability of the bus being in a failed condition at any given time (e.g., when it is needed because of a LOCA) would be only 1E-4 (the probability of Y09 being unavailable at the time of the random LOCA event).

The failure rate of the IA system per LOCA demand due to random IA system failures is estimated to be smaller than the Y09 failure rate. However, due to the LOCA, the resulting SIAS signal will isolate the service water flow from the instrument air and plant air compressors. This loss of cooling water could result in a trip or failure of the air compressors and an eventual reduction in instrument air pressure.

The timing of the events in this sequence is important. Initiation of RCS cooldown is addressed early in both the existing and the draft LOCA emergency procedures, and should begin well within 1 h after the LOCA. Restoration of the service water supply to the compressors and restoration of instrument air pressure is Step 20 of the existing procedure and steps "O" and "P" of the draft procedure. During this time period, loss of instrument air pressure is considered likely.

Once instrument air pressure is lost, restoration of service water is complicated by the fact that the service water isolation valves close on loss of air pressure. In the LOCA procedure, the operator is instructed to start the plant air compressor in this event.

This sequence places complicated demands on the operator, especially considering the LOCA in progress and other resulting equipment responses to the loss of instrument air pressure. For this reason, the probability that a loss of instrument air pressure will occur and not be recovered in the near term has been estimated to be 0.1.

If instrument air pressure is lost, the operator has the option of transferring ADV control to the auxiliary shutdown panel, which will provide an air supply from the salt water air compressors and 1E manual ADV controllers. Although this operation is available to the operator,

it requires opening manual air supply valves located in a tamper-proof (presumably locked) enclosure. Furthermore, the operation is not addressed in the existing or draft LOCA procedures, while the restoration of service water and normal instrument air is addressed specifically. For these reasons, tne probability that the operator will fail to transfer control of the ADVs given a loss of instrument air has been estimated to be 0.1.

Combining the failure probabilities as depicted on the fault tree and discussed above yields a probability of failing to initiate or continue RCS cooldown of 1.1E-2 per LOCA demand.

Assuming that RCS cooldown fails, the operator may open the pressurizer PORVs. This action increases the effective LOCA size to a point where RCS cooldown is not required. Although available, this operation is not addressed in the existing LOCA procedures for cooldown assurance. The operator is cautioned to depressurize the RCS if the reactor vessel pressure-temperature technical specifications are exceeded. This, however, would require lower vessel temperatures than the saturated conditions expected if RCS cooldown failed. In spite of the lack of procedural instruction, the operator should be given credit for deducing the need to depressurize. For this reason, the estimated probability of the operator failing to depressurize given failure of RCS cooldown is 0.5 per LOCA demand.

The draft procedure specifies that the operator should initiate auxiliary spray to depressurize the RCS if the RC subcooling exceeds 200°F. This condition does not exist in the sequence of interest. Instruction Step H(2)(b) directs the operator to initiate AFW if subcooling is below 30°F.

Combining the estimated frequency of the small LOCA, the conditional probability that RCS cooldown is not initiated or continued and that the RCS is not depressurized via either the PORVs or auxiliary spray yields an estimated overall sequence frequency of core damage events of 8E-6/ry. It should be noted that this frequency incorporates multiple operator failure probabilities that are, at best, difficult to estimate. The uncertainty in the estimated frequency is expected to be large.

5.2.2 Small-Break LOCA Sequence Involving PTS Conditions

Given a small-break LOCA and assuming that RCS cooldown is initiated and continued, the temperature of the coolant in the reactor vessel downcomer will decrease. The downcomer temperature will further decrease due to the addition of water from the HPSI system. The RCS pressure, however, will be determined by the saturation pressure at the higher core outlet temperature and will depend on the core decay heat rate, the LOCA size, and the SG heat transfer rate. Under these conditions, exceeding the reactor vessel RTNDT technical specification limit is credible for small-break LOCAs.

If the RTNDT limit is approached, the operator is cautioned to depressurize the RCS. Although not specified in the LOCA procedure, it is

assumed that the operator would open the pressurizer PORVs to depressurize the RCS with the existing procedure. In the draft procedure, the operator is instructed to initiate auxiliary spray at a RC subcooling limit of 200°F, which results in RCS depressurization. Failure of the operator to perform this function is assumed to result in a PTS condition as indicated in the LOCA event tree (Fig. 4.3).

The frequency of this sequence involves only the frequency of a small-break LOCA, 1.5E-2/ry, and the probability that the operator fails to open the pressurizer PORVs when indicated. Due to the relatively slow rate of change in reactor vessel conditions in this phase of the transient, it is assumed that the PTS condition will be avoided if the operator opens the PORVs or initiates auxiliary spray within 30 min of the indicated approach to the technical specification or subcooling limit. Based on the data of ref. 14, this would yield a probability of operator failure of 0.01 per demand and hence a PTS sequence frequency of 1.5E-4/ry.

It should be emphasized that this PTS frequency is for a stagnated LOCA overcooling event at pressure, but does not include the conditional probability of vessel failure. Based on ref. 5, the conditional probability of vessel failure given a stagnated LOCA and a 900 psi pressure is $\sim 10^{-4}$. Thus, the frequency of this sequence leading to vessel failure is $\sim 10^{-8}$/ry, which is not believed to be of significant concern.

5.3 STEAM GENERATOR OVERFILL

As discussed in Sects. 4.3.2.2 and 4.3.2.7, the MFW flow rate must be controlled following a reactor trip to prevent overfeeding the SGs. The event tree describing the overfeed transient is shown in Fig. 4.6. Two categories of potential SG overfill events were identified: rapid and slow. Slow overfeed transients occur via the bypass valves following closure of the FW regulating valves. As described in Sect. 4, slow overfeed transients are not considered hazardous even if SG overfill occurs.

Rapid overfeed transients, which could result in significant injection of high-temperature water into the steam lines, occur via the regulating valve. Following a reactor trip, a MFW regulating valve failure to close or spurious opening will initiate the sequence leading to rapid SG overfill. If the operator fails to trip the MFW pumps or isolate the FW line by closing the regulating valve or the MFW isolation valve, rapid SG overfill will result. The reactor trip used as the initiator for the SG overfeed event tree will also initiate turbine trip. Both trip systems are highly reliable, and failure of the reactor trip to initiate turbine trip will not preclude turbine trip on some other parameter. Likewise, failure of the turbine trip to initiate reactor trip will not preclude reactor trip on some other parameter. However, failure of the turbine trip signal to the regulating valve may contribute to rapid SG overfill. Hence, rapid SG overfill is partitioned into two cases.

In the first case, the regulating valve receives a closure signal from the turbine trip circuitry but the valve itself fails to close. In the second case, the regulating valve circuit fails to receive the closure signal from the turbine trip circuitry. Both cases were analyzed using fault tree analysis to determine the frequency of SG overfill.

5.3.1 Feedwater Valve Receives Closure Signal from Turbine Trip Circuitry

This case, depicted in Fig. 5.2, involves the following conditions: (a) the regulating valve fails to close, and (b) the operator fails to prevent overfill.

The regulating valve may fail to close due to loss of instrument air, mechanical failure, or failures of FW regulating system components. Loss of instrument air to the regulating valve is further classified into loss of electric power to the air supply solenoid valve and the solenoid valve failing closed. The FW regulating system failures are further partitioned into current-to-pneumatic (I/P) transducer failure and hand/auto module failure. The failure rates and frequencies for these events are listed in Table 5.1.

The valve failure itself is not expected to produce a rapid SG overfeed until the reactor is tripped. However, once valve failure initiates SG overfeed, the reactor and turbine are expected to trip on high SG level (or other parameter).

The "operator fails to prevent overfill" event was estimated to occur at a frequency of 0.1 per demand. This estimate is based on the following assumptions:

1. FW flow rate is 5.576 × 106 lbm/h/SG;
2. Steam flow rate is 5% of operating flow rate following turbine trip or 2.8 × 105 lbm/h/SG; and
3. Following high-level alarm indication, the addition of 25,605 gal (1.8 × 105 lbm) of water will result in SG overfill.

Calculated time to overfill based on these assumptions is 2 min. Clearly, 2 min is a short time for the operator to interpret the situation and take appropriate remedial action. However, the operator is instructed in Step 4 the Emergency Operating Procedure for Reactor Trip (EOP-1)[24] to verify that the FW regulating valves close and that FW bypass valves open to 5% flow. The supplemental action section of this procedure also includes four steps (4, 5, 6, and 7) that are designed to prevent SG overfill. Hence, a failure rate of 0.1/demand appears reasonable.

The frequency of SG overfill if the turbine trip signal to the FW valve is received is 9E-3/ry.

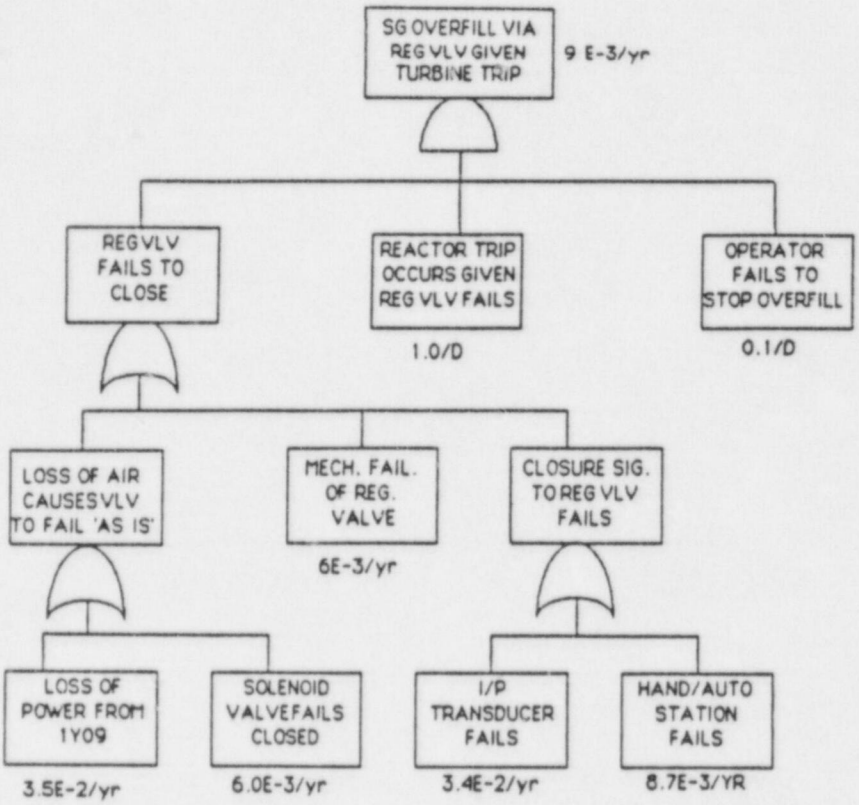

Fig. 5.2. Fault tree of SG overfill where regulating valve circuit receives turbine trip signal.

5.3.2 Feedwater Regulating Valve Circuit Fails to Receive Closure Signal from Turbine Trip Circuitry

This case, depicted in Fig. 5.3, involves the following conditions:

1. regulating valve fails to receive the turbine trip signal,
2. regulating valve is not closed, and
3. operator fails to isolate FW to SG.

The regulating valve may fail to receive the turbine trip signal because an "OR gate" module fails, the relay fails, or the cable fails to transmit the signal. The regulating valve may fail to close because it has failed open at power or because it fails to close. It should be noted that the failure rate for a regulating valve failing to close event is higher (0.5/y) than a similar event in Fig. 5.2 because the external "turbine tripped" signal is not available to block spurious signals originating from upstream modules. The 0.5/y valve was taken from Calvert Cliffs operating experience, in which 7 increasing FW flow events occurred in 14 years. As above, once the valve failure occurs, the reactor and turbine are expected to trip. The "operator fails to

Table 5.1. Basis of failure rates for steam generator overfill fault tree

Failure	Frequency/ Probability	Basis
Component Failures		
OR gate fails	5.2×10^{-3}/d	IEEE-500, p. 704 (6 tests/ year) (ref. 25)
Relay fails to close	5.7×10^{-4}/d	MILHDBK-217D (6 tests/year) (ref. 26)
Cable failure prevents valve closure	2.9×10^{-3}/d	IEEE-500 (6 tests/year) (ref. 25)
Regulating valve fails open at power	5.17×10^{-3}/yr	IEEE-500, p. 479 (ref. 25)
Loss of power for 1Y09	3.5×10^{-2}/yr	Reference 5
Mechanical failure of regulating valve	6×10^{-3}/yr	NREP (6 tests/year) (ref. 27)
I/P transducer fails	3.4×10^{-2}/yr	IEEE-500, p. 549 (ref. 25)
Solenoid valve fails closed	6×10^{-3}/yr	Comparable IEEE-500 (ref. 25)
Operator Error		
Operator fails to prevent overfill	0.1/d	2-3 minutes to act; but procedure instructs regulating valve closure
Operator fails to isolate feedwater	0.1/d	2-3 minutes to act; but procedure instructs regulating valve closure
Regulating valve fails to close	0.5/yr	NUREG/CR-3862 (ref. 28) (7 events in 14 years)

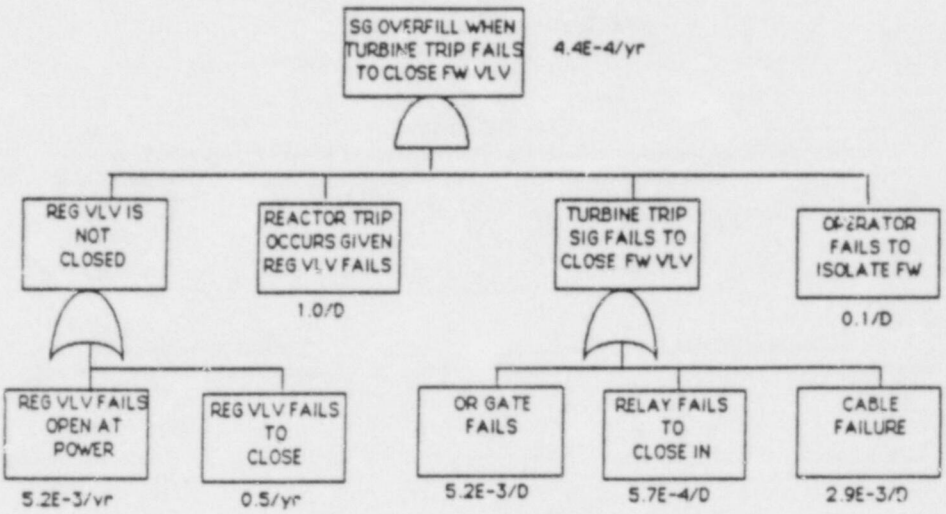

Fig. 5.3. Fault tree of SG overfill where regulating valve circuit fails to receive turbine trip signal.

isolate feedwater" event is equivalent to the "operator fails to prevent overfill" event of Fig. 5.2. The failure rate and frequencies for these events are listed in Table 5.1. The frequency for this case is 4.4E-4/y, an order of magnitude smaller than the valve failure case. The total frequency for the SG overfill event was calculated to be 9.4E-3/y, or one SG overfill event every 100 years.

On October 11, 1983, a SG overfill took place in SG 21 at Calvert Cliffs Unit 2. The SG overfill occurred 3 min after the initiator of the event and 2 min after the reactor trip.[23] Assuming ~19 y of reactor operation (Units 1 and 2 combined), the frequency for SG overfill is 0.05/y, which is in reasonable agreement with the calculated value of ~0.01/y (the 0.05 and 0.95 chi-squared limits for one event in 19 ry are 0.005 and 0.32 events per reactor year respectively.)

5.4 INITIATING EVENT PROBABILITIES

Quantification of expected frequencies of occurrence of the major sequences of interest depends on the initiating event frequencies as well as on the appropriate conditional probabilities associated with the success or failure of specific equipment operations (and the rough success and failure probabilities associated with operator actions where appropriate). An estimate of initiating event frequencies can be derived from the number of precursors or major sequence-initiating events that have occurred over a given number of plant operating years. These are summarized for Calvert Cliffs and/or other C-E plants in Table 5.2.

Table 5.2. Approximate frequency of initiating events/ sequence precursors based on Calvert Cliffs and other C-E plant operating histories

Event	Frequency* (events/plant year)
SG overfeed (high-level trip, overfill precursor)	0.2
SB-LOCA	0.01
Flooding	0.05
SG low level trip (AFW challenge)	0.6
Single electrical system failure	0.3

*All frequencies are based on 19 plant years of operation for Calvert Cliffs Units 1 and 2, except for the SB-LOCA, which is based on 88 plant years of operation for U.S. Combustion Engineering plants.

6. AUGMENTED FAILURE MODE AND EFFECTS ANALYSIS

6.1 RETRAN MODELING OF CALVERT CLIFFS-1

The FMEA described in previous chapters identified sequences of events judged sufficiently complex to merit further analysis in detailed dynamic simulations. This section describes the RETRAN model developed for this purpose and the results obtained. The mathematical tool was RETRAN2/Mod3,[29] the latest version of a widely used and extensively validated thermohydraulics production code obtained by license agreement with the developer, Electric Power Research Institute, and installed on the ORNL IBM-3033 computer. RETRAN2 is a first-principles methodology capable of treating two-phase flow with slip. Thermal equilibrium of phases is assumed except in the pressurizer, where nonequilibrium processes are important and special methodology is used. Heat transfer in solids is obtained from the conventional conduction equation. Point or 1-D kinetics is available for the reactor. The fundamental methodology is supplemented with a broad list of process submodels that calculate heat transfer coefficients, fluid and metal state properties, choked flow, form and wall friction losses, etc. Also supplied are component submodels for various types of valves and pumps (the latter of which incorporate four-quadrant characteristics for components in which two-phase or reverse flow may be expected) and head versus flow curves for others.

Extensive input allows the code to be highly particularized to a specific plant. Investment in time and manpower occurs primarily in setting up the base case. Changes are comparatively easy to implement.

6.1.1 Overview of the Model

The ORNL simulation is based upon a Calvert Cliffs-1 RETRAN model provided by BG&E and previously used in the utility's studies of certain aspects of plant dynamics. The BG&E model simulated principally the primary systems. The secondary side of each SG was represented by five nodes, and the balance of plant was represented by boundary conditions. To treat all cases of interest to the SICS Program, it was necessary to expand portions of the model, principally the SG and control system simulations. The additions are based upon Calvert Cliffs-1 plant-specific information provided by BG&E and C-E. The following components are explicitly represented (Fig. 6.1):

Primary systems
- core neutronics, including banked control rods
- thermohydraulics of both loops
- main pumps
- pressurizer, PORVs, safety valves, spray valves, heaters
- makeup and letdown
- high-pressure injection

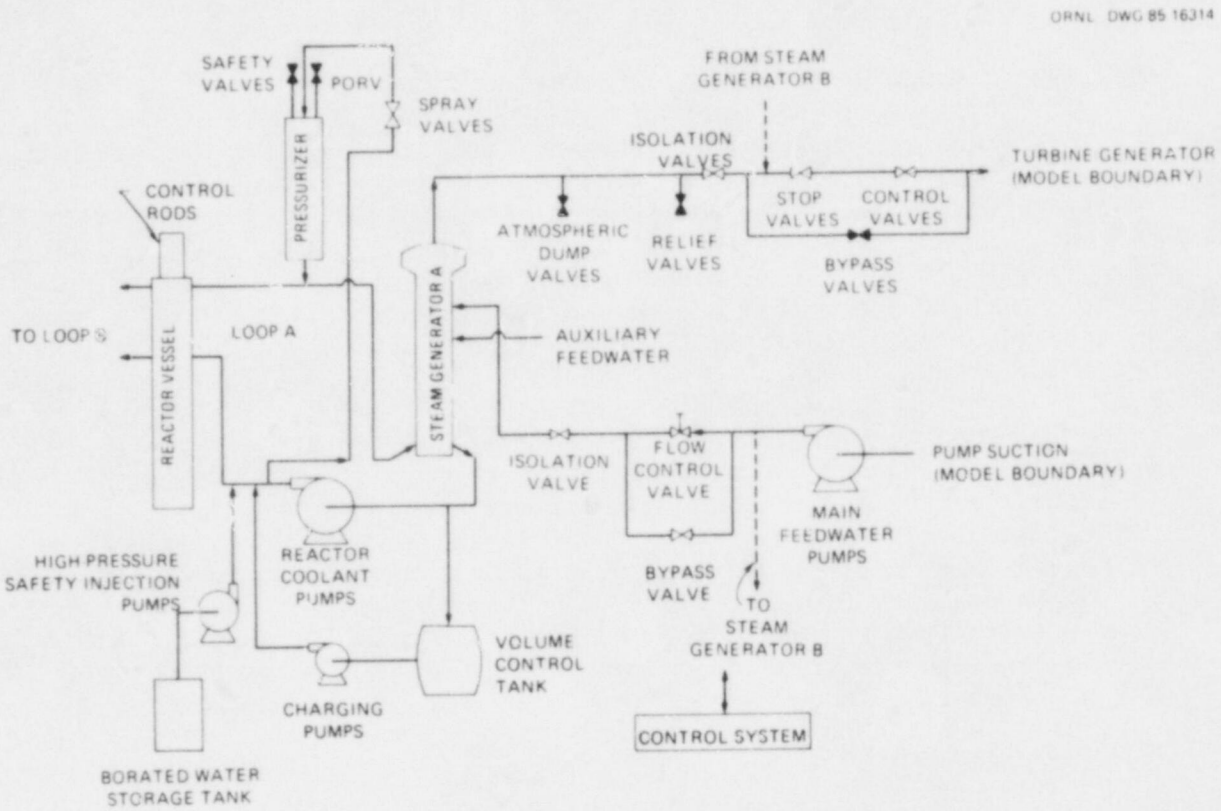

Fig. 6.1. RETRAN model of Calvert Cliffs-1.

Steam generators
- nodalization expanded to 10 nodes per secondary side
- wide- and narrow-range water level scales
- functional representation of moisture separator efficiency versus degree of overfill

Steam line safety and atmospheric dump valves

Feedtrain
- main feedpumps
- FW recirculation to condenser
- main feed regulating valves
- main feed isolation valves
- bypass valves

Turbine generator
- throttle valves
- main steam isolation valves
- turbine bypass valves

Control system
- reactor
- pressurizer water level
- pressurizer pressure
- SG water level, one-element and three-element modes
- FW pump speed
- FW bypass and recirculation
- turbine trips
- reactor trips
- MFW pump trips

Auxiliary feedwater, with controls

The primary side of the model is largely as supplied by BG&E. Simulated are the thermohydraulics of both loops; important heat absorbing metal masses of the vessel, plena, core, and pipes; makeup and letdown; and the HPI pumps. The nonequilibrium pressurizer includes PORVs, safety valves, and heaters. Neutronics are treated according to point kinetics. To this ORNL added simulation of banked control rods, achieved by modifying the effective neutron cross sections according to an appropriate program.

Refinement of the SG nodalization was prompted by the FMEA of credible malfunctions of the water level sensors. Sufficient nodes were added to permit direct simulation of the pressure taps used by the narrow-range scale in the upper portion of the generator and the wide range scale that spans the length of the generator. The ORNL calculation of generator water level is achieved by scaling the appropriate simulated pressure differentials to equal the known instrument readings at 100% power. This is the mathematical analog of the method used in the plant. Auxiliary feed flow is controlled at the low-low level set point, read on the wide-range scale.

Modeled valves include main feed valves and associated ΔP sensors that control pump speed. On turbine trip, these close and are isolated by block valves. Flow is shunted through bypass valves that require manual regulation to match afterheat; 15% capacity valves are regulated near 5%. The main pumps are protected against low-flow damage by recirculation lines that open when total flow per pump decreases below 498 lb/s. Steam line safety and atmospheric dump valves are banked and staged to open and reset at scheduled set points. The balance of plant is represented by boundary conditions at the turbine throttle valves and the main feedpump suction.

The control system was supplied in part by the BG&E model. Elements now in place consist of the following principal loops: (1) reactor power is modulated by matching measured coolant temperature to a demand temperature, (2) primary pressure is controlled by action of pressurizer heaters and spray, (3) generator water level is maintained by regulating the FW valves to match FW flow to steam flow and maintain level set

point, (4) primary inventory is controlled by the makeup and letdown system, and (5) FW pump speed is adjusted to yield fixed pressure loss across the MFW valves.

Protective or auxiliary control actions include HPI on low pressurizer pressure; initiation of AFW on low-low generator water level; reactor trip on high power, high or low primary pressure, and low SG level; trip of the MFW on high head pressure; and trip of recirculation valves on low pump flow.

6.1.2 Model Validation

The RETRAN2/Mod3 code, which provided the mathematical framework for the modeling described here, has received extensive validation against a broad spectrum of both process and systems data. The code in its present and previous editions has been used worldwide for many years to study PWR dynamics.

The Calvert Cliffs model supplied to ORNL was previously validated by BG&E against a loss-of-load event that occurred at Calvert Cliffs-2, sister plant to Unit 1, on October 11, 1983.[23] Parameters compared included pressurizer pressure and water level, loop A hot- and cold-leg coolant temperatures, loop B secondary pressure, and water level in both generators. The model showed generally good agreement with the data. The data have been supplied to ORNL and are being used to revalidate the expanded version.

6.1.3 Transients Run with the Model

The RETRAN model has been used to investigate three categories of scenarios: SG overfill, SG dryout, and primary-side depressurization that may uncover the core. The following 15 cases have been run:

Overfill:

1. Failure high of SG-A, steam flow reading at 1940 lb/s (nominal reading is 1640 lb/s); SG high-level turbine trip defeated.

2. Failure low of SG-A water level reading 10 in. below set point; SG high-level turbine trip defeated.

3. SG-A MFW valve failed full open in 1.5 s.

4. SG-A MFW valve failed full open in 1.5 s; MFW isolation valve failed open.

5. SG-A MFW valve frozen in place on reactor/turbine trip.

6. SG-A MFW valve frozen in place on reactor/turbine trip; MFW isolation valve failed open.

7. SG-A MFW valve failed full open in 1.5 s; with recent Calvert Cliffs-1 design change, FW isolation valves do not close on SG low-low level.

8. SG-A MFW valve frozen in place on reactor/turbine trip; with recent Calvert Cliffs-1 design change, FW isolation valves do not close on SG low-low level trip.

Dryout:

1. Failure low of SG-A steam flow reading at 1110 lb/s.

2. Failure high of SG-A level reading (narrow range) 10 in. above set point; low water level (narrow range) reactor trip defeated; low-low level AFW actuation trip (wide range) not failed.

3. Failure high of SG-A level reading 10 in. above set point on both the wide-range and narrow-range scales; low and low-low level trips defeated.

4. SG-A MFW valve failed completely closed (no leakage) in 5 s.

Primary-side depressurization:

1. Failure open of both PORVs.

2. Failure open of one PORV.

3. Small break (0.0015 ft^2) in hot leg of loop A.

The first eight cases assessed whether the stipulated malfunctions of SG controls could initiate an overfill event, the next four investigated whether stipulated failures of generator controls could induce dryout, and the last three explored whether small-break LOCAs on the primary side could result in core uncovery. In all cases the automatic power-level controller was also defeated.

The model initially included closure of main feed isolation valves on low-low generator water level trip (and AFW actuation), which until recently was the design of Calvert Cliffs-1. Closure of isolation valves on low-low trip has been deactivated. Discovery of this change came midway through the series of runs. Cases thought to be potentially affected by this change were repeated as indicated in the previous descriptions.

6.1.4 Calculation Results

6.1.4.1 Overfeed Transients. Flow to the generators is modulated by two error signals: steam flow is compared with feed flow, and generator

water level is compared with level set point. The sum of these errors is sent to the flow control valves. For the overfill case in which steam flow reading failed high at 1940 lb/s (compared with nominal 1640 lb/s), the control system initially acted to increase FW (Fig. 6.2). (In the plotted results, the first 60 s are used by the code to establish nominal steady state; the transients begin at 60 s.) However, the resulting increase in generator level nullified the steam flow error after ~1 min. Flow initially increased ~10% and then was restored to near nominal. There was negligible variation in primary pressure and temperature, and minor variation in SG level. This event did not result in overfill or overcooling.

In the second overfill study, the SG-A level reading was failed 10 in. below set point. The failure dominated the transient and was not compensated by the resulting feed flow-steam flow error. High-level trip was defeated. The SG-A moisture separators and steam dome were flooded in 10 min. (Fig. 6.3), at which time the liquid-steam mixture began injecting into the steam line (Fig. 6.4). (Figures 6.3 through 6.60 begin on p. 192.) Steam quality decreased to 85% (Fig. 6.5). The liquid content in the pipe between generator and turbine was ~1%. Since the level reading saturated before the generator was full because of pressure tap location, outlet quality provides a clearer indication of when the generator actually filled. Average core coolant temperature (Fig. 6.6) and power (Fig. 6.7) varied negligibly during the overfill, in part because of the slow rate of fill. When water began injecting into the steam line, pressure (Fig. 6.8) and feedflow to the generator (Fig. 6.9) varied slightly. The overfill did not result in overcooling the primary.

In the previous two overfeed studies, the error signal was of such size that the SG-A FW valve did not fail full open. In the next case the valve was postulated to fail full open in 1.5 s, thereby initiating presumably the maximum rate of overfeed. Generator A filled to the 50-in. high-level trip in 2 min (Fig. 6.10), at which time the reactor and turbine tripped. The feed valve to SG-B closed and the bypass valve opened to 5%, causing a small additional flow to SG-A (Fig. 6.11). Imbalances between feed flow and steam generation in SG-B caused its water level to drop to the low-low level set point 3 min into the overfill (Fig. 6.12), at which time AFW was initiated. A minute later, as previously scheduled at Calvert Cliffs-1, the MFW isolation valves to both SGs closed and overfill was effectively terminated (Fig. 6.11). No water was injected into the steam line. Minimum average core coolant temperature was 530°F (Fig. 6.13), minimum primary pressure was 1750 psig (Fig. 6.14), and minimum pressurizer level was 3 ft (Fig. 6.15).

The fourth overfeed case postulated that the MFW valve failed full open and that the associated isolation valve failed to close. As in the previous case, the reactor tripped on high SG level. The SG filled completely in 4.5 min. Because the reference pressure tap is several feet below the top of the generator, the level measurement saturated before the SG was full (Fig. 6.16). The abrupt drop in SG outlet

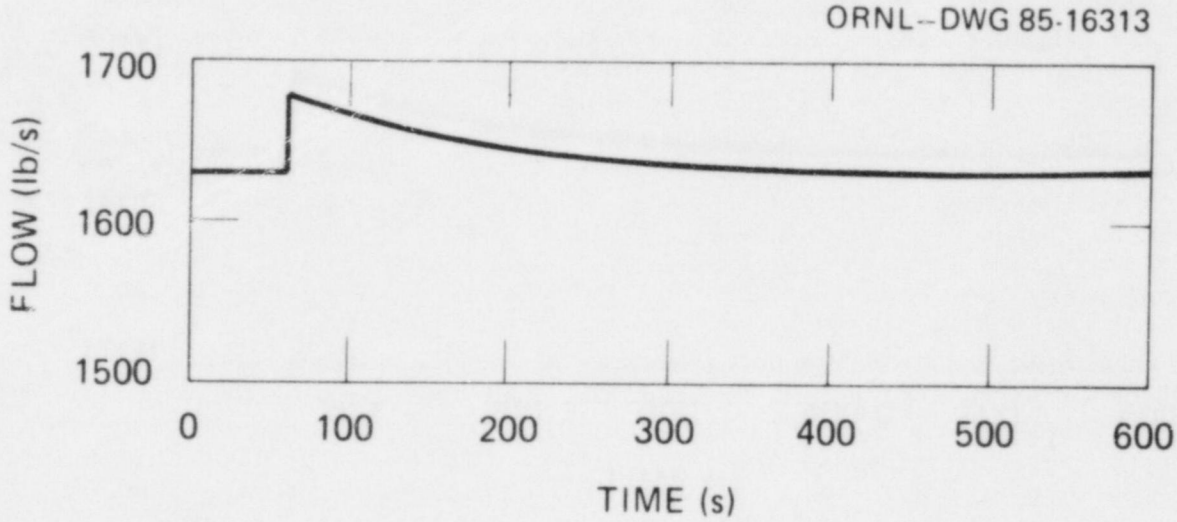

Fig. 6.2. SG-A FW flow with SG-A steam flow reading failed high at 1940 lb/s.

quality (Fig. 6.17) indicated when the SG was actually full. Shortly thereafter, liquid water was injected into the steam line (Fig. 6.18). Modest overcooling as a result of the overfill is apparent in the drop in core temperature, pressure, and pressurizer level (Figs. 6.19-6.21), although most of the variation is the nominal result of reactor trip.

In the fifth overfeed case, the MFW valve to SG-A was postulated to fail in place when the reactor and turbine tripped. Principal results were similar to the third case, in which the valve failed full open without failure of the isolation valve. In 95 s SG-A filled to 45 in. on the narrow-range scale. (Readings immediately following reactor/turbine trip appeared to be distorted by disturbances in FW and steam flows and hence in pressure differentials.) The SG-B water level dropped to the low-low (wide-range) level trip 45 s after onset of the transient, and feed isolation valves closed 60 s later and terminated the overfill (Fig. 6.22). Temperature and other variations on the primary side (Fig. 6.23) were similar to those of the third case.

When the previous case was repeated with the MFW isolation valve A failed open, the feedpumps tripped in 1.7 min on high pump outlet pressure and terminated the overfill at 45 in. before any water could be injected into the steam line.

The preceding two cases, which tripped FW isolation valve B on low-low SG level, were repeated after the recent Calvert Cliffs-1 design change in which the FW isolation valves no longer actuate on low-low level. In the rerun of failure of MFW valve A full open in 1.5 s, the results did not differ significantly from those with isolation valve closure on

low-low level. SG-A filled in 4.5 min after onset of the transient and 2.4 min after the reactor tripped on high SG water level (Fig. 6.24). Minor cooling of the primary occurred (Figs. 6.25-6.27).

In the second of the reruns, MFW valve A failed in place on reactor trip. SG-A filled and began spilling liquid water into the steam line 3 min after onset of the transient (Fig. 6.28), sooner than in the preceding case, because in the earlier one the reactor did not trip until SG high level was reached (Figs. 6.29-6.31). Minor cooling of the primary occurred.

In the original and rerun cases of MFW valve A failure, MFW valve B closed on reactor trip. The feedpump runback rate was such that pump outlet pressure increased significantly. When main valve A failed full open, with or without isolation valve B closure, feed flow was always sufficient to hold pump outlet pressure below high-pressure trip. When main valve A failed in place, the high-pressure trip was exceeded if isolation valve B further restricted flow by blocking the bypass valve. Feedwater recirculation was included in the calculations but in some cases was not sufficient to prevent high-pressure trip.

6.1.4.2 Dryout Transients. In the first dryout study the SG-A steam flow reading was failed low at 1110 lb/s. As in the overfeed event in which the steam flow reading was failed high, the resulting water level error nullified the flow error after ~1 min. FW flow decreased ~10% and then returned to near nominal (Fig. 6.32). Effects on the primary were negligible.

In the second dryout case, the SG-A narrow-range (operating scale) water level reading was failed high at 10 in. above set point. Reactor trip on low level, also read on the narrow-range scale, was defeated. The SG inventory depleted until the low-low level set point, read on the wide-range scale, was reached in 3.7 min, at which time the AFW was activated, and then the reactor tripped. Pressures and temperatures on the primary side experienced only minor variations during the partial dryout.

The third dryout study postulated failures of the second case plus the following: since the AFW system is turned on when the low-low level limit is reached, this case assumed in addition that the low-low level reading failed 10 in. above set point. With this combination of failures, SG-A level depleted ~335 in. during the first 10 min of the transient and then stabilized (Fig. 6.33), largely because of the low gain of the FW valve controller. The valve initially closed sharply from 82 to 71% open in response to the proportional part (Figs. 6.34 and 6.35). The integral is small (0.1 repeat per min), and subsequent closure was so slow that after 12 min the opening decreased only to 60%. Pressurizer pressure stabilized at 2285 psia (Fig. 6.36), average core temperature at 578°F (Fig. 6.37), and power at 91% (Fig. 6.38). Simple extrapolation of the results suggests that further significant depletion of the SG will be long term, requiring perhaps an hour.

The fourth dryout case postulated that the SG-A MFW valve failed closed in ~5 s (Fig. 6.39); valve leakage was assumed negligible. SG-A water level decreased to the low-level set point 22 s later (Figs. 6.40 and 6.41) and tripped the reactor (Fig. 6.42). In another 24 s, the low-low level trip (wide-range scale) was reached and AFW was started (Fig. 6.39). During the following 2 min, system variables stabilized (Figs. 6.43-6.46). The principal effect of the postulated FW valve failure appears to be the greater initial rate of inventory depletion in SG-A. Following reactor trip (which would normally close the FW valve) and then emergency feedwater (EFW) trip, transient parameters appeared to converge toward typical trip conditions.

6.1.4.3 Primary-Side Depressurization Transients. In the first depressurization study, both PORVs were postulated to fail open. This corresponds to a small break of 0.015 ft^2. In the first 1.5 min of the transient, the primary side depressurized to 1070 psia (Fig. 6.47). The reactor (Fig. 6.48) and the HPI system tripped at their respective set points (1875 and 1740 psia). Following the initial rapid depressurization, the pressurizer went solid (Fig. 6.49), and loss of inventory became balanced by makeup/HPI at 7 min. Primary pressure stabilized at ~700 psia. A steam bubble formed in the header above the core, and partial voiding occurred in the collectors and the hot legs. The saturated fluid was subcooled in the SG. Voiding of the core did not occur. At the end of 7 min the system appeared to have stabilized in this configuration (Figs. 6.50 and 6.51).

In the second depressurization study, one PORV was postulated to fail open. The primary depressurized less rapidly, as expected, but ~3 min into the transient, pressure decreased below the high-pressure pump deadhead and injection began to counter the leak (Fig. 6.52). The pressurizer went solid in 5 min (Fig. 6.53) and average reactor coolant temperature slowly dropped to 520°F (Fig. 6.54). Voiding of the upper head occurred (Fig. 6.55). During the 2 min before the pressurizer went solid, there was voiding of a few percent in the hot leg of loop B and in the control rod shroud region above the core. When the pressurizer went solid and pressure leveled off with temperature still declining slowly, the hot-leg and shroud voids collapsed. The system appeared stable, and no voiding of the core occurred.

In the third depressurization case, a small break of 0.0015 ft^2 was introduced in the hot leg of loop A. This corresponded to a leak one order of magnitude smaller than the two-PORV failure. The leak was larger than the makeup system could compensate but sufficiently small that pressure did not drop promptly to the high pressure injection point. Primary pressure (Fig. 6.56) and inventory (Fig. 6.57) declined gradually for 20.5 min until pressurizer low water level tripped the heaters. The rate of pressure decreased, then approximately doubled. Temperature variations were minor (Fig. 6.58). After 30.5 min the reactor tripped on low pressure at 1875 psig (Fig. 6.59). The pressurizer water level was 2.2 ft and dropped to 4 in. on reactor trip. Primary pressure rapidly fell below the 1275-psig HPI deadhead, and net loss of inventory was terminated. Just prior to reactor trip, when the pressure was 1882 psia,

the leak, makeup, and HPI rates were 23.5, 13.4, and 0 lb/s, respectively. Shortly after reactor trip, when the pressure was 1184 psia, the rates were 16.1, 18.2, and 50.4 lb/s. The sharp depressurization on reactor trip caused a maximum voiding of 25% in the upper head (Fig. 6.60). No other voiding occurred in the vessel.

6.1.5 Conclusions

Overfill studies indicate that the postulated control failures will result in only minor variations in pressures and temperatures on the primary side.

In the case of failure high of the steam flow reading, the resulting error in SG water level appears to counteract the false flow signal and largely nullify the effects after small variations in feed flow.

When the SG water level reading fails low and induces overfill in combination with high level trip failure, the principal consequence appears to be the sizeable quantity of water injected into the steam line. Effects on the primary side were small. While the calculation predicts injection of water into the steam line, it does not predict the extent (if any) to which phase separation occurs and water accumulates and loads the pipe.

With the previous Calvert Cliffs-1 design (MFW isolation on low-low SG water level), failure of MFW valve A full open or failure in place on reactor trip filled SG-A to the 45- to 72-in. range, at which point the overfill was terminated when low-low level in SG-B tripped the FW isolation valves. No water was injected into the steam line. Primary side variations were largely the consequence of reactor trip rather than the modest overfill. In order to completely fill the SG, it was necessary to further postulate failure of FW isolation valve A in combination with main valve A failing full open. Then SG-A filled in 4.5 min, water was pumped into the steam line, and modest cooling of the primary occurred. When the main valve failed in place and the isolation valve failed open, the feed pumps tripped on high outlet pressure and terminated the overfill without water injection into the steam line.

With the recent design change at Calvert Cliffs-1 (isolation valves not actuated on low-low SG level), failure of the SG-A MFW valve either full open or in place on reactor trip resulted in filling SG-A and spilling water into the steam line in 3 to 4.5 min. Cooling of the primary was minor.

Failure high of the SG-A steam flow reading did not lead to dryout, because of the compensating error signal in the level measurement. When only the operating level reading and low level trip were failed, dryout was truncated by actuation of auxiliary feed at the low-low level set point on the wide-range scale. When both the wide- and narrow-range readings were failed, SG inventory depleted further but dryout did not occur during the first 12 min because of the small gain of the FW valve controller. The system stabilized, and indications were that total

dryout would be a significantly longer-range effect under the postulated failures. When mechanical or other failure caused MFW valve A to close in a few seconds, reactor trip on low level and EFW trip on low-low level occurred within a minute, truncating dryout and establishing conditions typical of trip.

Failure of both PORVs open depressurized the primary side to ~700 psia, at which point HPI equilibrated with the leak. Voiding occurred above but not in the core. Failure of one PORV open initiated HPI ~3 min into the transient, and primary pressure bottomed out near 950 psig. No voiding of the core occurred. The transient was essentially a milder version of the two-PORV-failure case. A leak an order of magnitude smaller in the hot leg (larger than the makeup could compensate but small enough to produce slow depressurization) caused the pressurizer water level to drop to 2.2 ft before the reactor tripped on low pressure after 30 min. The rapid drop in pressure on reactor trip initiated HPI and terminated net inventory loss. Minimum pressurizer water level was ~4 in., and some voiding occurred in the upper head. These depressurization calculations, simulating small-break LOCAs in the range 0.0015 to 0.015 ft^2, do not evidence a critical size break in which the primary inventory would deplete to the extent of core uncovery before actuating HPI.

6.2 MODULAR MODELING OF CALVERT CLIFFS

6.2.1 Simulator Description

The Modular Modeling System (MMS) simulation of Calvert Cliffs-1 was developed to serve as a backup for the RETRAN model. The original plan for simulator follow-up on FMEA-identified sequences was to use the BG&E training simulator. As it became evident that the training simulator would not be available in time to produce results that could be included in the SICS analysis, and since the estimates for modifying and running the RETRAN program supplied by BG&E had also indicated that the required simulation capability might not be available in time, the "B&W Enhanced MMS" package was acquired from B&W. Due to the quick setup and relatively efficient simulation features of MMS, it is also expected that MMS could be used to investigate the dynamic behavior of other PWRs with somewhat different designs in order to better evaluate the generic implication of some of the sequences identified.

MMS was originally developed by the Electric Power Research Institute (EPRI) and its subcontractors to supplement the capability of larger systems analysis codes such as RELAP and RETRAN. The key feature of MMS is its modularity, permitting the systems analyst to build a system simulation from a complete set of more than 60 independently developed, preprogrammed models of both nuclear and fossil power plant components. The user is often able to choose the level of complexity of the component model to be used, depending on the immediate needs of the simulation. For example, there are three versions of PWR core modules covering a wide range of complexity. There is also a pre- and

post-processor program (MMS-EASE+), operating on IBM or compatible personal computers, that greatly eases program setup via graphics displays and preset data input sheets. The primary areas of interest for MMS applications are scoping safety analyses for postulated accident sequences up to and including small-break LOCAs (but not large-break LOCAs), and analysis of upset transients considering the behavior of the plant control and safety systems. The B&W version of MMS applied here has been enhanced considerably in the past few years, and most of the MMS modules have undergone thorough checkout and verification against experimental data. The B&W Enhanced MMS is a preprocessor for the general-purpose dynamic simulation language ACSL.

The model of the primary system consists of a reactor core thermal hydraulics module with point neutron kinetics, and two reactor coolant loops. The two reactor coolant pumps in each loop are combined into one equivalent pump. The pressurizer and surge junction modules can represent nonequilibrium conditions, consider droplet rainout and bubble rise, and account for bidirectional flow from the primary loop. The modeling allows the pressurizer to either go full or dry out, and includes "input" connections for the spray line, electric heaters, and relief valves. The safety injection systems are also included. The models for each of the two UTSGs simulate the mass and energy dynamics in the primary (four regions) and the secondary (five regions, moving boundary), utilizing the drift flux formulation for void fraction in the secondary. The conservation-of-momentum equations are also solved for the downcomer to subcooled region flow and the flow leaving the separators. A similar MMS model has been verified against plant data from an ANO-2 turbine trip event, and correspondence between the data and the predictions was excellent. ANO-2 is a C-E plant similar to Calvert Cliffs-1.

The MFW train model uses the condenser sump as a boundary condition (keeping track of the inventory), continuing downstream with modules representing the plant heat dump, two stages of low-pressure condensate heaters (LPCHs), condensate booster pumps, two more stages of LPCHs, MFW pumps, one stage of high-pressure FW heaters, and two SG inlet lines, each with independent control and isolation valves.

The AFW system model uses water from the currently selected tank of three condensate storage tanks as its input boundary condition, keeping track of the integrated water flow to monitor the inventory in all of the tanks. The two turbine-driven and one motor-driven AFW pumps are modeled explicitly. Downstream of the pumps, the four associated control valves and cross-connect lines that enable flow sharing between the two SGs are included with their associated controls. Each of the two AFW lines feed in to the MFW lines via check valves.

The current version of the model of the main steam and steam bypass system assumes that the steam flow to the main turbines is constant until there is a turbine trip (i.e., the high- and low-pressure turbines are not yet modeled explicitly). This is because most of the transients currently considered to be of most interest do not require turbine plant

details (although these modules are available in MMS). For each of the two SG steam lines, the model includes the flow-restricting orifice and the atmospheric dump valve, the main steam isolation valves, and four banks of safety relief valves. The high-pressure turbine header combines these two lines and goes to the four turbine-governing valves (with their associated controllers) or dumps to a condenser via four turbine bypass valves. The models for the main steam piping (as well as all other piping) account for conservation of mass, energy, and momentum, and for variable steam properties.

Control systems currently in the MMS model include a level controller for each SG, a control system for the pressurizer, and various trips to shut down pumps. The level in the SG downcomer is controlled to a set-point value by modulating the FW control valve. The valve control signal uses an error signal of the downcomer level deviation from set point along with the difference between FW flow and steam flow. In addition, MFW pump speed is controlled to maintain a pressure difference of 105 psid across the control valves. A condensate pump trip occurs if the level in the condenser hot well is below a minimum value. Likewise, a low suction pressure trip is included for the condensate booster pumps, and a bypass valve is included to maintain a minimum flow through the pumps. A condensate level control valve is used to maintain level in the hot well. The pressurizer pressure control system model consists of a spray valve, a vent valve, heaters, and a blowdown valve. The spray and vent valves are activated by a high-pressure signal, and the heaters are activated by low pressure. The primary letdown valve is modulated to maintain a fixed level in the pressurizer since the makeup flow is constant. Reactor power is controlled manually by changing the concentration of boron in the primary coolant, and turbine steam flow is controlled manually by modulating the turbine-governing valves.

6.2.2 Simulator Results

Although successful implementation of the RETRAN model made MMS backup unnecessary, validating transients were planned for simulation on MMS. These consist of the several postulated scenarios for SG overfill. (The current modeling setup for Calvert Cliffs does not include two-phase primary conditions, so any future work on small-break LOCA scenarios would have to be done with a revised model.) Results of SICS transients were not available in time to be included in this report.

The current status of MMS simulation of the Calvert Cliffs-1 plant is (1) models of the primary system, MFW train, AFW train, main and turbine bypass steam systems, and associated control and safety systems have been developed and coded in the MMS/ACSL simulation language; (2) the primary system model is operational, and several sample transients have been executed; and (3) debugging of the other individual subsystem stand-alone models is continuing. Because the RETRAN approach became operational first, MMS results do not appear in this report.

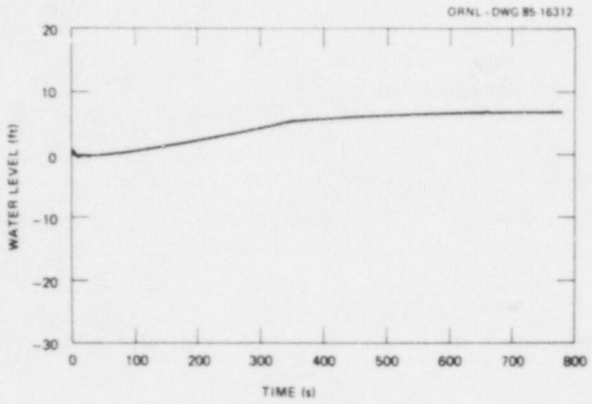

Fig. 6.3. SG-A water level with SG-A measured water level reading failed 10 in. below set point.

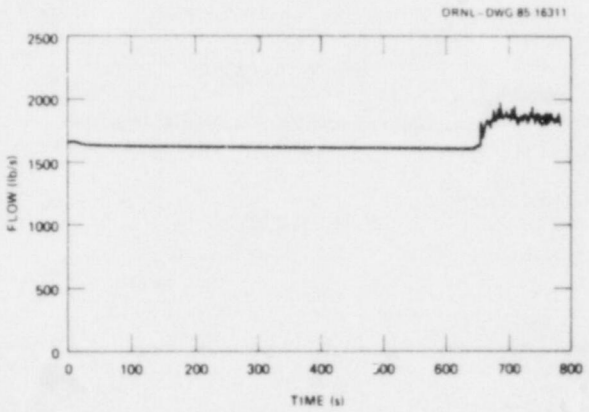

Fig. 6.4. SG-A steam flow with SG-A measured water level reading failed 10 in. below set point.

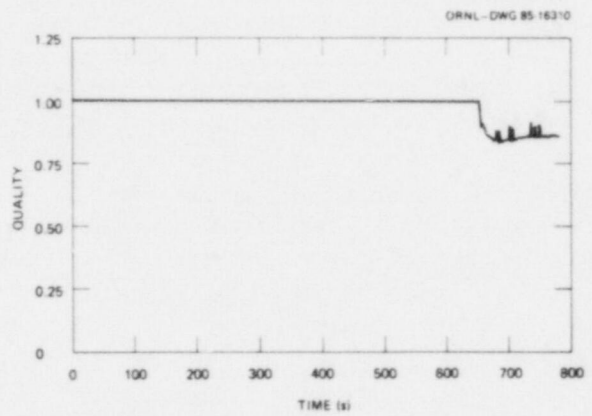

Fig. 6.5. SG-A outlet quality with SG-A measured water level reading failed 10 in. below set point.

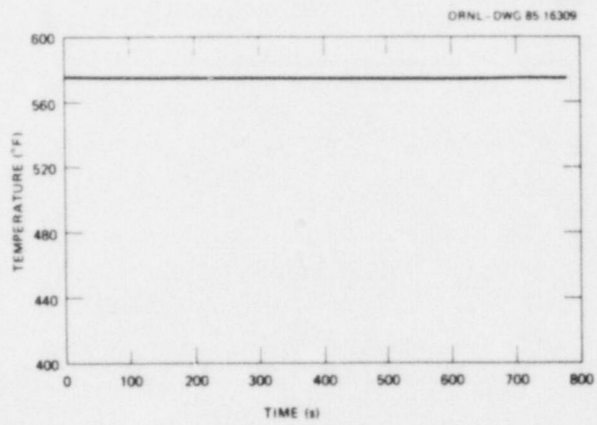

Fig. 6.6. Average core coolant temperature with SG-A measured water level reading failed 10 in. below set point.

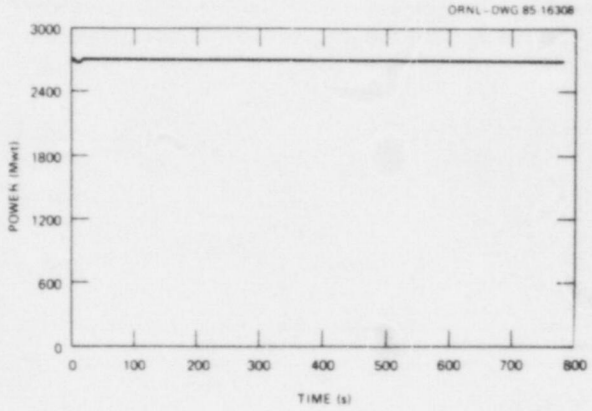

Fig. 6.7. Reactor power with SG-A measured water level reading failed 10 in. below set point.

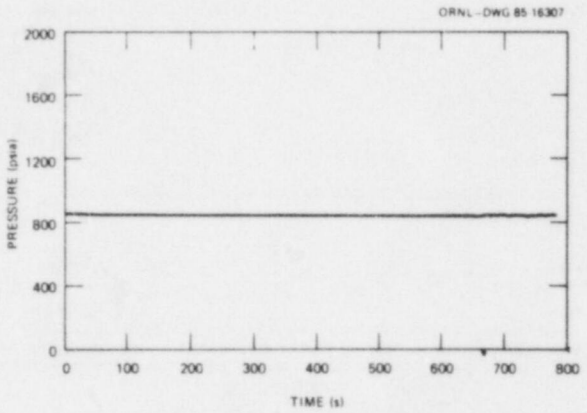

Fig. 6.8. Steam line A pressure with SG-A measured water level reading failed 10 in. below set point.

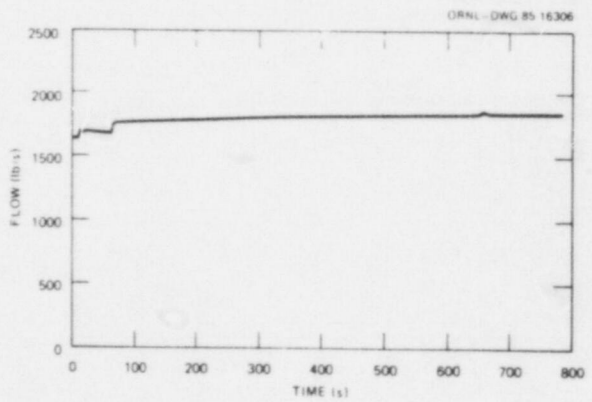

Fig. 6.9. SG-A FW flow with SG-A measured water level reading failed 10 in. below set point.

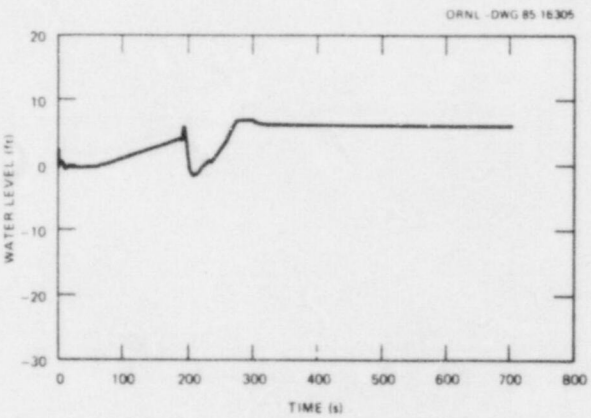

Fig. 6.10. SG-A water level with SG-A MFW valve failed full open in 1.5 s.

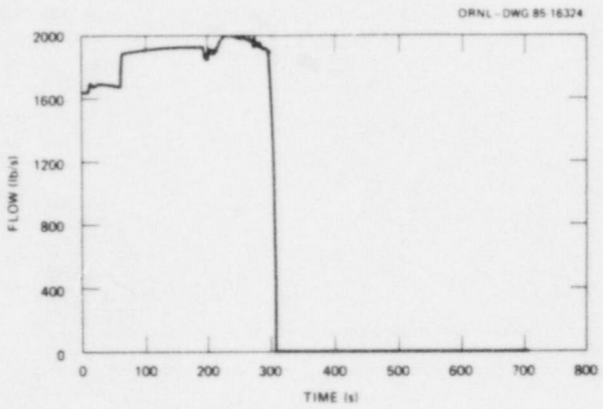

Fig. 6.11. SG-A FW flow with SG-A MFW valve failed full open in 1.5 s.

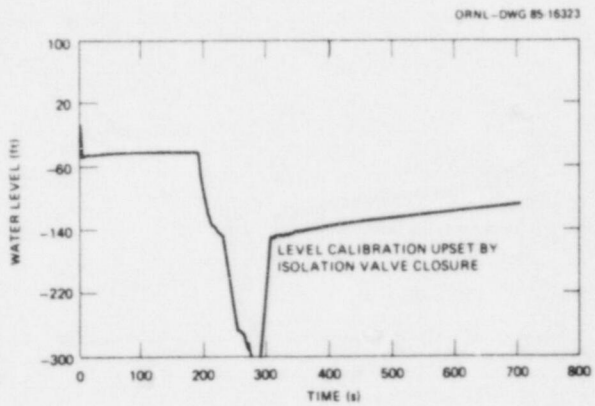

Fig. 6.12. SG-B wide-range water level with SG-A MFW valve failed full open in 1.5 s.

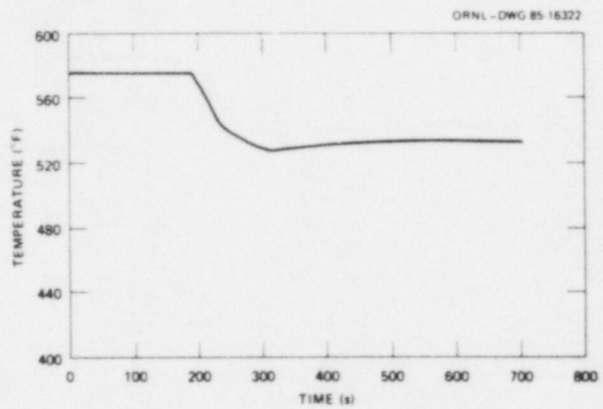

Fig. 6.13. Average core coolant temperature with SG-A MFW valve failed full open in 1.5 s.

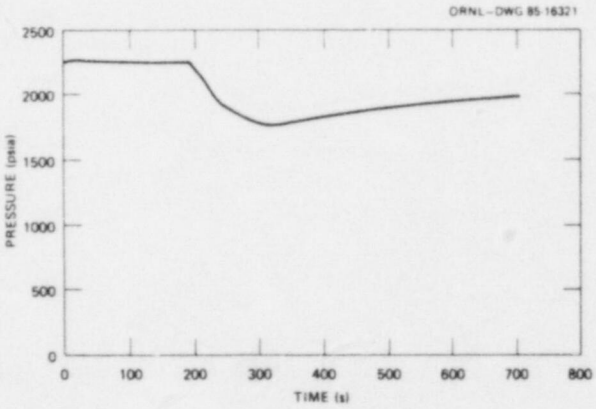

Fig. 6.14. Pressurizer pressure (psia) with SG-A MFW valve failed full open in 1.5 s.

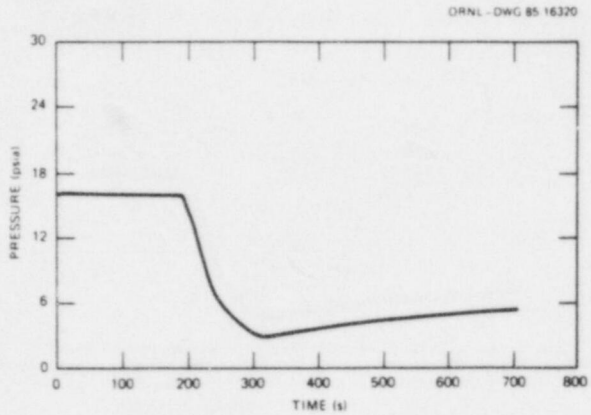

Fig. 6.15. Pressurizer water level with SG-A MFW valve failed full open in 1.5 s.

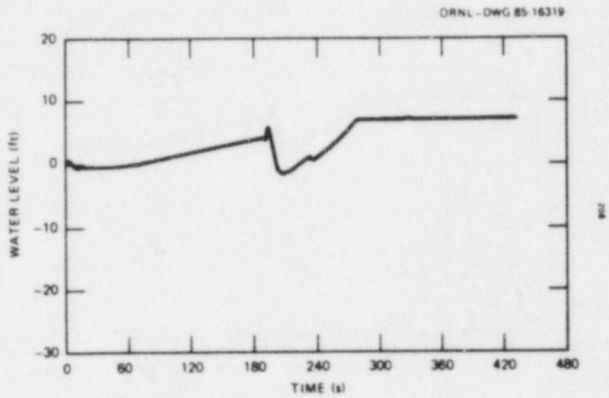

Fig. 6.16. SG-A water level with SG-A MFW failed open in 1.5 s; MFW isolation valve failed open.

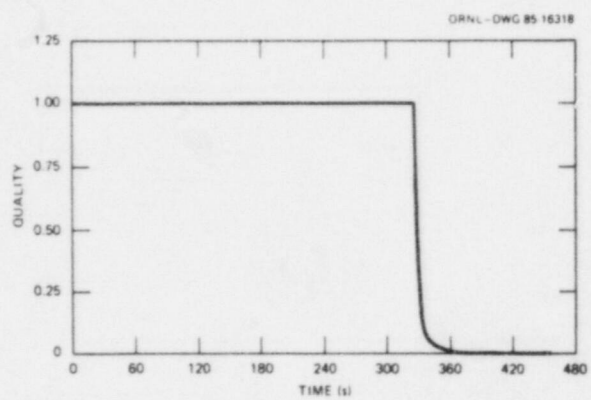

Fig. 6.17. SG-A outlet steam quality with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open.

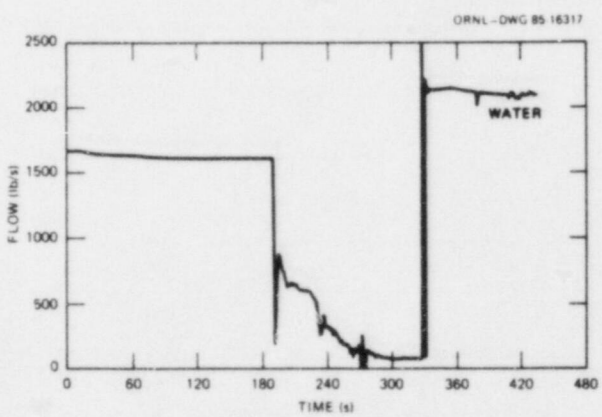

Fig. 6.18. SG-A exit steam flow with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open.

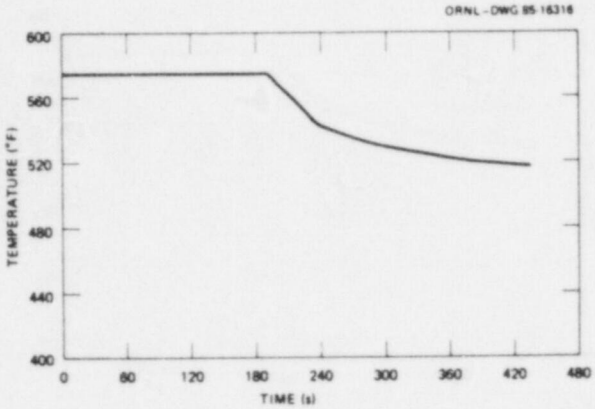

Fig. 6.19. Average core coolant temperature with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open.

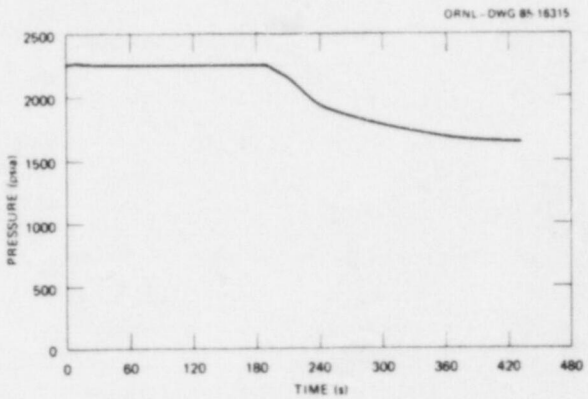

Fig. 6.20. Pressurizer pressure with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open.

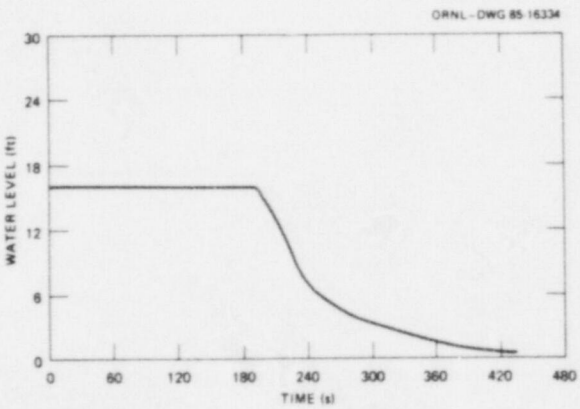

Fig. 6.21. Pressurizer water level with SG-A MFW valve failed open in 1.5 s and MFW isolation valve failed open.

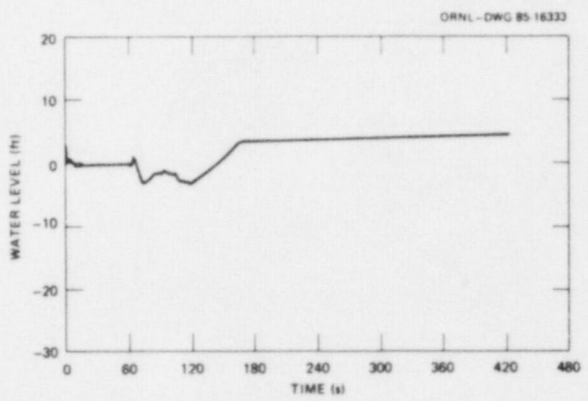

Fig. 6.22. SG-A water level with SG-A MFW valve frozen in place on reactor/turbine trip.

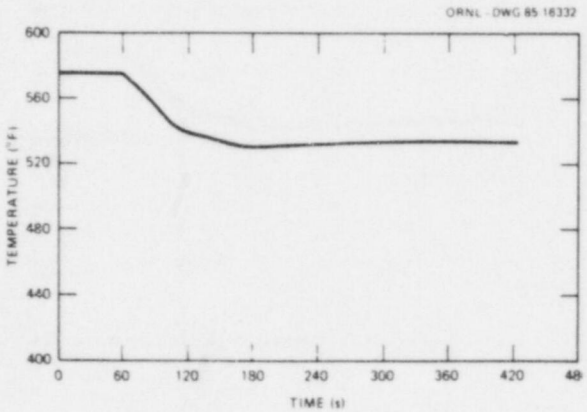

Fig. 6.23. Average core coolant temperature with SG-A MFW valve frozen in place on reactor/turbine trip.

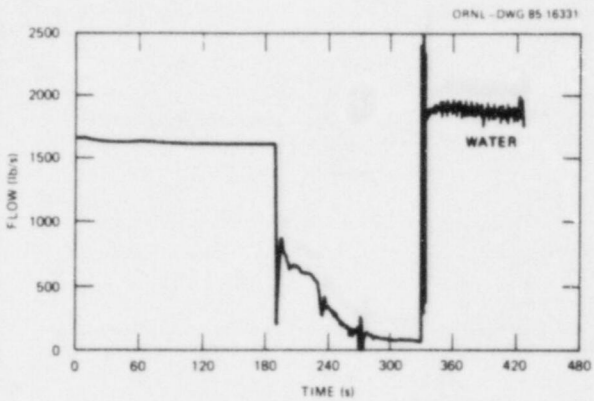

Fig. 6.24. SG-A exit steam flow with SG-A MFW valve failed full open in 1.5 s (run repeated after recent Calvert Cliffs-1 design change).

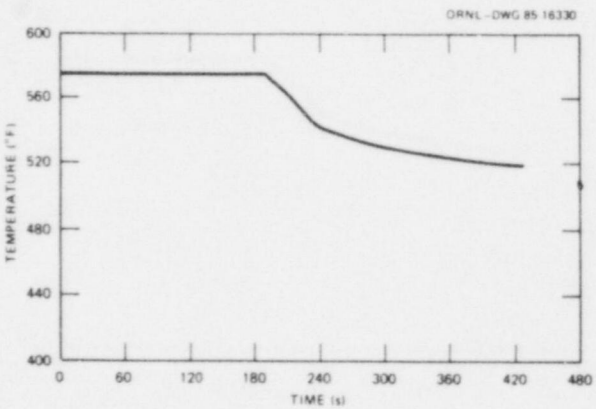

Fig. 6.25. Average core coolant temperature with SG-A MFW valve failed full open in 1.5 s (run repeated after recent Calvert Cliffs-1 design change).

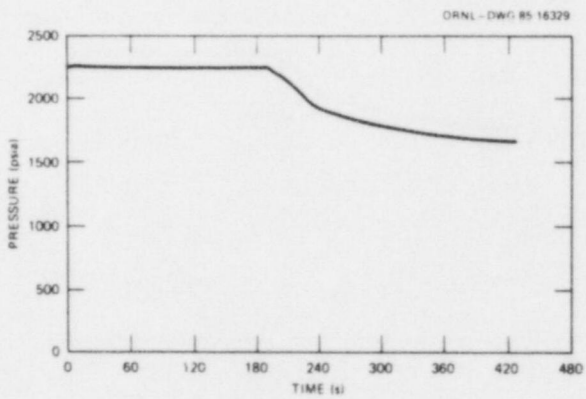

Fig. 6.26. Pressurizer pressure with SG-A MFW valve failed full open in 1.5 s (run repeated after recent Calvert Cliffs-1 design change).

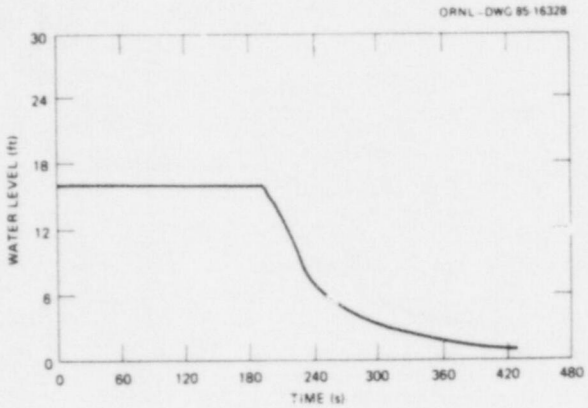

Fig. 6.27. Pressurizer water level with SG-A MFW valve failed full open in 1.5 s (run repeated after recent Calvert Cliffs-1 design change).

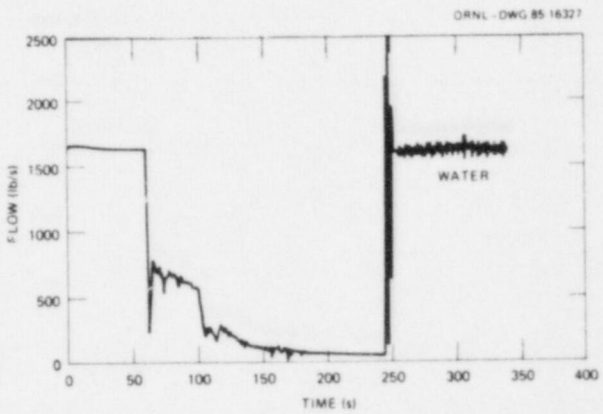

Fig. 6.28. SG-A exit steam flow with SG-A MFW valve failed in place on reactor trip (run repeated after recent Calvert Cliffs-1 design change).

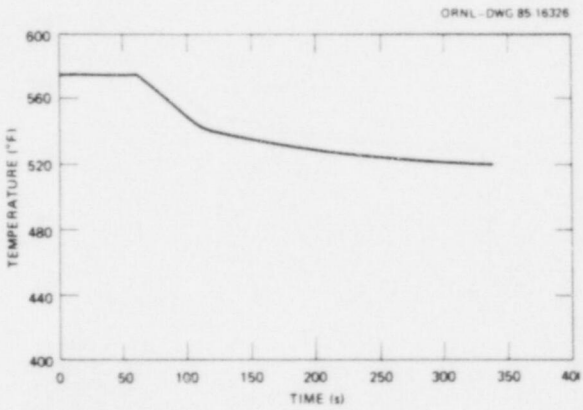

Fig. 6.29. Average core coolant temperature with SG-A MFW valve failed in place on reactor trip (run repeated after recent Calvert Cliffs-1 design change).

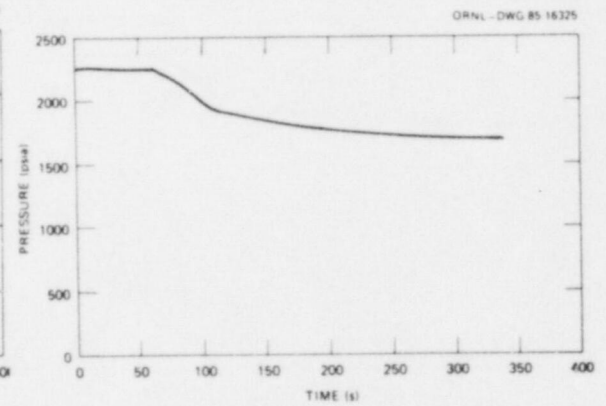

Fig. 6.30. Pressurizer pressure with SG-A MFW valve failed in place on reactor trip (run repeated after recent Calvert Cliffs-1 design change).

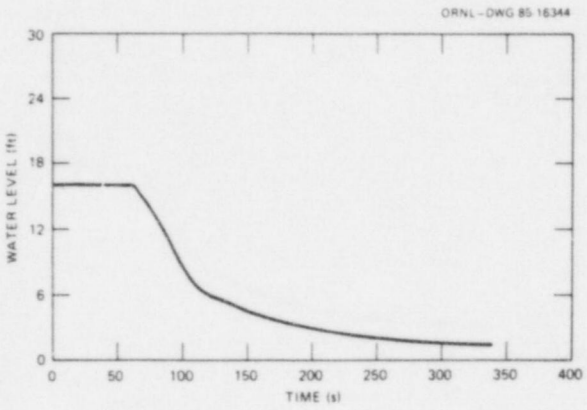

Fig. 6.31. Pressurizer water level with SG-A MFW valve failed in place on reactor trip (run repeated after recent Calvert Cliffs-1 design change).

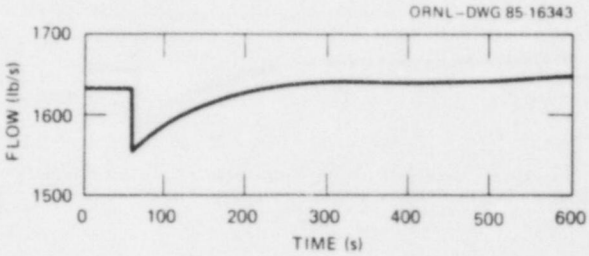

Fig. 6.32. SG-A FW flow with SG-A steam flow reading failed low at 1110 lb/s.

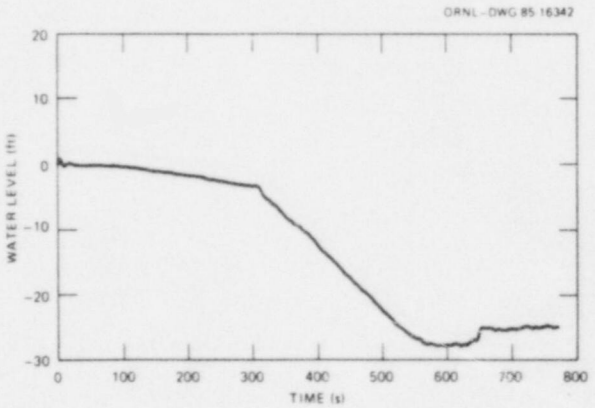

Fig. 6.33. SG-A measured water level with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

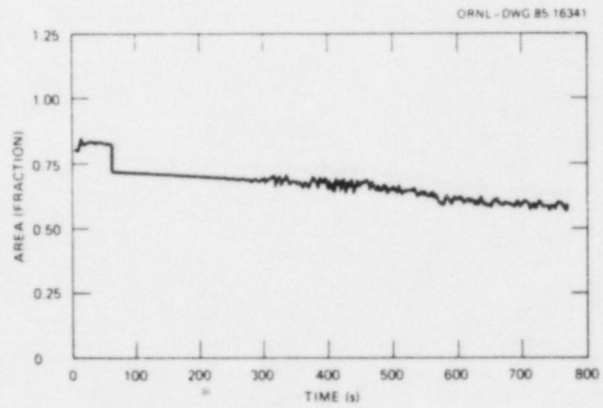

Fig. 6.34. MFW valve A area with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

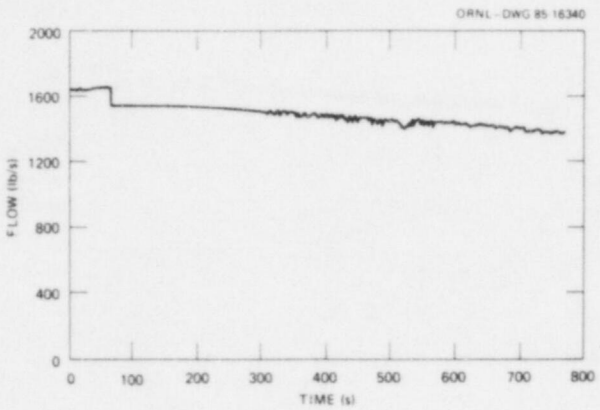

Fig. 6.35. SG-A FW flow with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

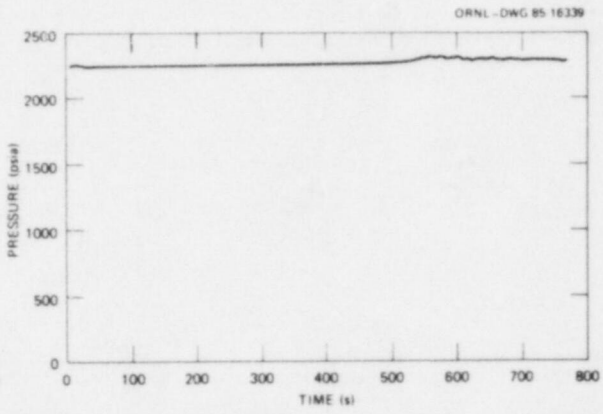

Fig. 6.36. Pressurizer pressure with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

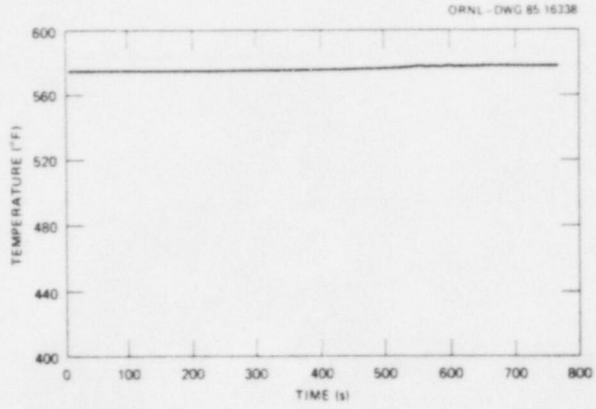

Fig. 6.37. Average core coolant temperature with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

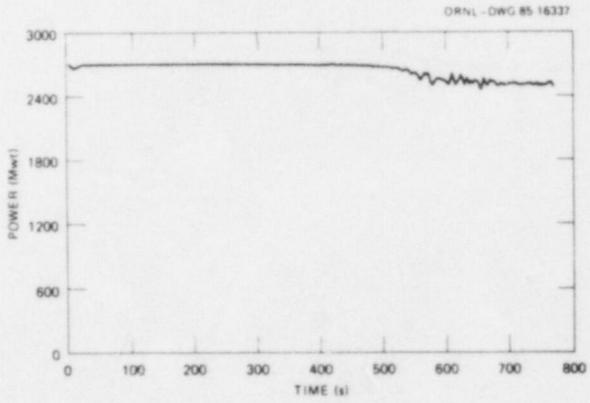

Fig. 6.38. Reactor power with SG-A measured level failed 10 in. above set point and low and low-low level trips failed.

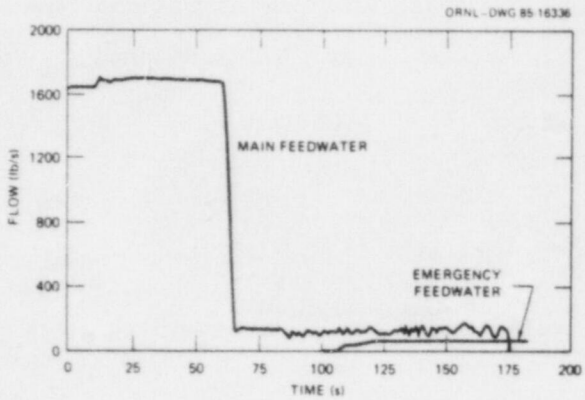

Fig. 6.39. SG-A FW flow with MFW valve A failed closed in 5 s.

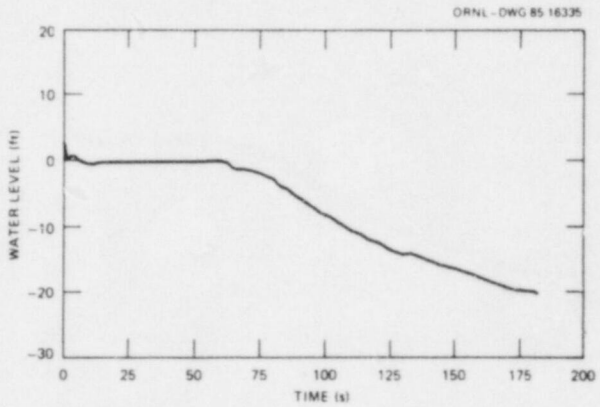

Fig. 6.40. SG-A water level (narrow range) with MFW valve A failed closed in 5 s.

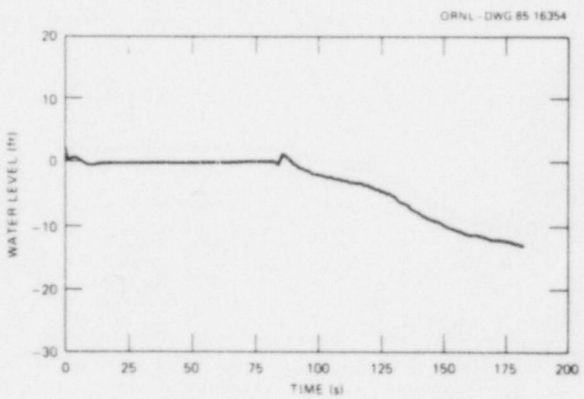

Fig. 6.41. SG-B water level (narrow range) with MFW valve A failed closed in 5 s.

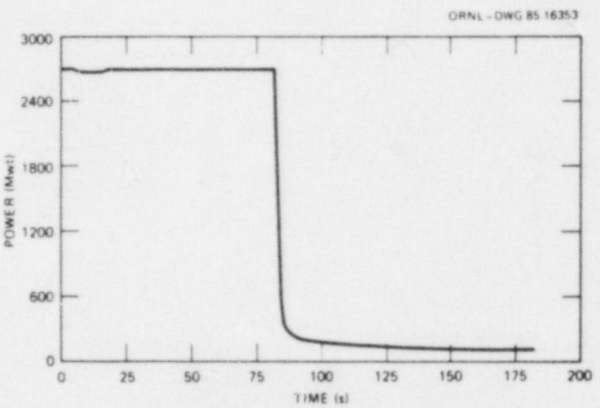

Fig. 6.42. Reactor power with MFW valve A failed closed in 5 s.

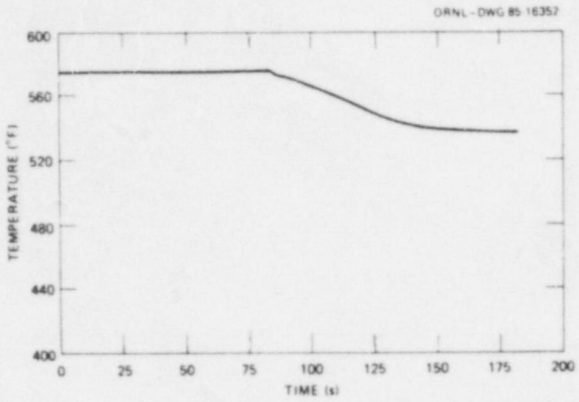

Fig. 6.43. Average core coolant temperature with MFW valve A failed closed in 5 s.

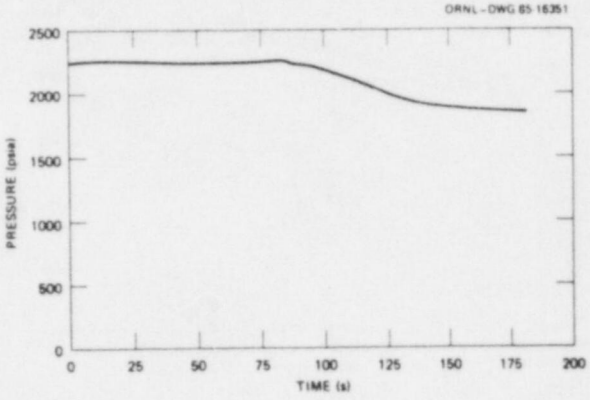

Fig. 6.44. Pressurizer pressure with MFW valve A failed closed in 5 s.

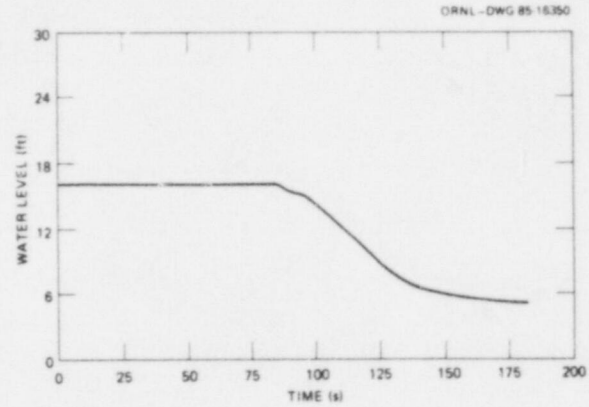

Fig. 6.45. Pressurizer water level with MFW valve A failed closed in 5 s.

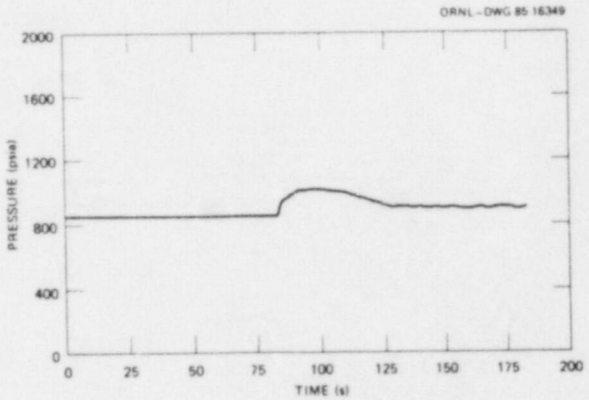

Fig. 6.46. SG-A steam pressure with MFW valve A failed closed in 5 s.

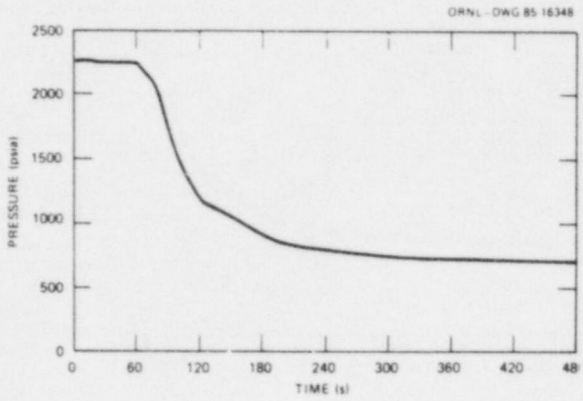

Fig. 6.47. Pressurizer pressure with both PORVs failed open.

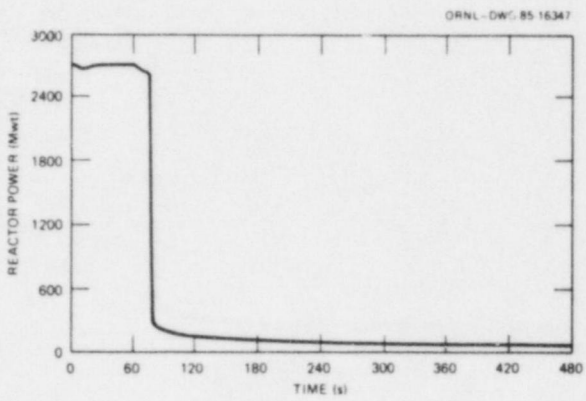

Fig. 6.48. Reactor power with both PORVs failed open.

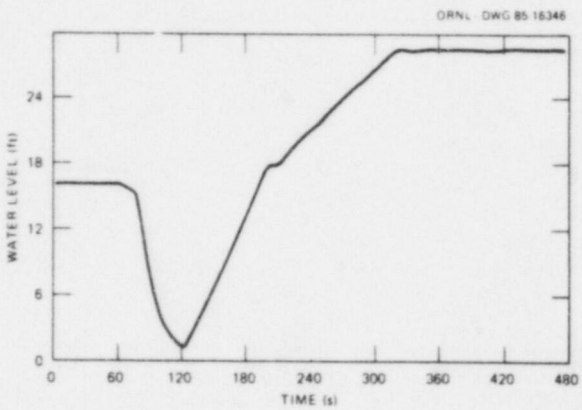

Fig. 6.49. Pressurizer water level with both PORVs failed open.

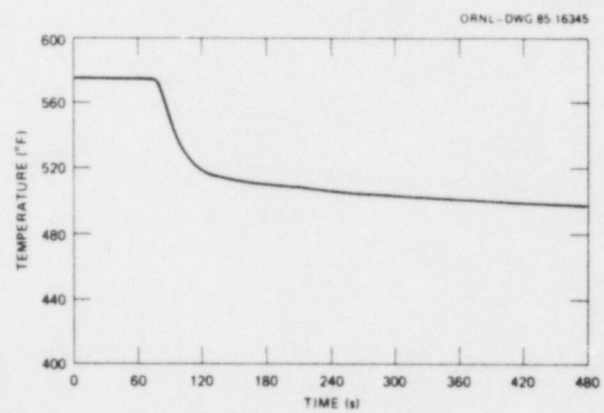

Fig. 6.50. Average core coolant temperature with both PORVs failed open.

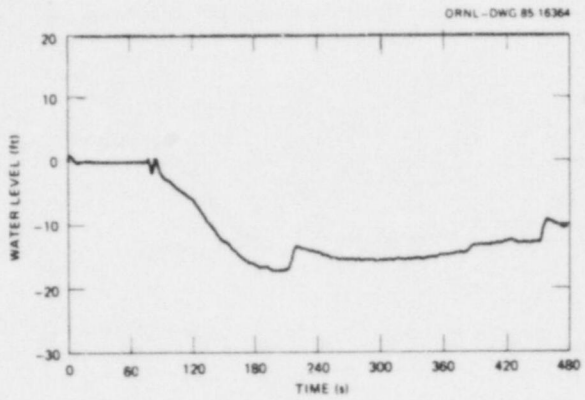

Fig. 6.51. SG-A water level with both PORVs failed open.

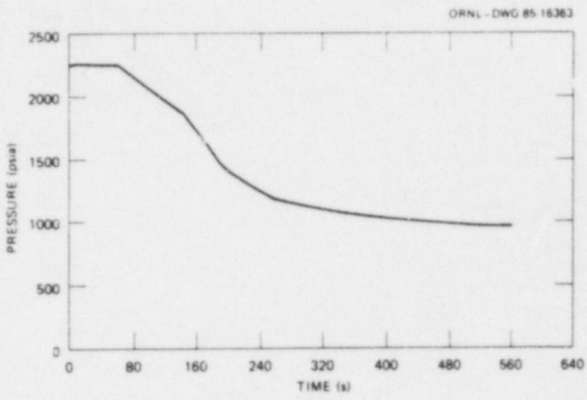

Fig. 6.52. Pressurizer pressure with one PORV failed open.

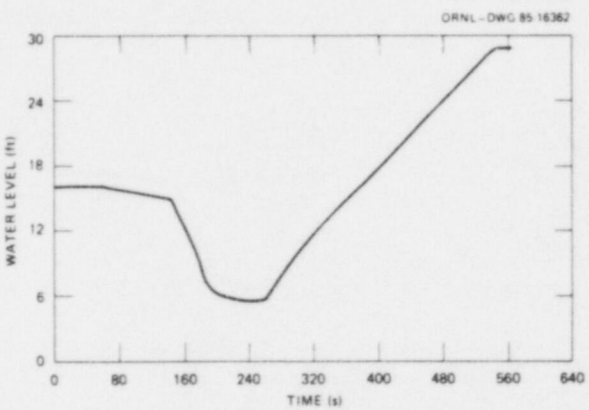

Fig. 6.53. Pressurizer water level with one PORV failed open.

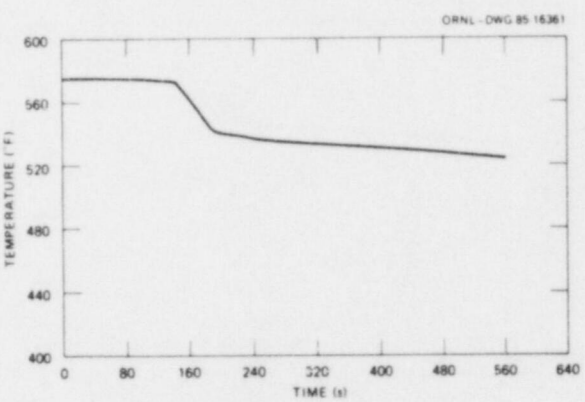

Fig. 6.54. Average core coolant temperature with one PORV failed open.

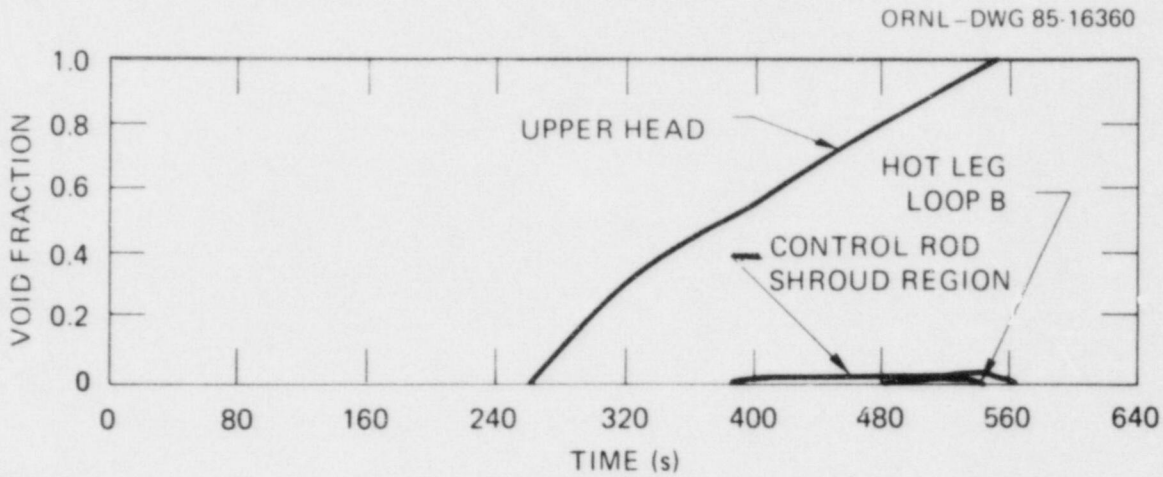

Fig. 6.55. Steam volume fraction with one PORV failed open.

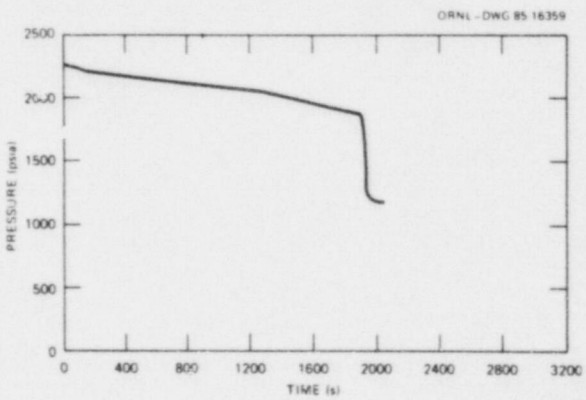

Fig. 6.56. Pressurizer pressure with small break (0.0015 ft^2) in loop A hot leg.

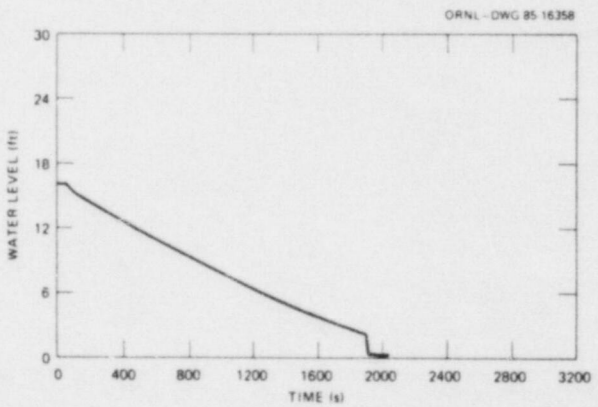

Fig. 6.57. Pressurizer water level with small break (0.0015 ft^2) in loop A hot leg.

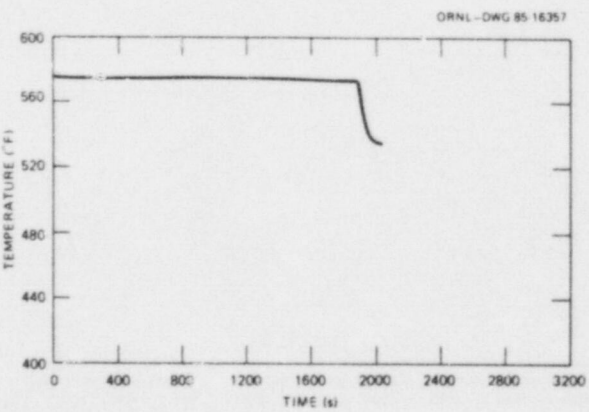

Fig. 6.58. Average core coolant temperature with small break (0.0015 ft^2) in loop A hot leg.

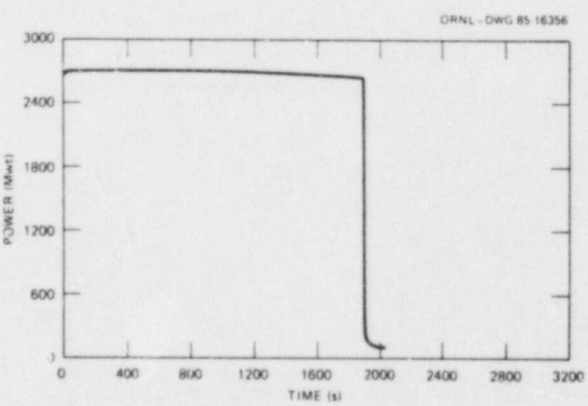

Fig. 6.59. Reactor power with small break (0.0015 ft^2) in loop A hot leg.

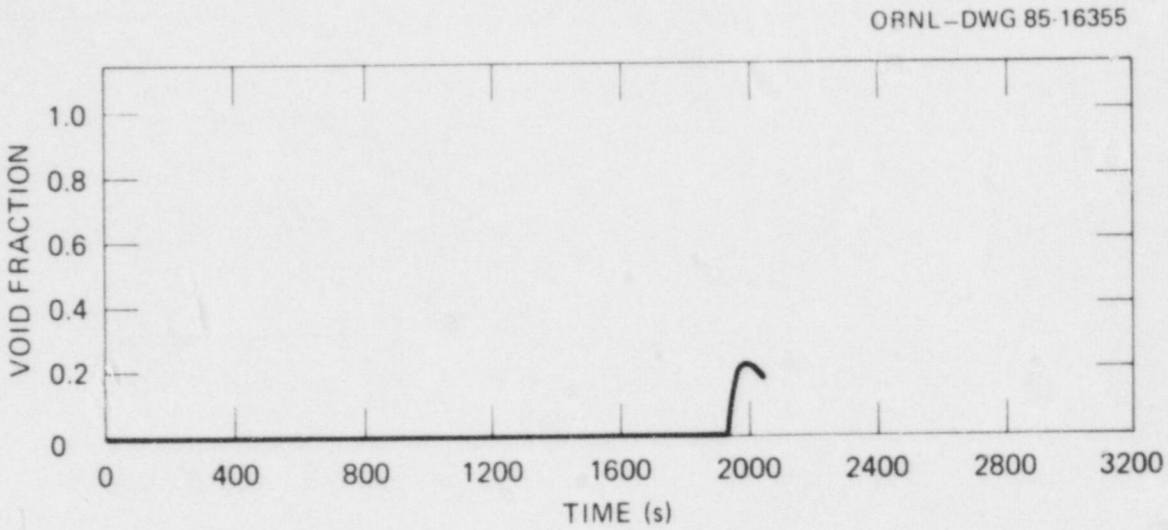

Fig. 6.60. Voiding in vessel upper head with small break (0.0015 ft^2) in loop A hot leg.

7. RESULTS AND CONCLUSIONS

The major activity reported here is the FMEA study in which all plant systems designated as being pertinent to SICS were systematically screened. By means of FMEA techniques, the potentially significant scenarios were identified. A summary of the most significant SICS accident sequences is given in Sect. 4.3. Augmented FMEAs--the thermal hydraulic analysis simulations that provide more details of the scenarios of particular interest--were run for several of these cases and are reported in Sect. 6.

Several control system failures were identified that lead to sequences worth pursuing. Of these, two types of postulated accident sequences were found to be potentially significant, and several others should at least be noted.

The first major type of sequence of concern deals with SG overfill, with two scenarios being of particular interest. In the first, it is assumed that a MFW control valve fails to the fully open position while the reactor is at power, and the excess feed rate causes the level in that SG to rise (the rate of rise depending on the excess feed rate available). Typically, more excess feed rate is available at lower powers. There would normally be an annunciator alarm when the downcomer level signal reaches 20 in. above the set point and, with no subsequent operator intervention, a turbine and reactor trip when the level reaches 50 in. above the set point. Upon turbine trip, normally the trip set controller runs back MFW flows to 5%, corresponding to approximately the initial steaming rate expected due to afterheat following 100% power operation. An additional control interlock, which grounds the MFW flow valve controllers' outputs on high level trip signal, would reduce FW flow even if the trip set controller failed. Except for the necessary trim control to match the feed flow to the steaming rate (either MFW via the bypass valve or AFW flow if MFW is not available), the overfill transient would be successfully terminated. However, if the MFW valve control failure is downstream of the controller, such as a failure in the current-to-pneumatic converter or a mechanical failure in the valve or its operator, the high MFW flow rate would continue, with the steaming rate corresponding to the afterheat rate. This much greater imbalance would result in a more rapid continuation of the overfill, which would then require prompt termination by the operator.

A second overfill scenario of more concern than the first assumes that the reactor is running at full power and is scrammed due to some problem unrelated to overfill malfunctions. If in this case a MFW valve stuck in its nearly full open position (i.e., it did not respond to the flow runback command), the overfill would proceed rapidly and would again need to be terminated by timely operator intervention. Depending on the details of the circumstances, the MFW pump may be tripped automatically on low suction pressure, or the SG may be isolated due to high differential pressure between SGs; however, with current plant designs and set points such automatic terminations cannot be assured. This

second scenario is of more interest than the first because (1) it involves only one possibly undetected failure (a stuck valve), and (2) the operator may be more likely to be distracted from acting on the overfeed problem by the alarms from the unrelated scram. It should be noted that a trip plus a stuck FW valve scenario did occur at Calvert Cliffs-2 in October 1983 (see Sect. 3.2.4.3) and was successfully terminated by prompt operator action.

The major concern about SG overfills is, of course, the injection of water into the steam line. There is concern for both the high-velocity and low-velocity injection scenarios. Especially in the high-velocity cases, the momentum transfer from the liquid to the steam line could induce motion of the steam line against its supports, which in turn might lead to failure of supports and possible deformation or collapse and rupture of the steam line itself. In the low-velocity case, the viscous shear forces are less likely to entrain the liquid and carry it out the end of the pipe, therefore allowing more liquid to collect in the lower portions of the lines. In either case, or in cases that fall in between, the amount of actual damage to the steam line and its associated valves is not readily predictable. The steam lines are designed to withstand seismic and deadweight loads but are not qualified to withstand severe dynamics loads due to waterhammer.

A follow-up sequence to the steam line failure that is also of concern is a SG tube rupture that may be precipitated by it. Such a tube rupture would provide a path for fission products in the primary system to be released outside the containment. In U-tube SGs such as Calvert Cliffs, however, the probability of a steam line break causing tube ruptures is generally considered to be lower than for once-through SGs.

The second major sequence of concern relates to very small-break LOCAs, which can be initiated either by pipe breaks or by control system malfunctions. The significance of this sequence, which is peculiar to this type of C-E plant, is based on the fact that the high pressure safety injection (HPSI) system pumps can deliver coolant at a head of no more than 1275 psi, and that consequently there may be situations in which the primary system pressure stays too high for the HPSI system to inject water. The normal plant makeup system can inject 132 gpm into the primary loop independent of system pressure because it employs positive displacement pumps. The FSAR analyses have indicated that equivalent break or leak sizes down to 0.1 ft^2 can be dealt with satisfactorily by the safety system. Our initial concern was that between a leak size corresponding to 132 gpm and a leak size of 0.1 ft^2, there may be a range of leak sizes large enough to reduce the primary system inventory significantly, yet too small for the system to depressurize rapidly enough from the normal operating pressure of 2250 psi for the HPSI to deliver an adequate flow rate. (The hole equivalent to a 132-gpm leak is 100 to 200 times smaller than the 0.1 ft^2 hole.) Reduction of primary inventory to the point where natural circulation cooling cannot be maintained would eliminate the option of further cooldown (and thus primary system depressurization) using the SGs. Without proper operator diagnosis and corrective action,

further reductions in inventory to the point at which the core is no longer covered with a two-phase mixture would lead to core damage. Subsequently, the results of the ORNL RETRAN analyses (Sect. 6.1) and a proprietary C-E study called to our attention by BG&E have indicated that this scenario is of much less concern. Both studies have analyzed a wide range of hole sizes, and in no case was core uncovery predicted. In the RETRAN calculations of the smaller postulated break size event (Sect. 6.1.6), a reactor trip on low primary pressure eventually reduced the pressure to the point where the HPSI system injected water into the primary system. The only remaining concern would be that a longer term (and thus lower probability) heatup following the trip would repressurize the system. If a critical range of hole sizes does in fact exist, it represents only a small portion of the credible range of leaks. The probability of occurrence is therefore small, thus significantly reducing the probability of core damage. Another mitigating factor is the long time (up to an hour or more) available to the operators to diagnose and correct the problem. However, it is our opinion that the current emergency operating procedures for LOCAs do not adequately cover this situation.

The FMEAs uncovered two other areas which are of less concern but which we felt should still be noted:

1. A turbine trip signal is generated by two-out-of-four SG high level signals. The logic diagram shows that the two-out-of-four logic condition funnels ultimately into a single equivalent OR "gate" whose failure could defeat the trip on this parameter. (The OR gate actually consists of multiple independent components, but it drives a single relay.) It is possible, however, that such an overfill would have other dynamic consequences that would lead to a turbine trip by another path; and

2. Apparently there are four valves in the component cooling water circuit, any one of whose failure closed would lead to a cutoff of cooling water to the reactor coolant pump seals. Such a condition, prolonged for several minutes, could lead to seal failures and in turn lead to an event that might be classified as a small-break LOCA. However, such an event is bounded by small-break LOCAs in the FSAR. Its possible special significance is that it is a single failure event.

Another event of interest that does not involve a component or system failure is detailed in Sect. 5.2.1. This scenario is rather complex, showing that following a LOCA automatic isolation of the service water system may result in subsequent failure of the instrument air and containment air supplies.

Other possible failures detailed in Sect. 4 might lead to a small-break LOCA, but all of them are bounded by cases presented in the FSAR.

In all of these postulated failures, proper operator intervention could end the transient or successfully mitigate its effects. In all of the

cases noted in C-E plant operating histories, in fact, proper operator action terminated the events successfully. However, it is our opinion that the emergency procedures currently in use at Calvert Cliffs could be improved substantially and thus help reduce the chances of a precursor turning into an accident. BG&E is currently upgrading their EOPs, and the newer versions are scheduled to be in effect at the beginning of 1986.

The results of the augmented FMEAs--simulator analyses of broad FMEA-developed sequences of particular interest--are reported in detail in Sect. 6. A RETRAN model derived in large part from a BG&E version for the Calvert Cliffs-1 plant was used to study postulated SG overfill and dryout sequences and several small-break LOCA scenarios. A Modular Modeling System (MMS) simulation of Calvert Cliffs-1 was developed for use as a backup to the RETRAN model, but was not needed since the RETRAN model was implemented successfully.

Probability estimates for the major sequence frequencies are developed and presented in Sect. 5. For the critically sized small-break LOCA to lead to probable core damage due to insufficient cooling, the estimate is less than one event in 100,000 reactor years. The probability for a rapid SG overfill, resulting in liquid entering the steam lines, is estimated to be ~1/100 ry.

Major FMEA studies were performed on plant electrical and instrument air systems. Because failures in these systems can affect large numbers of instruments and control systems, electrical and pneumatic reliability and availability are crucial to SICS concerns. The significant conclusions from these studies are that the plant design contains sufficient built-in backups so that failures in plant electrical and air systems are not expected to prevent the operators from bringing the plant to a safe shutdown condition. Although some postulated instrument failures led to leaks causing loss of all instrument air, many affected areas could be isolated by proper operator action and air supply to the rest of the system restored. The potential for some improvements in the operating procedures for accomplishing the recoveries was noted. Of special interest here is the time available for resolution of the problems. Only in the case of some postulated header breaks was the problem such that the leak could not be isolated.

A study was also made of plant operating experiences relevant to SICS (Sect. 3.2) for two purposes. First, such a study may uncover or suggest sequences of interest not detected by the broad FMEA or simulator exercises. Second, some rough idea of the probabilities of the major sequences may be derived from the rate at which such control system malfunction events occurred, thus leading at least to sequence precursors or initiating events if not to serious events themselves. The current review and analysis centered on Calvert Cliffs-1 but also derived data from Unit 2 and other operating C-E sister plants. The operating history at Calvert Cliffs is similar to that at other PWR plant sites (except for those that have experienced serious problems). Of the two types of events noted as being of significant concern, none

at Calvert Cliffs could be classified as small-break LOCAs, but one at another C-E plant could be. There were 3 SG overfeeds at Calvert Cliffs that resulted in high level trips as well as 11 cases of SG low-level trips (mostly during startup). Although no serious problems resulted from the low-level trips, they were potential challenges to the AFW system and, as such, could be considered as precursors to dryout or overheating events. A rough idea of the frequencies involved may be derived from noting that these are approximately the total of such events (depending on the completeness of the reporting systems) that occurred in 19 plant years of Calvert Cliffs operation, or 88 plant years of operation for all C-E plants. Analysis of the sum total of events for all C-E plants (and for U.S. power reactors in general) has shown that those related to maintenance and testing deficiencies resulted in frequent challenges to the plant protection systems (PPSs). Improvements in these procedures and systems, and improvements in the man-machine interface and communications systems (particularly in plants where much of the control is manual), would also reduce PPS challenges.

Other discussions of conclusions and recommendations are given in the sections on generic implications (Sect. 4.7), resolution of A-47 (Sect. 8), and possible future SICS-related work (Sect. 9). Another conclusion is that more investigations are required to resolve the question of generic applicability. The consensus at a 1983 ANS conference on anticipated and abnormal transients was that while most utilities/operators generally feel that identifying, solving, and discussing operational problems at their own plants would be of use to operators at sister plants, most of the major contributors to these problems are functions of detailed design and operating procedures, and hence generic solutions are unlikely to be universally applicable.

Because of the interest in very low probability events (0.0001 per plant year and less), more work would be appropriate on common cause-induced failures from external events such as earthquakes, floods, and EMP tests. It also is noted, however, that historically most serious problems with reactors have not been caused by external events or fires, but by design errors, instrumentation failures, operator and maintenance errors, poor communications, mechanical equipment flaws, and on-line test procedure problems. As a result, U.S. reactors have had their shutdown and emergency systems challenged and exercised more often than they should (averaging 5.5 shutdowns per plant year compared to 0.3 in Japan). We believe that dealing with these problems should take precedence over eventualities that have historically proven to be of less concern.

8. RECOMMENDATIONS FOR RESOLUTION OF USI A-47

8.1 BACKGROUND

The A-47 Task Action Plan (April 1984)[8] states that the objective of the task is ". . . to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures."

Nonsafety-grade control systems having the potential for affecting plant safety are presently covered by a general statement in NRC's Quality Assurance Criteria, 10 CFR50,[30] Appendix B, Criterion II: "The quality assurance program shall provide control over activities affecting the quality of the identified structures, systems, and components, to an extent consistent with their importance to safety."

Under existing standards, nonsafety systems that present potential safety problems are dealt with in three recognized ways:

1. Make the nonsafety system in question a part of the safety system, transferring to it all requirements for redundant channels, testing, and design approvals that characterize any protective channel. As a result of this type of approach, power sources that were not part of the safety system in IEEE 603-1977[31] have been found so vital to safety functions that they have been included in the safety system in IEEE 603-1980.[32]

2. Upgrade or enlarge the safety system to deal with any new hazard that has been found to be associated with a particular control element, the latter remaining in the nonsafety category.

   Standard 603, IEEE Standard Criteria for Safety Systems, describes possible safety interactions of nonsafety systems (Sect. 6.3.1): "Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met . . . ."

   There follow two possible remedies, both involving the provision of equipment not subject to failure due to the original initiating event, and capable of detecting the event and limiting its consequences to levels permitted by the design bases. One remedy is an alternate (diverse) sense and command (S&C) channel to substitute for the S&C channel that failed. The other remedy provides safety equipment outside the S&C system which is capable of providing protection despite complete loss of S&C.

3. Upgrade the nonsafety system in question to make it less likely to fail, or decouple the elements it has in common with safety systems without promoting the system in question to full safety system status. (Upgrading is covered in principle by the cited quotation from 10 CFR50, Appendix B.)[30]

   Decoupling is largely covered by General Design Criterion 24 of 10 CFR50, Appendix A, which requires that "The protection system shall be separated from control systems to the extent that failure of any single control system or channel . . . leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired." There are possible needs for decoupling beyond the requirements of Criterion 24 (e.g., multiple control channel failures from a common cause, or interactions not caused by interconnection); these may be addressed under general standards of "applicability, adequacy, and sufficiency."

8.2 INSIGHTS FROM THE SICS STUDY OF CALVERT CLIFFS-1

Questions that must be answered before USI A-47 can be resolved include the following:

1. Have any control-initiated or control-exacerbated safety problems been found, either plant specific or generic, that exceed the bounds of design basis accidents or are otherwise unacceptable?

2. If so, are these problems the result of inadequate guidance in current or past licensing design requirements, or do they simply represent the failure of plant designers to follow existing regulations?

3. If there is a need for additional guidelines and criteria, what changes and additions are required?

The answer to the first of these questions is affirmative. The following conclusions can be made:

Section 4.3.2.5 discusses the causes and effects of an intermediate range of small-break LOCAs in the Calvert Cliffs plant. Coolant losses of this nature can be initiated by control system action, and the action of other nonsafety control systems may be required for their relief. Consequences of inaction or improper action could include damage to the core.

Section 4.3.2.7 discusses the causes and effects of SG overfill in the Calvert Cliffs plant. Such overfill is initiated by control system action and can be terminated only by the timely intervention of the operator via nonsafety control systems. Consequences of inaction or improper action can include potential steam line break.

Questions (2) and (3) investigate appropriate design or operational remedies for such safety problems as may be found, and ask whether the existing licensing design requirements, if followed, would have required the implementation of such remedies during construction.

In the case of small-break LOCAs, two RCS failures were identified as potential causes: a release of reactor coolant due to RC pump shaft seal failure, or a failure to close or isolate the PORVs mounted on the pressurizer. (A fully open PORV is well above the range of small-break LOCAs of possible concern, i.e., those which exceed makeup pump capacity but which might not depressurize the primary fast enough to allow the HPSI to function in a timely manner.) The HPSI system is automatically actuated in the event of a LOCA, but (as explained in Sect. 4.3.2.5) in order for it to supply water for certain small breaks, the operator must be depended upon to depressurize the primary system and the SG, in turn depending on the operability of the appropriate control systems.

Figure 4.3 shows that initial recovery from such a LOCA is dependent upon SG depressurization via the atmospheric dump valve and/or the turbine bypass valve, opening of the PORV, and possibly operation of the chemical volume control system (CVCS). Should this depressurization not take place, pressurizer heater cutoff will eventually lead to an accelerated rate of pressure drop followed by reactor trip on low pressure before the core is uncovered. However, unique and unmistakable instructions in the small-break LOCA EOPs should ensure that required HPSI operation is not even temporarily blocked by high RCS pressure.

The other case of concern, overfill of the SG, can occur through failure of FW control valves to close following reactor trip. Once the overfeed transient is initiated, it can be terminated only by operator action. Automatic pump trip on sustained, verified, and intractable high SG level with failure of runback would appear to be a reasonable provision.

In order to accommodate such control malfunctions as described above, are additional criteria or design guidelines required?

Appendix B of 10CFR50 is concerned with proper functioning of important nonsafety controls, but it seemingly confines itself to the construction quality of those systems.

IEEE Standard 603 (quoted in Sect. 8.1) is close to the mark, but requires the target nonsafety system to both cause the challenge to safety and prevent the safety system from functioning properly.

NRC might well consider a standard such as "where proper functioning of a nonsafety system is required in order that protection sense and command channels can perform their protective action in response to a condition requiring protective action, the functioning of that nonsafety system shall be assured by the same standards of performance as are required of the protective channel."

Because of differences in design philosophy, conditions of concern that were identified for Calvert Cliffs are generally not the same as those found in the Oconee plant. Other C-E plants may or may not have concerns similar to those discussed for Calvert Cliffs. The recommendations apply specifically to the plants examined but are qualitatively valid for other plants of similar design. Such generic evaluations can be made without examining every nuclear station in the country, but they may be irrelevant at any given plant because of individuality in controls design. These issues are discussed in more detail in Sect. 4.7.

The conditions found in Calvert Cliffs-1 are not unusual or a cause for alarm. Although the design conditions do not appear to violate any existing standards, in some instances the plant does depend on operators for actions that are essentially safety functions, and in the resolution of USI A-47, NRC may well wish to require automatic operation or unequivocal EOPs for nonsafety actions essential to safety.

9. RECOMMENDATIONS FOR FUTURE WORK

No additional new funding for the SICS program is anticipated in FY 1986 and thereafter; recommendations for future work therefore fall into two broad categories: (1) follow-up work that can be done using carryover funds, and (2) new projects funded as other research programs. In the first category, the same project personnel will be available to respond to the broader reviews of USI A-47 that follow issuance of this report and the companion SICS report on Oconee. Another task that may be appropriate here would be a refinement of the simulator models including augmented verification and validation of the models using calculations and/or plant data as available.

In the second category, we believe that a number of topics (not necessarily related to Calvert Cliffs or other C-E plants) deserve consideration for follow-up work:

1. The credibility and usefulness of the generic extension of the Calvert Cliffs work to other C-E plants would be greatly enhanced if several of these other plants were examined in more detail than was possible in the present program (Sect. 4.7). This should be done.

2. Look into operator action in more detail. In particular, consider for specific sequences the chances for misdiagnosis; the ability to cope with failed systems; and the adequacy of procedures, training, and drills. Make use of training simulators if available.

3. Investigate "reasonable" combinations of multiple failures to a great extent. Several significant nuclear power plant incidents have occurred that would not be predictable if it were assumed that the multiple failures that did occur were indeed independent, or even if the failures were due to a common cause. The most recent, at Davis Besse on June 9, 1985, involved multiple control and safety equipment and operator error problems. At least 10 component failures were classified as independent. A significant feature of the event is that in the preceding six months at Davis Besse, ten interruptions of MFW occurred. Furthermore, problems with control of the AFW pumps were also experienced intermittently in that period. Hence the MFW failures, which could be categorized as AFW (safety system) challenges, should be considered as warnings of an incident about to happen. It would be useful to systematically determine behavior patterns of problems and their frequencies that could be used to warn of impending accidents. In particular, problems with AFW actuation and control appear to deserve more attention.

4. Consider external effects (earthquake, fire, flood, and sabotage), per the current task action plan for A-47.

5. Consider other mechanisms for failure categorized by ORNL consultant E. P. Epler.[33] Epler has pointed out that, except for the Browns

Ferry BWR fire, none of the external effects noted in Item 3 have contributed to major failures. On the other hand, other mechanisms more likely to be overlooked have dominated the early reactor failures and continue to appear in LWRs. These topics, with examples, are as follows:

a. Design errors: The TMI-2 pressurizer PORV position indication was taken from the relay operating the valve, not from the valve itself.

b. Redundancy: A Brunswick service water pump's coupling was mistakenly uncoupled in the one remaining active element of a redundant train, resulting in loss of service water for 7 h.

c. Degraded ac power: Low offsite voltage at Millstone wasn't low enough to start the diesels, and the resulting failure of ac contactors to close caused a sustained inrush current and blew control circuit fuses.

d. Testing: The H. B. Robinson batteries were discharged due to an inadvertently prolonged test, which led to a scram, destruction of turbine bearings, and deactivation of half of the shutdown heat sink equipment.

Many of these categories involve the effects of nonsafety-grade equipment failures and deficiencies in operating and maintenance procedures; they may be viewed, in part, as follow-ups to the tasks described in Item 1.

REFERENCES

1. R. S. Stone et al., "An Assessment of the Safety Implications of Control at the Oconee-1 Nuclear Plant," NUREG/CR-4047, ORNL/TM-9444 (March 1986).

2. S. J. Bruske et al., "Effects of Control System Failures on Transients and Accidents at a Three-Loop Westinghouse Pressurized Water Reactor," EG&G Idaho, Inc. (August 1984, in preparation).

3. S. J. Bruske et al., "Effects of Control Systems Failures on Transients and Accidents at a General Electric Boiling Water Reactor," NUREG/CR-4262, EGG-2394, Vol. 1, (May 1985).

4. T. J. Burns et al., "Pressurized Thermal Shock Evaluation of the Oconee-1 Nuclear Power Plant," NUREG/CR-3770, ORNL/TM-9176 (draft).

5. D. G. Ball et al., "Pressurized Thermal Shock Evaluation of the Calvert Cliffs Unit 1 Nuclear Power Plant," NUREG/CR-4022, ORNL/TM-9408 (October 1985).

6. Electric Power Research Institute Staff, "Calvert Cliffs-1 Reactor Vessel: Pressurized Thermal Shock Analysis for a Small Steam Line Break," EPRI NP-3752-SR (November 1984).

7. G. A. Murphey et al., "Survey and Evaluation of System Interaction Events and Sources," NUREG/CR-3922, ORNL/NOAC-224 (January 1985).

8. A. J. Szukiewicz, "NRC Task Action Plan for Unresolved Safety Issue A-47, Safety Implications of Control Systems," U.S. Nuclear Regulatory Commission, Division of Safety Technology (April 1984).

9. "A Ranking of Nuclear Plant Systems for Failure Modes and Effects Analysis", ORNL #62B-13819C/62X-30, SAI #1-245-08-492-02, December 1982.

10. Calvert Cliffs Final Safety Analysis Report (FSAR), Calvert Cliffs Nuclear Plant, BG&E, December 1980.

11. Calvert Cliffs Emergency Operating Procedure, EOP-3: Loss of Main Feedwater.

12. Calvert Cliffs Emergency Operating Procedure EOP-4, Steam Line Rupture.

13. "Review of Small Break Transients in Combustion Engineering Nuclear Steam Supply Systems," CEN-114-P, Amendment 1-P (July 1979).

14. R. E. Hall, J. Fragola, and J. Wreathall, "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," NUREG/CR-3010, BNL-NUREG-51601 (November 1982).

15. D. G. Eisenhut, "Resolution of TMI Action Item II.K.3.5, "Automatic Trip of Reactor Coolant Pumps," NRC Generic Letter 83-10 (February 8, 1983).

16. E. L. Ingham, "Advanced Gas-Cooled Reactor Design Approach to Safety," IAEA Specialists Meeting on the Safety and Accident Analysis for Gas-Cooled Reactors, Oak Ridge, Tenn., May 13-15, 1985.

17. The Nuclear Safety Analysis Center and Duke Power Company, "Oconee PRA, a Probabilistic Risk Assessment of Oconee Unit 3," NSAC-60 (1984).

18. Pickard, Lowe, and Garrick, Inc., "Seabrook Station Probabilistic Safety Assessment," PLG-0300 (December 1983).

19. "Interim Reliability Evaluation Program: Analysis of Arkansas Nuclear One - Unit 1 Nuclear Power Plant," NUREG/CR-2787, Appendix C, Table C-1.

20. Calvert Cliffs Emergency Operating Procedure EOP-14 (AOP-7D), Loss of Instrument Air.

21. Calvert Cliffs Emergency Operating Procedure, "EOP-5: Loss of Reactor Coolant," Revision 20, approved September 14, 1984.

22. Calvert Cliffs Emergency Operating Procedure, "EOP-500: Loss of Coolant Accident," Revision 0 (draft).

23. S. M. Mirsky and T. L. Cook, "RETRAN Analysis of a Calvert Cliffs Multiple Secondary Side Malfunction Event," Baltimore Gas & Electric Co. (draft), cover letter to Mr. Chong Chui dated March 13, 1985.

24. Calvert Cliffs Emergency Operating Procedure EOP-1, Reactor Trip.

25. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations," IEEE Standard 500-1984.

26. Military Handbook MILHDBK-217D, "Reliability Prediction of Electronic Equipment," revised June 1983.

27. "NREP Procedures Guide," NUREG/CR-2815 (draft), U.S. Nuclear Regulatory Commission, June 21, 1982, May 1985.

28. "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments," NUREG/CR-3862, May 1985.

29. L. J. Agee et al., "RETRAN-02 - A Program for Transient Thermal-Hydraulics Anaylsis of Complex Fluid Flow Systems," EPRI NP-1850-CCM. Electric Power Research Institute, Palo Alto, January, 1983.

30. 10 CFR50, United States Nuclear Regulatory Commission Rules and Regulations, Title 10, Chapter 1, Code of Federal Regulations-Energy Part 50, Domestic Licensing of Production and Utilization Facilities, September 1, 1978.

31. IEEE Trial-Use Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Standard 603-1977; Institute of Electrical and Electronics Engineers, Inc. (1977).

32. IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Standard 603-1980; Sponsor: Nuclear Power Engineering Committee of the Power Engineering Society of the Institute of Electrical and Electronics Engineers, Inc. (1980).

33. E. P. Epler, personal communication, 1985.

NUREG/CR-4265
Volume 1
ORNL/TM-9640/V1
NRC Distribution
Categories R1, RG, R4, R13

INTERNAL DISTRIBUTION

1. S. J. Ball
2. R. E. Battle
3. N. E. Clapp, Jr.
4. F. H. Clark
5. B. G. Eads
6. D. M. Eissenberg
7. E. W. Hagen
8. R. M. Harrington
9. A. P. Malinauskas
10. T. C. Morelock
11. F. R. Mynatt
12. L. C. Oakes
13. J. P. Renier
14. D. L. Selby
15. O. L. Smith
16-26. R. S. Stone
27. W. A. Waddell
28. J. D. White
29. R. S. Wiltshire
30. M. J. Kopp (Advisor)
31. P. F. McCrea (Advisor)
32. H. M. Paynter (Advisor)
33. H. E. Trammell (Advisor)
34. Central Research Library
35. Y-12 Document Reference Section
36. I&C Publications Office
37. I&C IPC
38. Laboratory Records Department
39. Laboratory Records Department, RC
40. ORNL Patent Section

EXTERNAL DISTRIBUTION

41. P. N. Austin, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
42-46. D. L. Basdekas, Nuclear Regulatory Commission, 5650 Nicholson Lane, MS1130SS, Division of Engineering Technology, USNRC, Washington, DC 20555
47-48. W. E. Bickford, Pacific Northwest Laboratories, Richland, WA 99352
49-54. S. J. Bruske, INEL, P.O. Box 1625, Idaho Falls, ID 83415
55. S. J. Caruthers, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
56. Ivan Catton, Room 25670 Boelter Hall, UCLA, Los Angeles, CA 90024
57. R. D. Dabbs, Technology for Energy, P.O. Box 15202, Knoxville, TN 37901
58. J. D. Freels, Technology for Energy, P.O. Box 15202, Knoxville, TN 37901
59. S. J. Hurrell, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
60. L. L. Joyner, Joyner Engineers and Trainers, PC., Route #2, Box 1072, Forest, VA 24551
61. J. F. Kapinos, C-E Power Systems, 9487-2403, 1000 Prospect Hill, Windsor, CT 06095

62. W. E. Kastenberg, University of California at Los Angeles, 5532 Boelter Hall, School of Engineering and Applied Science, Los Angeles, CA 90024
63. R. Kubik, EPRI Nuclear Power Division, P.O. Box 10412, Palo Alto, CA 94303
64. C. G. Lawson, 115 Orkney Road, Oak Ridge, TN 37830
65. C. W. Mayo, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
66. A. F. McBride, Science Applications, Inc., 800 Oak Ridge Turnpike, Oak Ridge, TN 37830
67-77. S. M. Mirsky, Baltimore Gas & Electric Company, P.O. Box 1475, Baltimore, MD 21203
78. W. S. Farmer, Electrical Engineering Branch, Division of Engineering Technology, Office of RES, USNRC, Washington, DC 20555
79. F. J. Mustoe, PWR Systems and Safety Department, National Nuclear Corporation Limited, Booths Hall, Chelford Road, Knutsford, Cheshire, WA16 8QZ, England
80. Office of Scientific and Technical Information, Oak Ridge, TN 37831
81. Office of Assistant Manager for Energy Research and Development, U.S. Department of Energy, Oak Ridge Operations, Oak Ridge, TN 37831
82. P. Pan, Los Alamos National Laboratory, MS K557, Los Alamos, NM 87544
83. B. K. M. Sun, EPRI Nuclear Power Division, P.O. Box 10412, Palo Alto, CA 94303
84-109. A. J. Szukiewicz, U.S. Nuclear Regulatory Commission, 7915 Eastern Avenue, MS-1130SS, Silver Springs, MD 20910
110-545. Given NRC Category distribution R1, RG, R4, and R13