NUREG-1218

Regulatory Analysis for Proposed Resolution of USI A-47

Safety Implications of Control Systems

Draft Report for Comment

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

A. J. Szukiewicz

NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 1717 H Street, N.W.
   Washington, DC 20555
2. The Superintendent of Documents, U.S. Government Printing Office, Post Office Box 37082,
   Washington, DC 20013-7082
3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the *Code of Federal Regulations*, and *Nuclear Regulatory Commission Issuances*.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. *Federal Register* notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

NUREG-1218

Regulatory Analysis for Proposed Resolution of USI A-47

Safety Implications of Control Systems

Draft Report for Comment

Manuscript Completed: March 1988
Date Published: April 1988

A. J. Szukiewicz

Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

This report presents a summary of the regulatory analysis conducted by the NRC staff to evaluate the value impact of alternatives for the resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The NRC staff proposed resolution presented herein is based on these analyses and the technical findings and conclusions presented in NUREG-1217.

The staff has concluded that certain actions should be taken to improve safety in light-water reactor (LWR) plants. The actions recommended that certain plants upgrade their control systems to preclude reactor vessel/steam generator overfill events and to prevent steam generator dryout, modify their technical specification to verify operability of such systems, and modify selected emergency procedures to ensure plant safe shutdown following a small-break loss-of-coolant accident.

CONTENTS

		Page
ABSTRACT		iii
ABBREVIATIONS		vii
EXECUTIVE SUMMARY		ix
1	STATEMENT OF THE PROBLEM	1-1
2	SUMMARY OF LIMITATIONS, ASSUMPTIONS, AND CONCLUSIONS	2-1
	2.1 Limitations and Assumptions	2-1
	2.2 Conclusions	2-3
3	ALTERNATIVES	3-1
	3.1 GE BWR Plant Designs	3-2
	3.2 W PWR Plant Designs	3-3
	3.2.1 Overfill Events	3-3
	3.2.2 Overcool Events	3-3
	3.2.3 Overpressure Events	3-4
	3.2.4 SGTR Events	3-4
	3.3 B&W PWR Plant Designs	3-4
	3.3.1 Overfill Events	3-4
	3.3.2 Overheat Events	3-4
	3.4 CE PWR Plant Designs	3-5
4	DISCUSSION OF ALTERNATIVES	4-1
	4.1 GE BWR Plant Designs	4-1
	4.2 W PWR Plant Designs	4-4
	4.3 B&W PWR Plant Designs	4-12
	4.4 CE PWR Plant Designs	4-17
5	SUMMARY OF ALTERNATIVES	5-1
6	PROPOSED RESOLUTION OF USI A-47	6-1
	6.1 GE BWR Plant Designs	6-1
	6.2 W PWR Plant Designs	6-1
	6.3 B&W PWR Plant Designs	6-2
	6.4 CE PWR Plant Designs	6-2
7	APPLICATION OF THE BACKFIT RULE, 10 CFR 50.109	7-1
8	REFERENCES	8-1

CONTENTS (Continued)

APPENDIX A: REJECTED ALTERNATIVES

APPENDIX B: SENSITIVITY STUDY FOR REACTOR VESSEL/
STEAM GENERATOR OVERFILL SCENARIOS

APPENDIX C: CONTROL SYSTEM DESIGN AND PROCEDURAL MODIFICATION FOR
RESOLUTION OF USI A-47

ABRREVIATIONS

ADV	atmospheric dump valve
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ATWS	anticipated transients without scram
B&W	Babcock and Wilcox Co.
BWR	boiling-water reactor
CE	Combusion Engineering
CFR	Code of Federal Regulations
CSF	control system failure
CSI	core spray injection
CSS	core spray system
ECC	emergency core cooling
ECCS	emergency core cooling system
EFW	emergency feedwater
FMEA	failure mode and effects analysis
FSAR	final safety evaluation report
GE	General Electric Co.
HPI	high-pressure injection
IEEE	Institute of Electrical and Electronics Engineers
INEL	Idaho National Engineering Laboratories
LCO	limiting condition for operation
LER	licensee event report
LOCA	loss-of-coolant accident
LPCI	low-pressure coolant injection
LTOP	low-temperature overpressure
MFW	main feedwater
MMS	modular modeling system
MSIV	main steam isolation valve
MSLB	main steam line break
NRC	U.S. Nuclear Regulatory Commission
NSS	nuclear steam system
NSSS	nuclear steam supply system
ORNL	Oak Ridge National Laboratory
PNL	Pacific Northwest Laboratory

PORV	power-operated, relief valve
PRA	probabilistic risk analysis
PTS	pressurized thermal shock
PWR	pressurized-water reactor
RCS	reactor coolant system
SAI	Science Applications Inc.
SAR	safety analysis report
SBLOCA	small-break LOCA
SGTR	steam generator tube rupture
SIAS	safety injection actuation signal
SRV	safety/relief valve
TBV	turbine bypass valve
TMI	Three Mile Island
UCLA	University of California at Los Angeles
USI	unresolved safety issue
W	Westinghouse Corp.

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) has conducted its technical evaluation of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The purpose of evaluating Unresolved Safety Issue (USI) A-47 was to determine the need for modifying control systems in operating reactors, to verify the adequacy of licensing requirements identified in Section 7.7 of the Standard Review Plan (NUREG-0800) for control systems, and to determine if additional criteria and guidelines were needed. To do this, the staff had to identify control systems whose failure could (1) cause transients or accidents to be potentially more severe than those identified and analyzed in the final safety analysis reports (FSARs), (2) adversely affect any assumed or anticipated operator action during the course of a transient or accident, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents to occur at a frequency in excess of those frequencies established for abnormal operational transients and design-basis accidents. This report summarizes the results of the regulatory analysis conducted by the NRC staff to formulate the final resolution of USI A-47. The technical findings and conclusions presented in this document are based on (1) the technical findings and conclusions presented in NUREG-1217, "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-47," and (2) the probabilistic risk analysis performed by Pacific Northwest Laboratory (PNL) and presented in NUREG/CR-4385, -4386, -4387, and -3958.

A concise set of limitations and assumptions was developed to confine the USI A-47 investigation to a manageable scope and to focus attention on the more safety-significant potential control system failures. These limitations and assumptions include the following;

(1) A minimum number of safety-grade protection systems would be available to trip the reactor and initiate overpressure protection systems or emergency core cooling (ECC) systems, if needed, during transients initiated by failures in the non-safety-grade control systems.

(2) Control system failures resulting from common-cause events such as earthquakes, floods, fires, and sabotage, or operator errors of omission or commission are not addressed in this review. Multiple control system failures in non-safety-grade equipment were, however, studied in a limited way.

(3) Transients resulting from control system failures during limiting conditions for operation (LCOs) or anticipated transient without scram (ATWS) events are not addressed in this review.

(4) The plant-specific designs were appropriately modified to comply with IE Bulletin 79-27 and NUREG-0737.

On the basis of the findings identified during this review, a number of alternatives for possible regulatory action are presented and discussed. The proposed

resolution was selected after considering the safety benefits derived in terms of risk reduction and the cost of implementation.

The alternatives were selected on the basis of their potential for reducing the frequency of the initiating failure or reducing the consequences of control system failures found to be significant. The following alternatives were selected as the proposed resolution for A-47. These alternatives are discussed in Section 4 of this report.

GE BWR Plant Designs

(1) Upgrade plant designs with no automatic reactor vessel overfill protection to a 1-out-of-1 (or better) automatic reactor vessel high-level feedwater trip system.

(2) Modify technical specifications for all plants to include provisions to periodically verify the operability of the overfill protection system and ensure that automatic overfill protection is provided at all times during power operation.

(3) Issue an information letter to all applicants and licensees informing them of the evaluation results of the failure analysis conducted for USI A-47.

W PWR Plant Designs

(1) Take no action to upgrade existing main feedwater overfill protection systems on plants that have installed redundant, steam generator, high water level, overfill protection systems consisting of a 2-out-of-3 (or better) steam generator, high water level, feedwater trip, isolation system.

(2) Modify technical specifications for all plants to include provisions to periodically verify the operability of the overfill protection system and ensure that automatic overfill protection is provided at all times during power operations.

(3) Take no action to upgrade existing reactor overpressure protection systems.

(4) Issue an information letter to all applicants and licensees informing them of the evaluation results of the failure analysis conducted for USI A-47.

B&W PWR Plant Designs

(1) Modify plants similar to the reference plant (i.e., Oconee 1, 2, and 3) to either:

    (a) Provide additional instrumentation to limit or terminate main feedwater flow on steam generator high water level. (The instrumentation should be separate from the existing main feedwater pump trip instrumentation. A system that initiates closure of main feedwater block valves on steam generator high water level is acceptable); or

(b) Modify the existing overfill protection system to minimize undetected failures in the system and facilitate online testing; or

c) Upgrade the existing overfill protection system to a redundant high water level trip system that satisfies the single-failure criterion for overfill protection. (A 2-out-of-4, steam generator, high water level, trip system actuating redundant feedwater isolation equipment is acceptable.)

(2) Install Class 1E instrumentation in plants similar to the reference plant (i.e., Oconee 1, 2, and 3) to automatically initiate auxiliary (emergency) feedwater to minimize the potential for loss of steam generator cooling under any condition of operation (including a loss-of-power event).

(3) Take no action on other plants that have installed or have committed to install an emergency feedwater initiation and control (EFIC) system (or its equivalent) incorporating redundant, steam generator, high water level, overfill protection.

(4) Modify technical specifications for all plants to include provisions to periodically verify the operability of the overfill protection system and ensure that automatic overfill protection is provided at all times during power operation.

(5) Issue an information letter to all applicants and licensees informing them of the evaluation results of the failure analysis conducted for USI A-47.

It should be noted that on December 26, 1985, an overcooling event occurred at Rancho Seco Nuclear Generating Station, Unit 1. The overcooling event occurred as a result of a loss of power to the integrated control system (ICS) (see NUREG-1195). As part of the A-47 review, failure scenarios resulting from a loss of power to control systems were evaluated for each of the reference plants. In addition, two other B&W plant designs using the ICS 820 model were also reviewed in order to identify any significant loss-of-power transients that may not have been identified on the Oconee reference design (which has an ICS 721 model). These alternatives reflect the staff's findings.

As a result of the Rancho Seco event, however, a comprehensive study by the B&W Owners Group has been initiated to reassess all B&W plant designs. The reassessment includes, but is not limited to, the ICS and the support systems such as the power supply systems and maintenance (Tucker, May 15, 1986). Recommended actions for design modifications, for maintenance, and for changes to operating procedures (if any) developed for the utilities by the B&W Owners Group will be coordinated with the NRC staff and are outside the scope of this study.

CE PWR Plant Designs

(1) Modify all plants to provide additional instrumentation to automatically terminate main feedwater flow on steam generator, high water level. The instrumentation should provide sufficient redundancy to satisfy the single-failure criterion for overfill protection.

(2) Modify technical specifications for all plants to include provisions to periodically verify the operability of the overfill protection system and ensure that automatic overfill protection is provided at all times during power operations.

(3) Reassess emergency procedures and operator training programs at plants with low-head, safety-injection pumps and modify those procedures and programs if necessary to ensure safe shutdown during small-break loss-of-coolant accidents (SBLOCAs).

(4) Issue an information letter to all applicants and licensees informing them of the evaluation results of the failure analysis conducted for USI A-47.

1 STATEMENT OF THE PROBLEM

Instrumentation and control systems utilized at nuclear power plants are comprised of safety-grade protection systems and non-safety-grade control systems. Safety-grade protection systems are used to (1) trip the reactor whenever certain parameters exceed allowable limits, (2) protect the core from overheating by initiating the emergency core cooling (ECC) systems, and (3) actuate other safety systems, such as closure of main steam isolation valves (MSIVs) or opening of the safety/relief valves, to maintain the plant in a safe condition. Non-safety-grade control systems are used to maintain a nuclear plant within prescribed pressure and temperature limits during shutdown, startup, and normal power operation. Non-safety-grade control systems are not relied on to perform any safety functions during or following postulated accidents, but they are used to control plant processes that could have a significant impact on plant dynamics.

The purpose of studying Unresolved Safety Issue (USI) A-47 was to evaluate the need for modifying control systems in operating reactors, to verify the adequacy of licensing requirements identified in Section 7.7 of the Standard Review Plan (NUREG-0800) for control systems, and to determine if additional criteria and guidelines were needed. To do this, the staff had to identify control systems whose failure could (1) cause transients or accidents to be potentially more severe than those identified and analyzed in the final safety analysis reports (FSARs), (2) adversely affect any assumed or anticipated operator action during the course of a transient or accident, (3) cause technical specification safety limits to be exceeded, or (4) cause transients or accidents to occur at a frequency in excess of those frequencies established for abnormal operational transients and design-basis accidents.

Included in the program established to resolve USI A-47 (NUREG-1217) was an investigation of the effects of control system failures on four reference plant designs subjected to single and multiple control system failures during automatic and manual modes of operation. Failures at different reactor power levels including low-, middle-, and full-power operating conditions were evaluated. The review concentrated on identifying control system failures that could lead to:

(1) steam generator (reactor vessel) overfill events
(2) reactor vessel overcooling events
(3) reactor core overheating events
(4) events or accidents that could be more severe than those previously analyzed in the FSAR.

Steam generator and reactor vessel overfill and reactor vessel overcooling events have been identified previously as potentially significant events that could lead to unacceptable consequences such as a steamline break, steam generator tube rupture, or reactor vessel damage. (See NRC, "AEOD Observations and Recommendations Concerning the Problem of Steam Generator Overfill and Combined Primary and Secondary System Behavior," December 17, 1980). A number of specific control system failure scenarios were identified that could potentially lead to such events.

2 SUMMARY OF LIMITATIONS, ASSUMPTIONS, AND CONCLUSIONS

The limitations, assumptions and conclusions presented here are based on the scope and results reported in NUREG-1217.

2.1 Limitations and Assumptions

A clear and concise set of limitations and assumptions had to be established to confine the investigation to a manageable scope and to focus attention on the more safety-significant aspects of control system failures. The limitations and assumptions used for USI A-47, and their bases are discussed below:

(1) Non-safety-grade control system failures would not cause simultaneous failure of both redundant trains of safety-grade protection systems. This assumption implies that a minimum number of safety-grade protection systems would be available for (a) actuation of the reactor trip system, (b) actuation of the overpressure protection system, and (c) the initiation of the minimum number of required emergency core cooling (ECC) systems, if needed during a control system failure transient. This assumption is considered valid on the basis that adequate separation and independence are required to be provided between the non-safety-grade control systems and the safety-grade protection systems. Independence is provided by verifiable isolation devices located between safety-grade and non-safety-grade systems and/or by physically locating the safety-grade systems in separate areas and routing the electrical cables in separate raceways throughout the plant. The staff performs audit reviews of the safety-grade systems as part of the licensing review process to ensure that an adequate degree of separation and independence has been provided. Also, as part of the A-47 program, a literature search was conducted to review the operating history of control system failures. The purpose of the review, in part, was to identify any control system failures that could cause a failure of both safety-grade protection systems. The staff's review (see Section 3.2 of NUREG-1217) did not identify any such failures. In addition, as part of the USI A-17, "Systems Interaction," program, spatial interactions between safety-grade protection systems and non-safety-grade control systems were considered.

(2) External events such as earthquakes, floods, fires, and sabotage were not considered in this study. Multiple control system failures were evaluated to assess some effects of common-cause failures on the plant. However, the review was limited to a selected number of combinations of control system failures. An attempt was made to select control system failure scenarios that would bound the dynamic effects of a number of control system failures. System failures were evaluated during automatic and manual modes of operation and at different reactor power levels that include low-, intermediate-, and full-power operation.

It should be noted that the staff and utilities have performed evaluations to assess the plant's ability to achieve safe shutdown during these external

events. Fire protection has been reviewed at all operating plants to ensure conformance to 10 CFR 50 Appendix R and to evaluate the plant's ability to cope with fire and flooding in different cable trays as well as in different areas of the plant. These reviews evaluated the effects of fires and flooding in control-grade as well as in protection-grade equipment. Also, as part of the USI A-46 activities, non-safety-grade and protection-grade equipment are evaluated to assess their seismic ruggedness and ensure that plants have the ability to achieve safe shutdown after a seismic event (see item 2 in Appendix A of NUREG-1217).

(3) Operator errors of omission or commission were not addressed in this review. Operating procedures for the important transients were reviewed. An assessment was made to determine whether operating procedures (to mitigate the transients of concern) were written in such a way that the operator could perform the task in the time alloted. The staff also determined whether there was sufficient information, i.e., alarms and/or indications, available in the control room for the operator to assess the conditions in the plant at the time of the event. In some cases, early recognition of transients was necessary. Given early recognition, there were actions that the operator could take to mitigate these events. For the purpose of developing the failure scenarios and analyzing the resulting transients, two of the four plants were assumed to have operators take no action for the first 10 minutes of the transient. The other plant reviews assumed operator action could be taken on the basis of available time for action during each transient. For the risk analyses in evaluating the core-melt frequency, operator action for all plants reviewed was determined on the basis of available time for action during each significant transient identified.

(4) Transients resulting from control system failures during limiting conditions for operation (LCOs) (for example, systems deliberately disabled for a short time for testing and/or maintenance) were not considered in the review.

(5) The processes used to modify and to maintain control systems were not considered in this review.

(6) Anticipated transient without scram (ATWS) events were not considered in the review. A separate generic study has been conducted to address this issue (NUREG/CR-4385). On July 26, 1984, the Code of Federal Regulations (CFR) was amended to include 10 CFR 50.62 (ATWS Rule) which requires specific improvements to be made in the design and operation of commercial nuclear power facilities to reduce the likelihood of failure to shut down the reactor following anticipated transients, and to mitigate the consequences of an ATWS event.

(7) Control system failures that could lead to failures of (a) tanks containing liquid located outside containment and (b) fuel handling accidents (for example, spent fuel or waste disposal systems accidents) were not considered in this review. These systems are designed to be separated from control systems that are used during normal plant operations.

(8) Individual utilities had to address IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control System Bus During Operation," and to modify

their plants appropriately in order to ensure that the operator would be able to achieve cold shutdown conditions following a loss of power of a single bus to instrumentation and controls in systems used in attaining cold shutdown. It should be noted that on December 26, 1985, a reactor vessel overcooling event occurred at Rancho Seco Nuclear Generating Station, Unit 1. The overcooling event occurred as a result of a loss of power to the integrated control system (ICS) (NUREG-1195). As part of the A-47 review, failure scenarios resulting from a loss of power to control systems were evaluated for each of the four reference plants. In addition two B&W plant designs using the ICS 820 model were reviewed. As a result of the Rancho Seco event, the B&W Owners Group (BWOG) has initiated a comprehensive study to reassess all B&W plant designs, including, but not limited to, the ICS and support systems such as power supplies and maintenance (Tucker, May 15, 1986). In addition, the BWOG is currently reevaluating IE Bulletin 79-27 in terms of all B&W-designed operating plants. Recommended actions for design modifications, for maintenance, and for changes to operating procedures (if any) developed for the utilities by the BWOG will be coordinated with the NRC staff and are outside the scope of this study.

(9) The requirements of NUREG-0737, "Clarification of TMI Action Plan Requirements," dated November 1980, were implemented or committed to be implemented on individual plant designs, including, but not limited to, Items II.E.1.1, II.E.1.2, II.K.2.2, II.K.2.9, and II.G.1.

2.2 Conclusions

On the basis of the technical work completed by the NRC staff and its contractors, the following conclusions have been reached:

(1) Control system failures are dependent on such individual plant characteristics as power supply configurations and maintenance. The control system designs between the plants supplied by the same nuclear steam supply system (NSSS) vendor are functionally similar enough that the transients resulting from the failure of the same type of non-safety-grade system on the different plants will produce similar transients.

(2) Control system failures have occurred that resulted in complex transients. Improvements made after the TMI-2 accident in the design of the auxiliary feedwater system and in operator information and training should greatly aid in the recovery actions in the future.

(3) Plant transients resulting from control system failures can be adequately mitigated by the operators provided the failures do not compromise proper operation of the minimum number of protection system channels required to trip the reactor and initiate the safety systems if such initiation is required.

(4) Transients or accidents resulting from or aggravated by control system failures (except those noted in this report that can contribute to reactor vessel/steam generator overfill or core overheat events) are less severe and, therefore, are bounded by the transients and accidents identified in the FSAR analysis.

(5) Control system failure scenarios have been identified that could potentially lead to reactor vessel/steam generator overfill events, core overheat events, and overpressure events.

(6) PWR plant designs having redundant, commercial-grade (or better), overfill-protection systems for the main feedwater system that satisfy the single-failure criterion are considered to adequately preclude water ingress into the main steamlines.

(7) BWR plant designs with commercial-grade (or better) overfill protection systems are considered to adequately preclude water ingress into the main steamlines.

(8) PWR plant designs that provide automatic initiation of the auxiliary feedwater flow on low steam generator level are considered to adequately preclude core overheating.

3 ALTERNATIVES

On the basis of technical findings presented in NUREG-1217 and the probabilistic risk analysis performed by Pacific Northwest Laboratory and presented in NUREG/CR-4385, -4386, -4387, and -3958, a number of alternatives for possible regulatory action are presented and discussed in the following sections. The selection of the alternatives for possible regulatory action identified in Section 5 is based on the value of the alternatives in terms of the safety benefits derived, that is, the risk reduction achieved and the cost of implementing the alternative. These alternatives focus on reducing the initiating failure frequency or eliminating the failure mechanism of the control systems that were found to be major contributors to events of concern.

Best estimates for equipment failure probabilities were used whenever possible in the analysis for core melt and risk associated with the control system failures identified. The risk reduction resulting from the proposed alternatives is represented by the difference between the base case before action is taken and the adjusted case that results from implementing the alternatives. The core-melt frequency and risk calculations were performed for a generic plant. Adjustments were then made to factor in vendor-specific or plant-specific design considerations associated with the particular alternative. The release categories in NRC's "Reactor Safety Study" (WASH-1400) most representative of these core-melt scenarios were used to estimate risk. The computer program CRAC-2 was used for the generic risk calculations applied to a typical midwest site.

Assumptions and parameters used in the calculations are:

(1) Dose consequences represent whole-body population dose commitment (person-rems) received within 50 miles of the site.

(2) Exclusion area of 1/2-mile radius was assumed, with a uniform population density of 340 persons per square mile beyond the 1/2-mile distance. (This is the projected average 50-mile-radius population density around U.S. LWRs for the year 2000.)

(3) Evacuation was not considered.

(4) Meterological data were taken from the U.S. Weather Service station at Moline, Illinois.

(5) The core inventory at the time of the accident was assumed to be represented by a 3412-MWt (1120-MWe) plant.

(6) A remaining 30 years of plant life was assumed for each unit (except as noted).

(7) For core-melt sequences, all exposure pathways except ingestion were included.

(8) The guidelines and procedures identified in the Value-Impact Handbook (NUREG/CR-3568) were used.

The analysis is conservative. In the factors contributing to conservatism are:

(1) Operator error: The probability assumeu for operator failure to diagnose and terminate the scenarios ranged from 0.5 for scenarios with misleading or conflicting information or rapid progression (i.e., overfill in several minutes) to 0.1 for scenarios with non-conflicting information and alarms. Actu' operator response might be better, particularly in plants with simulator programs stressing proper diagnosis of failures.

(2) Steamline break: The conditional probability of a main steamline break (MSLB), given spillover into the steamlines at power, was conservatively assumed to be 0.95, decreasing to 0.5 for the probability of an MSLB given spillover after shutdown. This conservative assumption was based on a few overfill events in foreign plants where some damage to the main steamlines was reported. Although several spillover events resulting in support damage have occurred to date in U.S. commercial plants, no steamline failures have occurred.

For this analysis, break location was also assumed to occur (i.e., 50 percent probability) upstream of the main steam isolation valves (MSIVs), making isolation impossible.

For the PWR analysis, the MSLB was also assumed to have a probability of inducing a steam generator tube rupture (SGTR). The values were taken from the results of USI A-3, A-4, and A-5 studies (NUREG-0844), and varied from 0.017 to 0.003, depending on the number of tubes ruptured. The combination of SGTR and unisolatable MSLB was therefore used as the major contributor to core damage for PWRs. For the purpose of estimating the release of radionuclides, severe core damage resulting from MSLB and SGTR was taken from the relevant plant-specific probabilistic risk assessments (PRAs), modified to include control system failures. Severe core damage was conservatively assumed to be equivalent to core melt.

Although a large number of alternatives were evaluated (NUREG/CR-4385, -4386, -4387, and -3958), only those alternatives that are thought to be more important and could significantly reduce risk are discussed in detail in Section 4 of this report. The rest of the alternatives that were considered but rejected on the basis that the risk reduction in implementing these alternatives was insignificant are included in Section 3, for completeness. These alternatives are summarized in Appendix A to this report, but they have not been included for detailed discussion in Section 4.

3.1 GE BWR Plant Designs

Review of the GE BWR design identified three failure scenarios that could potentially lead to reactor vessel overfill events (NUREG-1217).* Two of the three failure scenarios could also contribute to overcool events during low-pressure startup or shutdown operation. Table 3.1 of NUREG-1217 identifies the failure scenarios and the failure mechanisms contributing to these events.

The following alternatives, discussed in more detail in Section 4, consider modifications to some BWR plants in order to improve the overfill protection system. They are:

*See also Appendix B, Section A.

(1) Modify plants designed with overfill protection similar to the reference plant (2-out-of-3) to upgrade their reactor vessel high water level feedwater trip system.

(2) Modify plants designed with less reliable overfill protection systems (1-out-of-1, 2-out-of-2, etc.) to be upgraded to a reference plant equivalent.

(3) Issue an information letter to all utilities with BWR plants informing them of the analytical results regarding overfill protection.

3.2 W PWR Plant Designs

Review of the W PWR design identified eight failure scenarios that could potentially lead to undesirable events (NUREG-1217). Two of these scenarios were identified as contributors to overfilling events, two others contributed to overcooling events, two contributed to reactor coolant system overpressure events at low temperature and pressure startup and/or shutdown conditions, and two contributed to release of radioactive material during a steam generator tube rupture (SGTR) event. Table 3.2 of NUREG-1217 identifies the failure scenarios and the failure mechanisms contributing to these events.

The following eight alternatives are discussed in more detail in Section 4. These alternatives consider actions to be taken at different W plants in order to improve the overfill protection system (Section 3.2.1), prevent overcool transients (Section 3.2.2), and prevent overpressure transients (Section 3.2.3).

An additional ninth alternative considers action to minimize potential control system failures that could cause an SGTR event to be more severe than previously analyzed (Section 3.2.4).

3.2.1 Overfill Events*

(1) Include automatic shutoff of the auxiliary feedwater system on steam generator, high water level.

(2) Issue an information letter to all utilities with W plants informing them of the evaluation regarding overfill transients via auxiliary feedwater.

(3) Modify plants with overfill protection designs similar to the reference plant to upgrade the steam generator, high-water-level, main feedwater, trip system.

(4) Take action to change the steam generator, high-water-level, main feedwater trip system.

3.2.2 Overcool Events

(1) Include automatic actuation of the steam isolation block valves to the atmospheric dump valves (ADVs) and for the isolation valves to the condenser steam dump valves.

---

*See also Appendix B, Section B.

(2) Modify the ADV controller logic to reduce the frequency of spurious opening of the ADVs.

3.2.3 Overpressure Events

(1) Take no action for additional modifications to the design of the control system for pressurizer, power-operated, relief valves (PORVs).

(2) Issue an information letter to all utilities with W PWR plants about the potential overpressure vulnerabilities resulting from operating procedures at low-temperature and low-pressure, shutdown conditions.

3.2.4 SGTR Events

Issue an information letter to all applicants and licensees with W PWR plants informing them of the potential for non-safety-grade, control system failures to occur that could make SGTR events more severe than previously analyzed. This alternative is also discussed in detail in Section 4.

3.3 B&W PWR Plant Designs

Review of the B&W PWR design identified three failure scenarios that could potentially lead to undesirable events (NUREG-1217). One failure scenario could lead to steam generator overfill and two failure scenarios could lead to reactor-core overheating. Table 3.3 of NUREG-1217 identifies the failure scenarios and the failure mechanisms contributing to these events. The following alternatives are discussed in more detail in Section 4.

3.3.1 Overfill Events*

(1) Test the steam generator, high water level, main feedwater, trip system monthly to reduce the likelihood of undetected failures.

(2) Test the steam generator, high water level, main feedwater, trip system monthly and also modify the existing trip logic to preclude undetected failures of the trip circuit and facilitate online testing.

(3) Improve the steam generator, high water level, main feedwater, trip system.

3.3.2 Overheat Events

Provide automatic protection to prevent steam generators from drying out on loss of "hand" and/or "auto" power to the integrated control system.

On December 26, 1985, an overcooling event occurred at Rancho Seco Nuclear Generating Station, Unit 1. The overcooling event occurred as a result of a loss of power to the integrated control system (ICS) (NUREG-1195). As part of the USI A-47 review, failure scenarios resulting from a loss of power to control systems were evaluated for each of the reference plants. In addition two B&W plant designs using the ICS 820 model were reviewed.

As a result of the Rancho Seco event, however, the B&W Owners Group (BWOG) has initiated a comprehensive study to reassess all B&W plant designs, including,

*See also Appendix B, Section C.

but not limited to, the ICS and support systems such as power supplies and maintenance (Tucker, May 15, 1986). Recommended actions for design modifications for maintenance and for any changes to operating procedures (if any) developed for the utilities by the BWOG will be coordinated with the NRC staff and are outside the scope of this study.

3.4 CE PWR Plant Designs

Review of the CE PWR design identified four failure scenarios that could potentially lead to undesirable events (NUREG-1217): Two could lead to steam generator overfilling,* one could lead to reactor core overheating, and one could lead to an overcooling event. The overcooling event could potentially result in a possible thermal shock event in a plant with a vulnerable pressure vessel. Table 3.4 of NUREG-1217 identifies the failure scenarios and the failure mechanisms contributing to these events. The following alternatives are discussed in more detail in Section 4. These alternatives are intended to improve overfill protection and prevent overheat or possible pressurized thermal shock events during shutdown operations following a small-break, loss-of-coolant accident (SBLOCA).

(1) Include an automatic steam generator high water level main feedwater pump or main feedwater isolation valve trip system.

(2) Improve operator procedures to manually depressurize the primary system following an SBLOCA.

Several other alternatives were also considered (NUREG/CR-3958), but the risk reduction associated with implementing them was not found to be significant. These other alternatives focused on (1) different design modifications to the existing feedwater control system to improve the overfill protection capabilities and (2) improving administrative procedures to preclude possible pressurized thermal shock events during shutdown operations following an SBLOCA.

It was also concluded that the frequency of the failure scenario leading to a possible pressurized thermal shock event and eventual vessel failure was extremely small (estimated to be 1×10^{-8} event per year) and, therefore, not judged to be a significant concern. These other alternatives were, therefore, not considered practical and are not discussed in this report.

*See also, Appendix B, Section D.

4 DISCUSSION OF ALTERNATIVES

Alternatives for possible regulatory actions are discussed in the following sections. These alternatives focus on design modifications that could reduce the frequency of the initiating failure or could eliminate the mechanisms of control system failure that the staff found to be major contributors to events of concern. Only those alternatives judged to be important are discussed here.

4.1 GE BWR Plant Designs

The following alternatives propose methods to minimize the frequency of reactor vessel overfill. The detailed risk analyses and value impact analyses are presented in NUREG/CR-4387.

(1) Modify plant designs with overfill protection similar to the reference plant (i.e., 2-out-of-3) to upgrade their reactor vessel, high-water-level, feedwater-trip system.

Such modifications would upgrade plants with a 2-out-of-3 reactor vessel, high-water-level, feedwater-trip system to a 2-out-of-4 system. Implementing this alternative would minimize the effect of equipment failures that could lead to reactor vessel overfill.

The reference plant design has a commercial-grade, 2-out-of-3, reactor vessel, high-water-level, feedwater-trip system. The level sensors are powered by independent power sources. Two of the three water-level instruments, however, share a common tap for the reference leg. Implementing this alternative would add another high-water-level, trip channel and logic to improve the reliability and increase the redundancy of the existing design.

(a) Safety Benefit

In NUREG/CR-4387, the core-melt frequency is estimated to be reduced by 7×10^{-7} per reactor-year by changing the existing 2-out-of-3 system to a 2-out-of-4 system. The estimated risk reduction is 123 man-rem over the life of the plant.

(b) Cost

Adding another channel and modifying the logic circuits is estimated to cost between $150,000 and $1,300,000 per plant. This variation in cost depends on whether additional containment penetrations and electrical cabinets are needed. It is estimated that 50 percent of these plants would require additional penetrations and electrical cabinets. Therefore, implementing this alternative is estimated to cost utilities a total sum ranging from $3,000,000 to $13,000,000. It is estimated that it would cost NRC less than $75,000, based on a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

This alternative is not considered viable, considering the questionable safety benefit of adding another channel, and the high cost for changing the reference plant design from a 2-out-of-3 system to a 2-out-of-4 system.

(2) Upgrade plant designs with less-reliable, overfill-protection systems (1-out-of-1, 2-out-of-2, etc.) to a reference plant equivalent.

Most operating BWR plants provide commercial-grade protection against reactor vessel overfill identical to the protection provided for the reference plant (that is, a 2-out-of-3 high-water-level, pump-trip system with separate and independent electrical power supplies for each level sensor). Several plants, however, have overfill protection designs with less independence and less reliability. These designs vary from 1-out-of-1, or 1-out-of-2, to a 2-out-of-2 reactor vessel, high-water-level, feedwater-pump trip. On some designs, logic separation and electrical power independence could not be verified. Three early plants do not have any overfill protection systems that automatically isolate feedwater on a reactor vessel, high-water level, and rely solely on the operator to mitigate overfeed events (see Table A1 in Appendix A).

The relative safety benefits afforded by the different combinations of high-water-level, trip logics were evaluated using the reference plant as a model. The risk associated with the different trip systems was also estimated (NUREG/CR-4387).

(a) Safety Benefit

Although some safety benefit could be gained by providing additional reactor vessel, water-level redundancy and independence to the existing designs for BWR overfill protection systems that are less reliable than the reference plant design, the benefits are not considered significant for plants that have some sort of automatic, reactor vessel, high-water-level, feedwater-trip system. In NUREG/CR-4387, however, it is estimated, that for plants with no automatic, feedwater trip, the overfill frequency is 15 times greater than estimated for the reference plant. For plants with no automatic, feedwater trip on high-water level in the vessel, except for the early vintage, very-low-power-rated plants located at low-density population sites, it is estimated that implementing (as a minimum) a single reactor vessel, high-water-level, trip system would reduce the risk by 3600 man-rem over the life of the plant. Implementing a 2-out-of-4 reactor vessel, high-water-level, trip system would reduce the overall risk by 3800 man-rem over the life of the plant. Although the difference in the risk reduction between these two designs is not significant, the additional redundancy provided in the 2-out-of-4 design provides operational flexibility during maintenance and online testing. It also minimizes spurious actuation of the feedwater-trip system. For the early vintage, low-power-rated plants located in low-density population sites such as Big Rock Point and LaCrosse, the risk reduction to implement overfill protection is insignificant (i.e., less than 0.4 man-rem over the life of the plant).

(b) Cost

The cost of adding a single, high-water-level, pump trip or a 2-out-of-4 high-water-level, pump trip to plants that have no existing automatic trip logic could not be accurately determined, but is estimated to cost between $100,000 and $500,000, per plant. Of the three plants that do not have automatic, high-water-level, feedwater-trip systems, one plant (i.e., Oyster Creek) warrants an upgrade. Therefore, implementing this alternative is estimated to cost utilities approximately $100,000. For a more versatile design that would facilitate online testing, the estimated total industry cost would be approximately $500,000 (for this plant, additional penetrations are not needed to complete the modifications). It is estimated that it would cost NRC $5000, based on a 0.5 staff-month effort per plant, to review the design modification.

(c) Value Impact

This is a viable alternative, considering the safety benefit that can be gained by upgrading certain plants that have no overfill protection to a 1-out-of-1, high-water-level, trip configuration or better and the relatively low cost estimated for implementing the designs. It should be noted that although a single, high-water-level, feedwater-trip system is adequate, a more redundant design that facilitates online testing, minimizes spurious actuation, and permits bypass capabilities during equipment inoperability is preferred. It should also be noted that for early vintage, low-power-rated plants located in remote areas (i.e., Big Rock Point and LaCrosse), this alternative is not viable.

(3) Issue an information letter to all utilities that have BWR plants informing them of the evaluation results regarding overfill protection.

The review evaluated a large number of BWR plant designs and identified variations in the overfill protection design for BWR plants (see Table A1 in Appendix A). Sensitivity studies were performed to determine if the differences in the designs were significant. Although the staff concluded that only trivial safety benefit could be gained by providing additional, redundant, water-level sensors for the feedwater-trip system of plants that have overfill protection systems, variations in these designs can exist that may have not been considered in this review because of the assumptions made in utilizing the reference plant design as a base model. Plant-specific differences (such as power supply interdependencies, sharing of sensors between control and trip logic, operator training and procedures, and design for indication and alarms available to the operator) may exist. However, the staff believes that plant-specific differences will not significantly alter the estimate of failure rate utilized in the staff study. It is proposed that the staff issue an information letter to all utilities whose BWR plants have automatic, overfill-protection systems, advising them of the potential failure mechanisms for overfill and associated consequences.

(a) Safety Benefit

Implementing this alternative would provide licensees with information that could allow them to identify potential improvements in plant designs

and minimize potential common-mode failures that could increase the likelihood of overfill events.

Some safety benefit could be gained by modifying existing overfill protection designs if the designs are susceptible to common-cause failures associated with the plant-specific design. It is difficult, however, to determine this safety benefit accurately.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

No value impact is associated with implementing this alternative.

4.2 W PWR Plant Designs

The following proposed alternatives are methods to minimize steam generator overfill, reactor vessel overcool, and overpressure events. The detailed risk analyses and value impact analyses are presented in NUREG/CR-4385.

(1) Provide automatic shutoff (or flow restriction) of the auxiliary feedwater system on steam generator, high water level.

This alternative proposes that the existing auxiliary feedwater (AFW) system be modified to automatically restrict the AFW flow or trip the AFW pumps on steam generator, high water level.

For the reference plant study, the onset of steam generator overfill via the AFW system was predicted to occur in about 3 minutes. The AFW system is automatically initiated when the main feedwater pumps trip, and overfill conditions would occur via AFW flow if the operator failed to manually terminate AFW on steam generator, high water level.

(a) Safety Benefit

In NUREG/CR-4385, core-melt frequency is estimated to be reduced by about 6×10^{-8} per reactor-year by providing such automatic shutoff. It is estimated that risk would be reduced by about 9 man-rem over the life of the plant.

The potentially negative consequences of implementing this alternative (i.e., increasing the potential for inadvertent isolation of the AFW system) has not been factored into these estimates. Inadvertent isolation of the AFW system when the system is required could decrease the overall reliability of the system and could reduce plant safety.

(b) Cost

The switches on the steam generator that are used to control water level and that are already used to trip the reactor or initiate the feedwater-isolation system could also be utilized for this modification, thus

reducing equipment costs associated with implementing this alternative. The estimated cost to implement a high-water-level trip or restrict flow for the AFW system is about $45,000 per 3-loop plant. Implementing this alternative is estimated to cost utilities a total of $2,300,000. This does not include the cost for electrical penetrations and electrical systems cabinets that may be needed. Assuming that 50 percent of the plants would require additional penetrations, the estimated cost to industry is $27,000,000. It is estimated that it would cost NRC $250,000, assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

This alternative is not considered viable because the safety benefit is questionable and because a potentially high cost may be incurred.

(2) Issue an information letter to all applicants and licensees that have W PWR plants informing them of the results of reviews of steam generator overfill transients via the auxiliary feedwater systems.

Review of other W PWR plants identified variations in the design of the AFW systems that could change the time required to overfill the steam generators via the AFW system. Some plant designs represented improvements over the reference plant design. These improved designs utilize restricting orifices or flow-restricting control valves in the flow lines that prevent excessive AFW flow to any steam generator and allow more time for the operators to respond to overfeed events. This design feature would result in less-severe transients than those postulated for the reference plant. The review did not identify any plants at which overfill transients could be more severe than at the reference plant. Although it is the staff's judgment that the analysis conducted on the reference plant is a bounding analysis, there may be some plant designs for which some safety benefit could be gained either by providing automatic shutoff or flow restriction of the AFW system on steam generator, high water level or by improving administrative procedures to preclude such overfill events. Therefore, an information letter could be issued to all utilities to provide them with the data and the results of staff analysis.

(a) Safety Benefit

By implementing this alternative, personnel could potentially identify plant-specific designs for which some safety benefit could be gained in providing a steam generator, high-water-level trip to existing AFW designs or to improve administrative procedures to preclude overfill events via the AFW system. It is impractical, however, to quantify this safety benefit.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

No value impact is associated with implementing this alternative.

(3) Modify plants with overfill protection designs similar to the reference plant to upgrade the steam generator, high-water-level, main-feedwater-trip system.

Implementing this alternative would upgrade designs for plants with a 2-out-of-3 steam generator, high-water-level, main-feedwater-trip system to a 2-out-of-4 system. Implementing this alternative would minimize redundant equipment failures that could lead to steam generator overfill and ensures compliance with Section 4.7(3) of IEEE Standard 279-1971 relating to control and protection system interaction.

The reference plant design has a safety-grade, 2-out-of-3, steam generator, high-water-level, main-feedwater-trip system. This alternative would include an additional safety-grade, water-level instrument and logic modification for each steam generator.

(a) Safety Benefit

The estimated core-melt frequency associated with the overfill transient is extremely small (less than 10^{-10} per reactor-year) because the high-quality, redundant, safety-grade, trip system has already been incorporated into the design. Therefore, only insignificant risk reduction could be gained by incorporating additional redundancy.

(b) Cost

The estimated cost for adding another safety channel is between $250,000 and $1,300,000 per plant. The cost depends on whether additional containment penetrations and electrical cabinets are needed for these modifications. It is estimated that 65 percent of the plants would need some modification and that half of these plants could require additional penetrations and cabinets. Therefore, implementing this alternative is estimated to cost utilities a total sum ranging from $8,000,000 to $24,000,000. It is estimated that it would cost NRC $250,000, assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

This alternative is not considered viable because virtually no safety benefit will be derived from it and because the cost of modifying the existing design is potentially high.

(4) Change the steam generator, high-water-level, main-feedwater-trip system.

Review of a number of operating plant designs and new designs under review for an operating license confirmed that all but three W PWR plant designs (Haddam Neck, San Onofre 1, and Yankee Rowe) have either a 2-out-of-3 or a 2-out-of-4, steam generator, high-water-level, trip system to terminate the main feedwater flow during an overfill event. These systems are redundant and are designed to meet safety-grade requirements. San Onofre and Yankee Rowe do not have automatic overfill protection. Haddam Neck has an overfill protection system consisting of a safety-grade, 1-out-of-2, steam generator, high-water-level interlock which automatically shuts the main feedwater control valves to the steam generator. The newer designs

incorporate the more redundant 2-out-of-4 system that gives additional flexibility during testing and satisfies all the prescribed safety requirements, including those that relate to control and protection systems interactions addressed in Section 4.7(3) of IEEE Standard 279-1971. The licensee event report (LER) review of operating history of W PWR plants, revealed that no steam-generator-overfill events have occurred as a result of feedwater overfill transients. The staff, therefore, concludes that sufficient design features are provided on all but three W plants for feedwater isolation and for operator training to mitigate overfeed transients in sufficient time to prevent steam-generator-overfill events.

(a) Safety Benefit

Not applicable.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

This alternative is not viable. The existing designs provide an adequate degree of protection for overfeed transients to prevent steam-generator-overfill events; therefore, no additional requirements are recommended.

(5) Provide automatic actuation of the steam-isolation, block valves to the atmospheric dump valves (ADVs) and for the isolation valves to the condenser-steam dump valves.

The following control system failure modes were identified that could lead to reactor overcool transients: Case 1 - Inadvertent opening of all five condenser-steam dump valves during full-power operation, and Case 2 - Inadvertent opening of the atmospheric dump valves, condenser to steam dump valves, or main turbine, stop valves during hot-shutdown conditions. This alternative requires that the control system design be modified to automatically close the isolation block valves to the steamline, power-operated, relief valves [i.e., atmospheric dump valves (ADVs)] and to the condenser-steam dump valves. This modification would isolate the steam flow resulting from inadvertent opening of these valves, and would mitigate overcooling events resulting from such failures.

For Case 1, multiple independent failures are needed to open all five condenser-steam dump valves. A special arming circuit installed at most W plants would have to fail or be disabled, in addition to another single failure in the control circuit, for all valves to fail open. The failure frequency to open all the condenser-steam dump valves is, therefore, estimated to be very low. In addition, most operating plants and plants under review for operating licenses have systems designs that represent an improvement over the reference plant design. These designs will automatically terminate steam flow by isolating the steamlines via the MSIVs on a low-steamline-pressure signal. For those plants in which a control system failure results in inadvertent opening of relief valves downstream of the MSIVs, the overcooling transient should be less severe than for the reference plant design.

For Case 2, the major control system contributors in terms of the frequency of initiating failures to an overcooling event were failures associated with inadvertent opening of the ADVs. The contribution associated with condenser-steam dump valve failures (i.e., failure frequency) is estimated to be a factor of 10 less than the ADVs and the contribution associated with the turbine stop valve failures is estimated to be a factor of 100 less than the ADVs. For Case 2, only ADVs are considered.

(a) Safety Benefit

In NUREG/CR-4385, public risk associated with Case 1 failures has been estimated. The estimated core-melt frequency associated with this failure scenario is extremely small (less than 10^{-10} per reactor-year). This is due to a combination of the low, initiating frequency and the low probability of subsequent fuel damage or core-melt following an accident on the steam side of a PWR. The estimated public risk is less than 0.003 man-rem for the life of the plant. For those plants that provide automatic MSIV closure on a low steamline pressure signal, the core-melt frequency contribution would be even smaller than predicted for the reference plant. For Case 2, a higher core-melt frequency was calculated because of potential single failures that could open the ADVs. The estimated core-melt frequency associated with such overcooling events is 8×10^{-7} per reactor-year. The estimated public risk is 118 man-rem for the life of the plant. The estimated reduction in core-melt frequency associated with implementing automatic actuation of the block valves (for ADVs only) is 1.4×10^{-7} per reactor-year. The estimated risk reduction was 20 man-rem for the life of the plant.

(b) Cost

For Case 1: The estimated cost of providing instrumentation for automatic isolation valve closure logic for the condenser-steam dump valves is $65,000 per plant. Implementing this alternative is estimated to cost utilities a total of $3,400,000. If additional valves are needed to replace the existing valves, the cost would be significantly greater and would vary from plant to plant, depending on how many steam dump valves the plant has.

For Case 2: The estimated cost of providing automatic block valve closure logic for ADVs is between $123,000 and $1,200,000 per plant. The variation in cost depends on whether additional containment penetrations and electrical cabinets are needed. It is estimated that 50 percent of the plants could require additional penetrations and cabinets. Therefore, implementing this alternative is estimated to cost utilities a total sum between $6,500,000 and $37,000,000. It is estimated that it would cost NRC $250,000, assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

For Case 1: This alternative is not considered viable because virtually no safety benefit will be derived from implementing automatic isolation of the condenser-steam dump valves.

For Case 2: This alternative is not considered viable because the safety benefit is insignificant and the cost of modifying the existing design to provide automatic isolation of the ADVs is potentially high.

It should be noted that Generic Issue 70 (Bernero, April 30, 1985) was established to assess the need for improving the reliability of the PORVs and block valves in light of plant-protection and accident-mitigation requirements. This study will be applicable to all PWRs that have PORVs. Once that issue is resolved, additional insight may warrant reconsideration of the existing designs.

(6) Modify the ADV controller logic to reduce the frequency of spurious opening of the ADVs.

This alternative also deals with false ADV lifts resulting from control system failures (same as Case 2 of Alternative 5). This alternative would not eliminate mechanical failures, but is intended to minimize the ADV failure rate resulting from electrical faults. It was assumed that an enable circuit to the existing design would be required.

(a) Safety Benefit

In NUREG/CR-4385, the estimated reduction in the frequency of core melt from implementing this alternative is 1.5×10^{-7} per reactor-year. The estimated risk reduction is about 20 man-rem for the life of the plant.

(b) Cost

The estimated cost to the utilities of modifying the ADV controller logic is between $123,000 and $1,200,000 per plant. The variation in cost depends on whether additional penetrations and electrical cabinets are needed. It is estimated that 50 percent of the plants could need additional penetrations and cabinets. Therefore, implementing this alternative is estimated to cost utilities a total ranging from $6,500,000 to $37,000,000.

(c) Value Impact

This alternative is not considered viable because only a very small safety benefit could be gained, and because the cost of implementing this modification is potentially high.

(7) Upgrade the design of the control system for pressurizer PORVs.

Although a number of alternatives were considered in Section 3 to minimize overpressure events, the alternative for additional modification for overpressure protection was not considered appropriate for the following reasons:

(i) The pressurizer PORVs in W PWR plants are powered from independent, safety-grade, power supplies in essentially the same configurations as in the reference plant design. Some plants provide independent, non-Class 1E, battery-backed, power supplies, which the staff has also found acceptable. This design minimizes the potential of a common-mode failure resulting from a loss of electric power and minimizes

the potential for an overpressure event resulting from control system failures.

(ii) A large number of plant designs contain additional improvements over the reference plant design. These improvements consist of overpressure-relief capability through the residual heat removal (RHR) system (during cold-shutdown operations) which allows more time for the operator to respond to overpressure events. This design feature results in less-severe transients than are produced on the reference plants.

Only a few plant designs were identified as being identical to the reference plant design in which additional, pressure-relief capability via the RHR system was not provided. The staff believes, however, that sufficient reviews were conducted previously (NUREG-0371, -0748) to conclude that all the W designs provide a design system equivalent to or better than the design system of the reference plant.

In addition, two major ongoing generic studies are determining the need for additional modifications to existing pressurizer PORV systems [i.e., Generic Issue 70 (Bernero, April 30, 1985) and Generic Issue 94 (Denton, July 23, 1985)]. Conditioned on the satisfactory resolution and completion of these generic issues, this alternative is considered a viable option.

(a) Safety Benefit

In NUREG/CR-4385, the contribution of frequency of core melt for the overpressure event on the reference plant design is less than 1×10^{-10} per reactor-year. This is due primarily to the low initiating frequency estimated for the identified failure mode. Because most of the plants provide equivalent or better designs than the reference plant provides, the core-melt frequency contributions for other plants are expected to be as low. No safety benefit would be gained by instituting additional requirements.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

Not applicable.

(8) Issue an information letter to all applicants and licensees that will operate W PWR plants about the potential overpressure vulnerabilities resulting from operating procedures at low-temperature and low-pressure, shutdown conditions.

This alternative was considered because variations in plant procedures could exist that could create the potential for the operator to cause reactor vessel, overpressure conditions by prematurely transferring the PORV setpoints to a higher value during shutdown or startup operations. The staff did not review the appropriate plant procedures to determine which plants are susceptible to this problem. The nuclear steam supply

system vendor stated (Westinghouse, WCAP-10797) that most W PWRs have procedural and administrative controls that would make the pressure transients at these conditions less severe than conditions analyzed for the reference plants, primarily because of the capability of the RHR system to relieve pressure. The adequacy of this capability is currently being reevaluated under Generic Issue 94.

(a) Safety Benefit

In NUREG/CR-4385, the overpressure consequences for this scenario have been estimated. The estimated contribution of this overpressure event (frequency of core melt) is less than 1×10^{-10} per reactor-year. This is due primarily to the low, initiating frequency estimated for the identified failure mode. A reduction in the frequency of core melt for any modification to the procedures would, therefore, be insignificant.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

This alternative is not considered viable because essentially no safety benefit is to be gained from implementing this alternative. The resolution of Generic Issue 94 may result in additional changes which have not been considered here.

(9) Issue an information letter to all applicants and licensees with W PWR plants informing them of the potential for non-safety-grade, control-system failures to occur that could make SGTR events more severe than previously analyzed.

Two control-system failure scenarios were identified during the review. One was an inadvertent opening of a ADV (or safety-grade relief valve) coincident with a loss of offsite power. The other was an instantaneous, main feedwater, overfeed transient coincident with an inadvertent opening of the ADV (or safety/relief valve).

Staff analysis indicates that the contribution of these events to the frequency of core melt is extremely small, primarily because of the low, estimated, initiating frequency for the combination of failures identified. This alternative was considered, however, because the designs of the offsite power systems on different plants vary and because the reliability of these systems can alter assumptions made in this report about the frequency of accidents. Such variations could change the calculations on core-melt frequency.

(a) Safety Benefit

In NUREG/CR-4385, the safety benefit of informing applicants and licensees about this potential was estimated. The estimated contribution of the event to the frequency of core melt, involving a simultaneous failure of the

feedwater control system coincident with an inadvertent opening of the ADV, is less than 1×10^{-10} per reactor-year. Therefore, any design modification would reduce the frequency of core melt only insignificantly. The contribution to the frequency of core melt for the event involving an inadvertent opening of the ADV coincident with a loss of offsite power, however, is estimated to be 1×10^{-8} per reactor-year. The estimated public risk associated with this event is about 2 man-rem for the life of the plant.

(b) Cost

Not applicable.

(c) Value Impact

This alternative is not considered viable. Variations in the reliability of offsite power for different plant designs may modify the frequency of loss of offsite power (up to 8 hours) by a factor of 30 (NUREG-1032). Such variations would not change the contribution to the frequency of core melt enough to warrant modifications to the design.

4.3 B&W PWR Plant Designs

The following alternatives propose methods to minimize steam generator overfill and reactor vessel overheat events. The detailed risk analyses and value impact analyses are presented in NUREG/CR-4386.

(1) Test the steam generator, high-water-level, main-feedwater-trip system every month to reduce the likelihood of undetected failures.

The design of the reference plant (Oconee Nuclear Station, Unit 1) calls for a non-safety-grade, main-feedwater-pump trip utilizing a 2-out-of-2 steam generator, high-water-level, trip system from each steam generator. The design is subject to a number of single failures, each of which can prevent a feedwater trip on high water level. The system is designed in an "energized to trip" configuration in such a way that a loss of control power (i.e., 125-V dc) to the control system would not trip the feedwater pumps. A loss of power to the level sensors with available 125-V dc control power would cause the main feedwater pumps to trip. This alternative was considered in order to reduce the frequency of undetected failures which could lead to steam-generator-overfill events. Only three plants (Oconee Nuclear Station, Units 1, 2, and 3) utilize this design. Other B&W designs are discussed below.

(a) Safety Benefit

In NUREG/CR-4385, the safety benefit of such monthly testing was estimated. The estimated reduction in the frequency of core melt as a result of performing monthly inspections is 3.2×10^{-6} per reactor-year. The estimated reduction of risk is 450 man-rem for the life of the plant. An increased test frequency, however, could increase the likelihood of inadvertent loss-of-feedwater (LOF) events. The challenges to the protection systems resulting from these inadvertent LOF events could potentially lead to adverse

system vendor stated (Westinghouse, WCAP-10797) that most W PWRs have procedural and administrative controls that would make the pressure transients at these conditions less severe than conditions analyzed for the reference plants, primarily because of the capability of the RHR system to relieve pressure. The adequacy of this capability is currently being reevaluated under Generic Issue 94.

(a) Safety Benefit

In NUREG/CR-4385, the overpressure consequences for this scenario have been estimated. The estimated contribution of this overpressure event (frequency of core melt) is less than 1×10^{-10} per reactor-year. This is due primarily to the low, initiating frequency estimated for the identified failure mode. A reduction in the frequency of core melt for any modification to the procedures would, therefore, be insignificant.

(b) Cost

The utilities would incur no appreciable cost by implementing this alternative.

(c) Value Impact

This alternative is not considered viable because essentially no safety benefit is to be gained from implementing this alternative. The resolution of Generic Issue 94 may result in additional changes which have not been considered here.

(9) Issue an information letter to all applicants and licensees with W PWR plants informing them of the potential for non-safety-grade, control-system failures to occur that could make SGTR events more severe than previously analyzed.

Two control-system failure scenarios were identified during the review. One was an inadvertent opening of a ADV (or safety-grade relief valve) coincident with a loss of offsite power. The other was an instantaneous, main feedwater, overfeed transient coincident with an inadvertent opening of the ADV (or safety/relief valve).

Staff analysis indicates that the contribution of these events to the frequency of core melt is extremely small, primarily because of the low, estimated, initiating frequency for the combination of failures identified. This alternative was considered, however, because the designs of the offsite power systems on different plants vary and because the reliability of these systems can alter assumptions made in this report about the frequency of accidents. Such variations could change the calculations on core-melt frequency.

(a) Safety Benefit

In NUREG/CR-4385, the safety benefit of informing applicants and licensees about this potential was estimated. The estimated contribution of the event to the frequency of core melt, involving a simultaneous failure of the

feedwater control system coincident with an inadvertent opening of the ADV, is less than 1×10^{-10} per reactor-year. Therefore, any design modification would reduce the frequency of core melt only insignificantly. The contribution to the frequency of core melt for the event involving an inadvertent opening of the ADV coincident with a loss of offsite power, however, is estimated to be 1×10^{-8} per reactor-year. The estimated public risk associated with this event is about 2 man-rem for the life of the plant.

(b) Cost

Not applicable.

(c) Value Impact

This alternative is not considered viable. Variations in the reliability of offsite power for different plant designs may modify the frequency of loss of offsite power (up to 8 hours) by a factor of 30 (NUREG-1032). Such variations would not change the contribution to the frequency of core melt enough to warrant modifications to the design.

4.3 B&W PWR Plant Designs

The following alternatives propose methods to minimize steam generator overfill and reactor vessel overheat events. The detailed risk analyses and value impact analyses are presented in NUREG/CR-4386.

(1) Test the steam generator, high-water-level, main-feedwater-trip system every month to reduce the likelihood of undetected failures.

The design of the reference plant (Oconee Nuclear Station, Unit 1) calls for a non-safety-grade, main-feedwater-pump trip utilizing a 2-out-of-2 steam generator, high-water-level, trip system from each steam generator. The design is subject to a number of single failures, each of which can prevent a feedwater trip on high water level. The system is designed in an "energized to trip" configuration in such a way that a loss of control power (i.e., 125-V dc) to the control system would not trip the feedwater pumps. A loss of power to the level sensors with available 125-V dc control power would cause the main feedwater pumps to trip. This alternative was considered in order to reduce the frequency of undetected failures which could lead to steam-generator-overfill events. Only three plants (Oconee Nuclear Station, Units 1, 2, and 3) utilize this design. Other B&W designs are discussed below.

(a) Safety Benefit

In NUREG/CR-4385, the safety benefit of such monthly testing was estimated. The estimated reduction in the frequency of core melt as a result of performing monthly inspections is 3.2×10^{-6} per reactor-year. The estimated reduction of risk is 450 man-rem for the life of the plant. An increased test frequency, however, could increase the likelihood of inadvertent loss-of-feedwater (LOF) events. The challenges to the protection systems resulting from these inadvertent LOF events could potentially lead to adverse

overheat transients. It was impractical to estimate the risk associated with these negative contributions.

(b) Cost

The estimated cost of developing test procedures and inspecting the system on a monthly basis is about $100,000 per plant. This estimate does not include plant downtime that could occur because of inadvertent, feedwater-pump trips caused by additional testing. Only Oconee 2 and 3 are similar in design to the reference plant. Therefore, the estimated total cost to utilities for implementing this alternative is $300,000. The NRC would incur no costs if this alternative were implemented.

(c) Value Impact

This alternative is not considered viable. Considering only the benefits derived from implementing this alternative and the relatively low cost incurred, it would at first appear that this alternative is viable. The staff finds, however, that the likelihood of increasing the number of transients from an inadvertent loss of feedwater resulting from more testing is sufficiently high that potential risks outweigh any estimated safety benefits. In addition, it may not be possible to test a complete control system circuit on the present design during normal plant operation, and the utility could incur additional costs in providing a fully testable system.

(2) Test the steam generator, high-water-level, main-feedwater-pump, trip system monthly, and also modify the existing trip logic to preclude undetected failures in the trip circuit and facilitate online testing. This alternative is applicable only to Oconee 1, 2, and 3 plants.

This alternative would also include additional design modifications to:

(i) permit full online testing of the trip system, and

(ii) provide an additional trip relay in parallel with the existing master trip relay to prevent a single failure (or an undetected failure) from initiating a trip.

This alternative differs from Alternative 1 (above) by specifying

(i) additional redundancy to the existing trip logic, and

(ii) additional circuit modifications to permit full test capability of the overfill protection system.

(a) Safety Benefit

In NUREG/CR-4386, the safety benefit of implementing such modifications and instituting monthly testing as described was estimated to reduce the core-melt frequency by 7×10^{-6} per reactor-year. The estimated risk reduction is 1000 man-rem for the life of the plant.

(b) Cost

The estimated cost for developing new test procedures, providing monthly inspections, and modifying existing logic is $200,000 per plant. This does not include downtime costs that could be incurred as a result of inadvertent, feedwater-pump trips caused by additional testing. Only Oconee 2 and 3 are similar to the reference plant. Therefore, implementing this alternative is estimated to cost utilities a total of $600,000. It is estimated that it would cost NRC $15,000, based on a 0.5 staff-month effort per plant, to review the design modification.

(c) Value Impact

Even given the potential for LOF events resulting from additional testing, the risk reduction gained from these modifications makes this alternative viable. The potential uncertainty for an increased number of LOF transients exists for this alternative as for Alternative 1. The improved reliability of the design as a result of implementing this alternative, however, improves the estimated risk reduction. It should be noted that other alternatives may be preferred.

(3) Upgrade the steam generator, high-water-level, main-feedwater-pump, trip system.

This alternative would propose that the overfill protection system on the reference plant be upgraded to satisfy the single-failure criterion. Two cases were considered to improve the existing plant design. Case 1 would provide an additional, independent, main feedwater, trip system actuated from a separate, steam generator, high-water-level channel to isolate the feedwater flow via a trip of the main feedwater block valves. The current design provides a 2-out-of-2, high-water-level, trip system that only trips the main feedwater pumps. Case 2 would propose that the existing design be upgraded to a 2-out-of-3 or 2-out-of-4, high-water-level, trip system. Several modifications to the trip system logic were evaluated in NUREG/CR-4386. As a result of that evaluation, it was concluded that most of the benefits gained from implementing a 2-out-of-4 trip system rather than a 2-out-of-3 system were associated with greater flexibility and ease in testing the trip system during power operation. There was no substantial difference between the reduction in risk for a 2-out-of-3 or a 2-out-of-4 trip, logic system. These alternatives would not require additional testing beyond what is presently provided.

Only the two other B&W PWR plants (Oconee 2 and 3) have overfill-protection systems similar to the overfill-protection system of the reference plant. All other operating plant designs and plants currently in the licensing review stage have modified their designs or have committed to modify their designs by the time of the next refueling. These modified designs are safety grade. The initiating logic is either a 2-out-of-4 or a 1-out-of-2 taken-twice, high-water-level, trip system actuating redundant main feedwater isolation systems (i.e., closure of main feedwater isolation and control valves). One plant design currently under review for an operating license will use a safety-grade, 2-out-of-3 trip, logic system. The design at other B&W PWR plants offers, or will offer, an adequate degree

of protection for steam generator overfill events. These designs represent a substantial improvement; therefore, no additional changes are recommended for these plants. It should be noted, however, that the plants that have committed to, but have not yet implemented, these designs are more at risk than the reference plant design because they lack a high-water-level, main feedwater trip. It is recommended that these design modifications be implemented at other plants in a timely manner.

(a) Safety Benefit

In NUREG/CR-4386, the safety benefit of this upgrade was estimated. For Case 1 the estimated reduction in the frequency of core melt is 9×10^{-6} per reactor-year. The estimated risk reduction is 1300 man-rem over the life of the plant. For Case 2, the estimated reduction in the frequency of core melt is 8×10^{-6} per reactor-year. The estimated risk reduction is 1200 man-rem over the life of the plant.

(b) Cost

Cost is not estimated for Case 1. It is assumed that existing steam generator, water-level transmitters used for other functions (e.g., startup range transmitters) could be utilized to monitor a high-water-level condition in the steam generator. The cost per plant for implementing this alternative would, therefore, be relatively low (less than $100,000). If additional electrical penetrations, electrical cabinets, and water-level transmitters are required, the cost would be higher. Only Oconee 2 and 3 are similar to the reference plant; therefore, the estimated cost per plant is $300,000. If additional penetrations, cabinets, and transmitters are needed, the cost per plant could be as high as $1,100,000 and the total cost to utilities could be as high as $3,300,000.

For Case 2, the estimated cost for modifying the design to a 2-out-of-3, high-water-level, pump-trip configuration is $300,000; the estimated cost per plant is $600,000 for modifying the design to a 2-out-of-4 system. These estimates do not include installation of additional electrical penetrations or control cabinets that may be needed. Only Oconee 2 and 3 are similar to the reference plant; therefore, the estimated total cost to utilities is $900,000 and $1,800,000, respectively. If additional penetrations and cabinets are needed, it could cost the utilities as much as $5,000,000 to install a 2-out-of-4 system in the three plants. It is estimated that it would cost NRC $15,000 (for either case), assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

For Case 1, this alterrative is considered viable, considering the substantial risk reduction that can be gaind by implementing it and the potentially moderate costs that would be incurred. For Case 2, this alternative is also considered viable, considering the significant risk reduction that can be gained from implementing an upgrade and the relatively low cost. If, however, additional electrical penetrations are needed, this alternative could become too expensive and of less benefit than Case 1.

(4) Provide automatic protection to prevent steam generators from drying out on loss of "hand" (manual) control or "auto" (automatic) control power to the integrated control system.

Two scenarios were identified that could potentially lead to core overheat events. These events could occur if the operator did not take proper action to ensure feedwater flow to the steam generators. Loss of hand power and loss of auto power in the integrated control system (ICS) were identified as the initiators of the overheat scenarios.

A number of corrective actions could be taken to avoid this dryout scenario. They include:

(i) Provide automatic initiation of the emergency feedwater system on steam generator, low water level (preferred).

(ii) Provide sufficient feedwater flow at minimum pump speed to keep the steam generator from drying out.

(iii) Trip the main feedwater pumps on loss of hand power (a main feedwater pump trip would automatically initiate the emergency feedwater systems).

(iv) Train operators to cope with a loss of hand or auto power to the ICS.

(v) Install alarms in the control room to alert operators to loss of hand and auto power to the ICS.

Some of these actions take place automatically; others require operator interaction.

All B&W PWR plants, with the exception of the reference plant and Oconee 2 and 3 designs, provide automatic initiation of the emergency feedwater system on steam generator, low water level (action i), minimizing the potential for loss of steam generator cooling. Therefore, this concern is plant specific and applies only to Oconee 1, 2, and 3 plants.

(a) Safety Benefit

In NUREG/CR-4386, the safety benefit of implementing such automatic protection was estimated. The estimated reduction in the frequency of core melt to implement the different options is between 2×10^{-6} per reactor-year and 9×10^{-6} per reactor-year. The preferred option of the five options listed above is to provide automatic initiation of the emergency feedwater system on steam generator, low water level. The estimated risk reduction for the preferred option is between 155 man-rem and 870 man-rem over the life of the plant.

(b) Cost

It is considered extremely unlikely that the cost of implementing the suggested corrective actions would exceed $150,000 per plant. Therefore, it

would cost utilities a total of $450,000 to implement this alternative. It is estimated that it would cost NRC $15,000, assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

This alternative is considered viable because some safety benefit could be gained with minimal modifications.

4.4 CE PWR Plant Designs

The following alternatives propose modifications to minimize steam generator overfill events and reactor vessel overpressure events. The detailed risk analyses and value impact analyses are presented in NUREG/CR-3958.

(1) Provide an automatic, redundant, steam generator, high-water-level, main feedwater pump or feedwater isolation valve, trip system.

Implementation of this alternative would mean that all CE PWR plant designs have a 2-out-of-4, steam generator, high-water-level, feedwater-isolation system. The reference plant design currently utilizes a 2-out-of-4, steam generator, high-water-level signal to trip the main steam turbine. A turbine trip signal will, in turn, trip the reactor, shut the main feedwater valves, and open the startup feedwater valves to 5 percent of rated flow. Although the current feedwater runback system does reduce the frequency of steam generator overfill events should an overfeed transient occur, the operator is still needed to manually trip the feedwater pumps or the feedwater isolation valves to prevent overfill if a failure renders the feedwater-water runback system inoperable. This design is similar to the design of other CE PWR plants.

The main feedwater isolation system should be initiated at a higher, steam generator, water-level setpoint than is used for the runback control. This would permit the existing control system to perform its function and would minimize the need to automatically terminate main feedwater.

(a) Safety Benefit

In NUREG/CR-3958, the safety benefit of such a system was estimated. The estimated reduction in the frequency of core melt is 4×10^{-6} per reactor-year. The estimated risk reduction is 570 man-rem over the life of the plant.

(b) Cost

It was assumed that existing instrumentation to generate the high-water-level signal and the existing motor-operated feedwater isolation valves could be used. The cost for implementing this alternative (i.e., a 2-out-of-4, steam generator, high-water-level, feedwater isolation) would, therefore, be relatively low (less than $100,000 per plant). It would cost utilities a total of $1,500,000 to provide this automatic-trip system. If additional electrical penetrations and electrical cabinets were required, the cost would be higher. It is assumed that existing penetrations and

cabinets can be used for implementing this alternative. It is estimated that it would cost NRC $75,000, assuming a 0.5 staff-month effort per plant, to review the design modifications.

(c) Value Impact

This alternative is considered viable, considering that a moderate safety benefit can be gained and considering the potentially low cost of modifying the existing designs.

(2) Improve operator procedures for manually depressurizing the primary system following an SBLOCA.

This alternative would specify to those utilities that were operating plants with low-head, high-pressure injection pumps having limited discharge flow capacities at pressures greater than or equal to 1275 psi, to revise their emergency procedures and operator training programs to ensure that the operators can safely depressurize the secondary (steam) system via the atmospheric dump valves or the turbine bypass valves and can cool the plant down during any SBLOCA. This preferred cooldown via the secondary system would, in turn, depressurize the primary system. The primary PORV would provide additional backup. The procedure should clearly describe any transfers the operator performs in the event that a loss of instrument air or loss of electric power prevents manual operation of the valves. The use of the pressurizer PORVs and spray valves to depressurize the plant during an SBLOCA and to ensure that the R_TNDT limits are not compromised should also be clearly described.

(a) Safety Benefit

In NUREG/CR-3958, the safety benefit of such improved procedures was estimated. The estimated reduction in the frequency of core melt is 8×10^{-6} per reactor-year. The estimated risk reduction is 850 man-rem over the life of the plant.

(b) Cost

The cost of revising both procedural changes and operator training programs to implement the alternative is not expected to exceed $10,000 per plant. Seven plants (Calvert Cliffs Nuclear Power Plant, Units 1 and 2; Fort Calhoun Station, Unit 1; Millstone Nuclear Power Station, Unit 2; Palisades Nuclear Plant Unit 1; and St. Lucie Plant, Units 1 and 2) use high-pressure, safety-injection pumps that have discharge heads less than or equal to 1275 psi. It is estimated to cost utilities no more than a total of $70,000 to implement this alternative. No NRC staff costs are anticipated.

(c) Value Impact

This alternative is considered viable, considering the moderate safety benefit that can be gained and the very low cost to implement this alternative.

5 SUMMARY OF ALTERNATIVES

Table 5.1 summarizes the alternatives considered during this study.

Table 5.1 Summary of Alternatives

Alternative	Estimated risk reduction		Cost		Is option viable?
	Core-melt frequency (plant-year)	Man-rem (30 years)	Per plant	Utility total	
For GE BWR Plants					
1. Upgrade overfill protection from 2-out-of-3 to 2-out-of-4	6×10^{-7}	123	$150K $13M	$3M-$13M	No
2. Upgrade overfill protection to a reference plant design (i.e., (2-out-of-3)	-	45-123	$150K- $1.3M	$1.2M- $10M	No
3. Upgrade plants with no overfill trip to a 1-out-of-1 or better (2-out-of-4)	-	3600-3800	$100K- $150K	$100K- $500K	Yes*
4. Issue information letter regarding results and assumption of overfill protection	-	-	None	None	Yes
For W PWR Plants					
1. Provide automatic shutoff of AFW on steam generator, high-water level	6×10^{-8}	9	$45K	$2.3M	No
2. Issue information letter regarding results and assumptions of overfill protection	-	-	None	None	Yes
3. Upgrade overfill protection from 2-out-of-3 to 2-out-of-4	$<1 \times 10^{-10}$	Insignificant	$250K- $1.3M	$8M- $24M	No

*For instrumentation only. If additional isolation valves are needed to replace or modify the existing valves, the cost would be substantially greater.

Table 5.1 (Continued)

Alternative	Estimated risk reduction		Cost		Is option viable?
	Core-melt frequency (plant-year)	Man-rem (30 years)	Per plant	Utility total	
4. Upgrade overfill protection (except) for three very early plant designs)	-	-	-	-	No
5. Provide automatic closure of steam block valves					
Case 1 - For steam dump to condenser	$<1 \times 10^{-10}$	Insignificant	$65K*	$3.4M*	No
Case 2 - For atmospheric dump	1×10^{-7}	20	$123K-$1.2M	$6.5M - $37M	No
6. Modify ADV controller logic	1.5×10^{-7}	20	$123K-$1.2M	$6.5M - $37M	No
7. Upgrade pressurizer PORV system	-	-	-	-	No
8. Issue information letter on potential overpressure vulnerabilities	-	-	None	None	No
9. Issue information letter on control system failures that could exacerbate SGTR	1×10^{-8}	2	None	None	No

*For instrumentation only. If additional isolation valves are needed to replace or modify the existing valves, the cost would be substantially greater.

Table 5.1 (Continued)

Alternative	Estimated risk reduction: Core-melt frequency (plant-year)	Estimated risk reduction: Man-rem (30 years)	Cost: Per plant	Cost: Utility total	Is option viable?
For B&W PWR Plants					
1. Test overfill protection system monthly	3×10^{-6}	450	$100K	$300K	No**
2. Test overfill protection system monthly and provide logic modification	7×10^{-6}	1000	$200K	$600K	Yes**
3. Upgrade overfill protection					
Case 1 - Provide an additional independent feedwater flow termination	9×10^{-6}	1300	$100K - $1.1M	$300K - $3.9M	Yes**
Case 2 - Provide a 2-out-of-3 or a 2-out-of-4 system	8×10^{-6}	1200	$300K - $600K	$1M - $2M ($5M max.)	Marginal**
4. Upgrade overfill protection on plants that provide redundant overfill protection	-	-	None	None	No
5. Provide automatic initiation of AFW to minimize loss of steam generator cooling on loss of blast power	2×10^{-6} to 9×10^{-6}	155 - 870	$150K	$450K	Yes**

**Applicable to Oconee plants.

Table 5.1 (Continued)

Alternative	Estimated risk reduction		Cost		Is option viable?
	Core-melt frequency (plant-year)	Man-rem (30 years)	Per plant	Utility total	
For CE PWR Plants					
1. Provide automatic overfill protection (feedwater pump or feedwater isolation valve closure trip)	4×10^{-6}	570	<$100K	$1.5M	Yes
2. Improve operator procedures to permit safe shutdown following an SBLOCA	8×10^{-6}	850	$10K	$70K	Yes

6 PROPOSED RESOLUTION OF USI A-47

The following alternatives represent recommended actions for resolution of unresolved Safety Issue A-47. Appendix C details the control system design and procedural modification for resolving USI A-47.

6.1 GE BWR Plant Designs

(1) Upgrade plant designs with no automatic reactor vessel overfill protection to a 1-out-of-1 (or better) reactor vessel, high-water-level, feedwater-trip system (except Big Rock Point and LaCrosse plants).

(2) Modify technical specifications on all plants to include provisions to periodically verify the operability of the overfill-protection system and ensure that automatic overfill protection is provided during power operation.

(3) Issue an information letter to all applicants and licensees informing them of the results of the overfill analysis. Because design variations exist in individual plants (e.g., in the overfill trip logic, in the power supplies for the trip logic, in operator training, in plant procedures, and in the design of plant alarms and indication systems), the failure rate estimates for the initiating events assumed in the staff's evaluation may vary from plant to plant. The information letter would allow individual applicants and licensees to assess the consequences of overfill transients on their plants.

6.2 W PWR Plant Designs

(1) Take no action to upgrade existing main feedwater, overfill-protection systems on plants that have installed redundant, steam generator, high-water-level, overfill-protection systems consisting of 2-out-of-3 (or better), steam generator, high-water-level, feedwater-trip, isolation system.

(2) Modify technical specifications on all plants to include provisions to periodically verify the operability of the overfill-protection system and ensure that automatic overfill protection is provided during reactor power operation.

(3) Take no action to upgrade existing reactor, overpressure systems.

(4) Issue an information letter to all applicants and licensees informing them of the results of the overfill analysis. Because plant-specific differences exist (described in item 6.1(3) above), failure-rate estimates for initiating events assumed in the staff's evaluation may differ from plant to plant. The information letter would allow individual applicants and licensees to assess the consequences of potential, overfill transients.

6.3 B&W PWR Plant Designs

(1) Modify plants that are similar to the reference plant (i.e., Oconee 1, 2, and 3) to eitner:

(a) Provide additional instrumentation to limit or terminate main feedwater flow on steam generator, high-water level. The instrumentation should be separate from the existing main feedwater pump, trip instrumentation. A system that initiates closure of main feedwater isolation valves on steam generator, high-water level is acceptable; or

(b) Modify the existing overfill protection system to minimize undetected failures in the system and facilitate online testing; or

(c) Upgrade the existing overfill protection system to a redundant high-water-level, trip system that satisfies the single-failure criterion for overfill protection. A 2-out-of-4, steam generator, high-water-level, trip system activating redundant, main feedwater isolation equipment is acceptable.

(2) Plants similar to the reference plant (i.e., Oconee 1, 2, and 3) should install Class 1E instrumentation to automatically initiate auxiliary (emergency) feedwater to minimize the potential for loss of steam generator cooling (including during a loss-of-control-power event).

(3) Take no action on other plants that have installed or have committed to install an emergency feedwater initiation and control (EFIC) system (or its equivalent) incorporating a redundant, steam generator, high-water-level, overfill protection.

(4) Modify technical specifications on all plants to include provisions to periodically verify the operability of the overfill-protection system and ensure that automatic overfill protection is provided at all times during reactor power operations.

(5) Issue an information letter to all applicants and licensees informing them of the results of the overfill analysis.

6.4 CE PWR Plant Designs

(1) Modify all plants to provide additional instrumentation to terminate main feedwater flow on steam generator, high-water level. The instrumentation should provide sufficient redundancy and satisfy the single-failure criterion for overfill protection.

(2) Modify technical specifications on all plants to include provisions to periodically verify the operability of the overfill-protection system and ensure that automatic overfill protection is provided during reactor operation.

(3) Reevaluate plant designs similar to the reference plant (i.e, Calvert Cliffs Nuclear Power Plant, Units 1 and 2; Fort Calhoun Station, Unit 1; Millstone Nuclear Power Station, Unit 2; Palisades Nuclear Plant, Unit 1; and St. Lucie Plant, Units 1 and 2) to modify, if necessary, their

emergency procedures and operator training program to ensure that the operators can safely shut down the plant during any SBLOCA utilizing the ADVs or the TBVs. The reassessment should ensure that a single failure would not negate the operability of the valves needed to achieve safe shutdown.

(4) Issue an information letter to all applicants and licensees informing them of the results of the overfill analysis.

emergency procedures and operator training program to ensure that the operators can safely shut down the plant during any SBLOCA utilizing the ADVs or the TBVs. The reassessment should ensure that a single failure would not negate the operability of the valves needed to achieve safe shutdown.

(4) Issue an information letter to all applicants and licensees informing them of the results of the overfill analysis.

7 APPLICATION OF THE BACKFIT RULE, 10 CFR 50.109

The staff finds that the supporting analyses documented in this regulatory analysis comply with the provisions of 10 CFR 50.109. The following information is provided in answer to the specific requirements in paragraph (c) of 10 CFR 50.109.

(1) Statement of specific objectives that the proposed backfit is designed to achieve.

The specific objective of the proposed A-47 actions identified in Section 6 is to enhance the safety of operating nuclear power plants by:

(a) minimizing the potential for water ingress into the steamlines, thereby decreasing the potential to damage the main steamline or the equipment associated with the steamlines (such as valves, pumps, and sensing lines);

(b) minimizing the potential for a loss of steam generator cooling under any condition of operation that could cause a significant reduction in flow of main feedwater;

(c) ensuring that the operators can safely depressurize the primary system and cool down the plant during any small-break, loss-of-coolant accident.

(2) General description of the activity that would be required by the licensee or applicant in order to complete the backfit.

The resolution of USI A-47 is based mainly on providing:

(a) or upgrading existing control systems to ensure automatic overfill protection of the main steamlines in the event of a main feedwater, overfeed transient, and to periodically verify its operability to ensure that overfill protection is operable at all times during reactor operation;

(b) automatic initiation of auxiliary (emergency) feedwater under any condition of operation that results in a significant reduction in the main feedwater flow;

(c) a reevaluation and modification, if necessary, of selected CE plant emergency procedures and operator training to ensure that operators can safely depressurize the primary system (via the atmospheric dump valves or the turbine bypass valves) and cool down the plant during any small-break, loss-of-coolant accident.

(3) Potential change in the risk to the public from the accidental offsite release of radioactive material.

Quantifying the net safety benefit in terms of risk for requiring technical specifications to include periodic verification of overfill-protection operability proved to be impractical. Justification for the technical specification requirement is based on the fact that overfill protection is needed to mitigate a design-basis accident (DBA) (i.e., feedwater malfunctions that result in increased feedwater flow). This requirement is consistent with the proposed Commission policy statement of what is needed in technical specifications.

The safety benefit for providing an upgrading existing, automatic, overfill protection for different NSSS vendors and the safety benefits for the other proposed requirements are estimated and discussed in Section 4 of this report. They are also summarized below.

For GE BWR plants, design change to upgrade existing, overfill-protection systems does not significantly reduce risk. Modifications to only one plant that does not have any overfill protection (i.e., Oyster Creek) is however warranted. It is estimated that providing automatic, overfill protection can potentially result in reducing the risk by as much as 3600 man-rem over plant life.

For Westinghouse plants, changes to upgrade existing, overfill-protection systems from a 2-out-of 3 to a 2-out-of 4 steam generator, high-water-level trip does not significantly reduce risk. Modification to two plants that do not have any overfill protection is, however, warranted

For Babcock and Wilcox plants, upgrading overfill protection on three plants (i.e., Oconee 1, 2, and 3) is warranted. The estimated risk reduction to provide additional redundancy in the existing, overfill-protection system could be as much as 1200 to 1300 man-rem over the plant life for each of the three plants.

To provide automatic initiation of auxiliary (emergency) feedwater on loss of, or significantly reduced, main feedwater flow, the risk reduction is estimated to be between 155 to 870 man-rem over the life of the plant for each of the three Oconee plants that warrant a design modification.

For Combustion Engineering plants, the risk reduction to provide automatic overfill protection is estimated to be 570 man-rem over the life of each plant.

To improve operating procedures on CE plants to manually depressurize the primary system following an SBLOCA, an estimated risk reduction of 850 man-rem over the life of each plant is estimated.

(4) Potential impact of radiological exposure of facility employees.

No estimate was made. However, it would add to the estimated public risk given in Section 4 of this report. Modifications could be made during plant shutdown, thereby reducing radiological exposure to employees.

(5) Installation and continuing costs associated with the backfit, including the cost of facility downtime or the cost of construction delay;

The estimated costs to the licensees for complying with the proposed resolutions of USI A-47 are presented in Section 4 of this report and are summarized below. The cost of facility downtime is not included in the estimates. The implementation schedule will be negotiated with the licensees in accordance with the NRC policy on integrated schedules for plant modifications stated in Generic Letter 83-20, dated May 9, 1983. The proper integration of the proposed work scope into each plant's schedule may allow for the modifications to be conducted during plant outages.

For BWRs, the cost to incorporate overfill protection on Oyster Creek is estimated at $100,000. For a more versatile design that facilitates online testing and repair, the estimated cost is $500,000. The cost to incorporate testing requirements into the technical specifications is about $15,000 per plant. It should be noted that most BWR plants that comply with the Standard Technical Specifications already incorporate testing of overfill protection.

For Westinghouse plants, most technical specifications incorporate testing of overfill protection. The estimated cost to incorporate the testing requirements into the technical specifications for the remaining plants is $15,000 per plant.

For Babcock and Wilcox plants, the cost to upgrade the Oconee overfill protection systems is estimated to be $100,000 per plant. For a more versatile design that incorporates more redundancy, the estimated cost is $600,000 per plant. If additional penetrations are needed to complete the modifications, an additional $1,000,000 per plant is needed. The estimated cost to incorporate testing requirements into the technical specifications is $15,000 per plant. The cost to provide automatic initiation of auxiliary (emergency) feedwater on the three Oconee plants is estimated not to exceed $150,000 per plant.

For Combustion Engineering plants, the cost to provide automatic overfill protection is estimated to be $100,000 per plant. It was assumed that existing instrumentation to generate the high-water-level signal and existing motor-operated feedwater isolation valves could be used, and that existing penetrations and cabinets can be utilized. The estimated cost to incorporate testing requirements into the technical spefications is $15,000 per plant. The cost to reassess and modify, if necessary, the emergency procedures and operator training to ensure that the operator can safely shut down the plant during any SBLOCA is estimated not to exceed $10,000 per plant.

(6) The potential safety impact of changes in plant or operational complexity including the relationship to proposed and existing regulatory requirements.

None.

(7) The estimated resource burden on the NRC associated with the proposed backfit and the availability of such resources.

The cost to the NRC for implementing the proposed resolution of USI A-47 is estimated and discussed in Section 4 of this report.

The principal cost to NRC would be the cost for reviewing the designs submitted by the individual licensees. It is estimated that a review of 22 plant design modifications and a review of the emergency procedure modifications on 7 plants would be needed. It is estimated that 0.5 staff-month will be needed to review each of these changes, for a total expenditure of 14.5 staff-months. In addition, it would require 0.1 staff-month per plant to verify the modified technical specification, for a total expenditure of 12 staff-months. At an estimated rate of $120,000 per staff-year, the total cost would be $265,000.

(8) The potential impact of differences in facility type, design, or age on the relevancy and practicality of the proposed backfit.

The proposed backfit is plant specific. Differences in facility type design or age have been considered.

(9) Whether the proposed backfit is interim or final and, if interim, the justification for imposing the proposed backfit on the interim basis.

The proposed backfit represents the final staff position on USI A-47.

The proposed method of implementation is issuance of a generic letter under the provisions of 10 CFR 50.109. The staff is recommending implementation through issuance of a generic letter rather than through a standard review plan revision or issuance of a regulatory guide because the proposed requirements apply only to the operating plants. The more-recent plant designs incorporate improvements that embody the proposed requirements. It is recommended, however, that the appropriate sections in the standard review plan be revised to reflect the staff requirements (as discussed in the generic letter) for future plants.

8 REFERENCES

Bernero, R., NRC, Memorandum to T. Speis, April 30, 1985, "Generic Issue 70, PORV and Block Valve Reliability - Task Action Plan (TAC 5526)."

Denton, H., NRC, Memorandum to R. Bernero, July 23, 1985, "Schedule for Resolving and Completing Generic Issue No. 94, Additional Low-Temperature Overpressure Protection for Light Water Reactors."

Institute of Electrical and Electronics Engineers, Standard 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," 1971.

Tucker, H. (Chairman-BWOG), Letter to D. Crutchfield, NRC, May 15, 1986, "B&W Owners Group Plant Reassessment."

U.S. Nuclear Regulatory Commission, Generic Letter 83-20, "Integrated Scheduling for Implementation of Plant Modification at Duane Arnold," May 9, 1983.

---, NUREG-0371, Vol. 1, No. 1, "Approved Category A Task Action Plans," November 1977.

---, NUREG-0737, "Clarification of TMI Action Plan Requirements," November 1980.

---, NUREG-0748, Vol. 4, No. 8, "Operating Reactors Licensing Actions Summary," October 1984.

---, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR Edition, July 1981.

---, NUREG-0844 (Draft for Comment), "NRC Integrated Program for Resolution of Unresolved Safety Issues A-3, A-4, and A-5 Regarding Steam Generator Tube Integrity," April 1985.

---, NUREG-1032 (Draft for Comment), "Evaluation of Station Blackout Accidents at Nuclear Power Plants," May 1985.

---, NUREG-1195, "Loss of Integrated Control System Power and Overcooling Transient at Rancho Seco on December 26, 1985," February 1986.

---, NUREG-1217 (Draft for Comment), "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants, Technical Findings Related to Unresolved Safety Issue A-47," April 1988.

---, NUREG/CR-3568 (PNL-4646), "A Handbook for Value-Impact Assessment," Pacific Northwest Laboratory, December 1983.

---, NUREG/CR-3958 (PNL-5767), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.

---, NUREG/CR-4385 (PNL-5543), "Effects of Control System Failures on Transients, Accidents and Core-Melt Frequencies at a Westinghouse Pressurized Water Reactor," November 1985.

---, NUREG/CR-4386 (PNL-5544), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a Babcock and Wilcox Pressurized Water Reactor," December 1985.

---, NUREG/CR-4387 (PNL-5545), "Effects of Control System Failures on Transients, Accidents, and Core-Melt Frequencies at a General Electric Boiling Water Reactor," December 1985.

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

---, Office for Analysis and Evaluation of Operational Data, "AEOD Observations and Recommendations Concerning the Problem of Steam Generator Overfill and Combined Primary and Secondary System Blowdown," December 17, 1980.

---, Office of Inspection and Enforcement, IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control System Bus During Operation," November 30, 1979.

---, Office of Inspection and Enforcement, Information Notice 80-70, "Reliance on Water Level Instrumentation With Common Reference Leg," September 4, 1984; Supplement 1, August 26, 1985.

Westinghouse Corp., WCAP-10797, "Westinghouse Comments on EG&G Idaho, Inc., Report - Effects of Control System Failures on Transients and Accidents at a 3-Loop Westinghouse Pressurized Water Reactor (August 1984)," February 1985.

APPENDIX A

REJECTED ALTERNATIVES

In this appendix are discussed other alternatives that were considered for possible regulatory action but were rejected because the risk reduction in implementing these alternatives was extremely small.

GE BWR Plant Designs

Several alternatives were considered that could minimize potential failures (e.g., pipe cracks, leaks) in the primary sensing lines of the common reference leg of the reactor vessel, water-level instruments associated with the vessel, overfill-protection system. They include:

(1) Inspect the instrument sensing lines annually.
(2) Replace the existing sensing lines with stronger materials.
(3) Provide independent sensing lines for each vessel, water-level instrument associated with the vessel, overfill-protection system.

Reactor vessel, water-level, primary-sensing-line installations on all BWR plants were not reviewed. A review of the overfill-protection, logic systems on other plants (Table A1), however, determined that most BWR designs (18 to 20 plants) provide a 2-out-of-3, high-water-level, main-feedwater-trip system similar to the reference plant. The staff finds that the installation of the water-level instruments on these other plants is also similar, so that 2-out-of-3, water-level instruments have a common, reference leg.

Considering the very small reduction in the overall risk and the substantial cost in implementing these alternatives however, it was determined that implementing such alternatives is not practical.

It should be noted that IE Information Notice 80-70 was issued to all nuclear reactor facilities holding an operating license or a construction permit. This notice alerted the utilities to the potential degradation of safety associated with operator reliance on water-level instruments that share a common, reference leg. Recipients were expected to review the information for applicability to their own plants and to consider actions, if appropriate, to prevent problems occurring at their own facilities.

Two additional alternatives summarized in this section were also considered, but were rejected on the same basis (i.e., very small, risk-reduction estimates associated with implementing these alternatives). These alternatives were considered in order to minimize reactor vessel overfill via the condensate system or via the low-pressure coolant injection (LPCI) or the core-spray system (CSS). They include:

(1) Provide automatic isolation of condensate flow on reactor vessel, high-water level.

(2) Provide automatic trip of the LPCI or the CSS on reactor vessel, high-water level.

These alternatives were rejected because implementing such automatic-trip features could cause other potentially significant problems that could reduce the reliability of the condensate-feedwater system during startup or shutdown operation or negate the LPCI and the CSS safety function, if required.

W PWR Plant Designs

Several alternatives similar to those discussed for the GE BWR plant designs were considered for the W PWR plants. They include:

(1) Inspect the instrument-sensing lines annually.
(2) Replace the existing, primary, sensing lines with stronger materials.

As in the case of the GE design, the estimated high cost and very small reduction in risk associated with implementing these alternatives precluded them from serious consideration.

Several other alternatives to minimize overpressure events were also considered. In these cases, however, the failure scenarios contributing to the events were caused by multiple, independent failures of such low probability that the overall risk associated with these scenarios is insignificant and implementing these alternatives is not considered practical. These alternatives are summarized below.

(3) Provide independent power sources to the letdown valve and to the pressurizer PORVs.

A single loss of power to the letdown valve and to one pressurizer PORV was identified as a dominant failure that could potentially contribute to a reactor-coolant-pressure transient during low-temperature and pressure shutdown or startup operating conditions. An additional independent failure in the second pressurizer PORV, however, would be needed to cause an overpressure transient. Because all of the pressurizer PORV designs (including the reference plant) are designed to conform to NRC Branch Technical Position RSB 5-2 (NUREG-0800), similar failure scenarios with similar initiating frequencies identified in the review of the reference plant could occur at other W plants. Some new plants have improved the reference plant design by providing separate Class 1E power to each of the PORVs.

Such designs could further reduce the initiating frequency of the identified failure scenarios, thereby further reducing the overall risk contribution of this event.

It should be noted that during certain periods plants are allowed to operate under limited conditions for operation (LCOs), where one, redundant, pressurizer PORV may be rendered inoperable for a limited period of time. Under these conditions, if the system is subjected to a pressure transient (such as the one identified in this review), the plant is vulnerable to an overpressurization event. A single failure in the available, pressurizer, PORV system can render

the overpressure-protection system inoperable. This concern and additional low-temperature, overpressure-protection concerns for light-water reactors are being evaluated separately under Generic Issue 94 (Denton, July 23, 1985). Any requirements resulting from that study will be furnished at the completion of that activity.

(4) Provide positive indication of low-temperature, low-pressure, mode switch, position selection.

A failure to properly realign the setpoints in the pressurizer PORV control logic when transferring from normal operating mode to the cold-shutdown mode or vice versa was identified as a potential common-mode failure that could prevent both pressurizer PORVs from opening when required. This alternative would provide an indicator light for each switch position, allowing positive indication of the circuit connection in each pressurizer PORV's control logic. A failure of the pressurizer PORVs to open because of incorrect setpoint setting would then need both a switch failure and an operator failing to notice an improper connection. This alternative was considered to minimize system failures that could lead to an overpressure event during cold-shutdown conditions. Similar failure scenarios with similar initiating frequency could occur at other W plants. A large number of plant designs, however, offer additional improvements over the reference plant design. This improvement is by way of overpressure-relief capability through the RHR system during the low-temperature operation of shutdown. This overpressure-relief capability allows more time for the operator to respond to overpressure events, resulting in less-severe transients than postulated for the reference plant. As a result of a low-temperature, overpressurization event at Turkey Point Plant, Unit 4, in 1981, the staff is reevaluating the adequacy of this RHR overpressure relief capability (Denton, July 23, 1985). Any requirements resulting from that study will be furnished when that study is complete.

(5) Modify the pressurizer PORV control circuitry to reduce the frequency of component failures that could lead to overpressure events.

The potential negative effects of increasing the complexity of the existing control circuits is not considered a practical alternative.

(6) Modify the high-pressure, safety-injection system.

Additional enable circuits were considered to prevent spurious initiation of the injection pumps during low-temperature startup or shutdown conditions.

It was estimated that a plant was vulnerable to overpressure transients during low-temperature and low-pressure conditions for a few hours during each cool-down/heatup sequence when the PORV setpoint is switched to the higher setpoint, thus restricting the operation of the PORV to a much higher, pressure-relief capability.

In addition to the low-risk contribution of such an event, the possible adverse consequences of reducing the reliability of the safety-injection system by implementing this alternative could significantly affect the overall safety of the plant. This alternative is, therefore, not considered a viable option.

(7) Modify the manual safety-injection, actuation switches.

This alternative was considered to minimize operator error that could lead to overpressure events as a result of a single action during startup or shutdown conditions.

The present design has two switches in parallel; either switch is capable of initiating safety injection. The present design ensures that the failure of a single switch would not prevent actuation of the safety-injection system.

In addition to the low-risk contribution of such an event, the staff believes that changing the switch logic to actuate both switches to initiate safety injection would increase the potential for the safety-injection system to fail. This failure could be more detrimental to plant safety. Changing the logic of the manual switches would presume that inadvertent actuation of the safety injection system presented a greater safety hazard than failure on demand, which has not been shown to be the case.

Table A1 Reactor vessel overfill protection systems

BWR plants with no automatic, overfill protection

- Big Rock
- LaCrosse
- Oyster Creek

BWR plants with automatic, overfill protection equivalent to or better than the reference plant design

- La Salle 1, 2*
- Shoreham*
- WNP-2*
- Browns Ferry (1, 2, 3)*
- Susquehanna 1, 2*
- Hope Creek 1, 2*
- River Bend 1, 2*
- Nine Mile Point 1, 2*
- Hatch 1, 2*
- Duane Arnold***
- Cooper****
- Grand Gulf**
- Limerick 1, 2**
- Fermi 2**

BWR plants with automatic, overfill protection, but with less independence and reliability than the reference plant

- Dresden 2, 3++++
- Quad Cities 1, 2++++
- Peach Bottom++
- Brunswick 1, 2+++
- Pilgrim+++
- Vermont Yankee+
- Monticello+
- FitzPatrick 1+

* 2-out-of-3, high-water-level trip - separate power supplies
** 1-out-of-2 taken twice - power supply separation unknown
*** 2-out-of-3 high-water-level trip - power supply separation unknown
**** 3-level system - logic and power supply separation unknown
\+ 1-out-of-1 high-water-level feedwater trip
++ 2-out-of-2 high-water-level feedwater trip - separation of power unknown
+++ 2-out-of-2 high-water-level feedwater trip - common power supply
++++ 2-level system - logic and power supply separation unknown

APPENDIX B

SENSITIVITY STUDY FOR REACTOR VESSEL/STEAM GENERATOR OVERFILL SCENARIOS

A number of postulated reactor vessel and steam generator overfill events were evaluated and their contribution to plant risk was estimated. Most overfills of the reactor vessel or steam generator were initiated by failures in the main feedwater control and high-water-level trip circuits. If these events were not terminated by the operator, they could lead to water filling the steamlines and could possibly result in steamline damage or a total steamline failure. A large uncertainty exists concerning this potential and, therefore, a high probability of main steamline break (MSLB) given a spillover of water into the steamlines was conservatively assumed in the analysis summarized in Sections 3 and 4 of the present report.

For overfill events to impact public safety significantly and contribute to risk, the events must at some point make a transition to a main steamline break coupled with failures leading to core melt.

In modeling the risk contribution, dominant accident sequences identified in the probabilistic risk assessments (PRAs) of the reference plant (or PRAs of similar plants if none were available for the reference plant) were modified by estimating the frequency of control system failure-induced overfill transients leading to main steamline break. This frequency is dependent on the estimated frequency of overfeed events initiated by control system failures, the operator's likelihood of manually terminating the event, and by the probability of the main steamline break given an overfill event, for boiling-water reactors (BWRs), or by the probability of a main steamline break and a steam generator tube rupture, for pressurized-water reactors (PWRs).

This appendix evaluates the sensitivity of the overfill event to core-melt frequency and plant risk when these parameters are varied.

The sections that follow discuss the sensitivity analysis for overfill events resulting from control system failures of the main feedwater control system for each of the four nuclear steam supply system (NSSS) vendors.

On the basis of this sensitivity analysis, it is concluded that the probability estimates used for operator action to terminate overfill events and for steamline break accidents given steam generator or reactor vessel overfill are in line with operating experience for precursors to such events. This sensitivity analysis, which uses more-realistic probability estimates (derived from operating experience) for overfill scenarios and steamline damage (given overfill events), supports the proposed staff resolution.

A. General Electric (GE) BWR Plants

The overfill-induced, loss-of-coolant accident (LOCA) frequency P_{LOCA} was calculated using the following relationship;

$$P_{LOCA} = (P_{OF})(P_{OA})(P_{FP})(P_{MSLB})$$

where: P_{OF} = frequency of overfeed events induced by control system failures (based on the reference plant design)

P_{OA} = probability of operator failure to manually terminate an overfeed event

P_{FP} = probability that the main feedwater pump will continue to operate after water enters the steamlines

P_{MSLB} = probability of a main steamline break after water enters the steamlines

The risk contribution was estimated by multiplying the modified dominant LOCA sequences by the appropriate release factors.

The sensitivity to variations in the assumptions for overfeed events and to variations in the conditional probability estimates for main steamline breaks given overfill is discussed below.

The estimated probability of control system, failure-induced, overfill events via the main feedwater and the condensate control system was calculated to be 3.3×10^{-3} events per reactor-year. The actual number of overfill events identified by the licensee event report (LER) search for BWR plants is 6 in approximately 415 reactor-years or 14.5×10^{-3} events per reactor-year. This is 4.2 times greater than the probability calculated from scenarios on control system failure.

The estimated values for the conditional probability of a main steamline break (MSLB) during an overfill event was conservatively assumed to be 0.95 in the analysis summarized in Sections 3 and 4 of the present report. On the basis of a literature search of operating history, there were two events in Europe in the early 1960s in which steamline damage resulted from water entering the steamline. The damage was limited to components mounted on the steamlines (i.e., valve standpipes, instrument connections, etc.); no damage was reported to the main steamline piping. On the basis of actual experience, the conditional probability (of an MSLB occurring during an overfill event) of 0.13 was, therefore, used for all plants (i.e., BWRs and PWRs) as a best estimate (i.e., two events, in which damage occurred, out of a total of 15 overfill events identified); this probability would be 7.3 times smaller than the probability used in the initial estimates.

Utilizing these operating experiences, the overfill-induced LOCA frequency would then be $(14.5 \times 10^{-3})(0.9)(0.13) = 1.88 \times 10^{-3}$ events per reactor-year. This includes failure of the operator to take timely action to terminate the event. This is a factor of 1.5 less than the initial estimate of 2.88×10^{-3} events per reactor-year. Steamline damage was also equated to steamline break

in these estimates. The risk reduction to implement (as a minimum) a single reactor high-water-level trip system on selected plants that do not have any automatic overfill protection would, therefore, be reduced by a factor of 1.5, to a new estimated value of 2400 man-rem over the life of a plant. Cost estimates for the proposed design modification is about $100,000 per plant. Utilizing $1000 per man-rem saved as a guideline, design modifications that approach $2,400,000 would still be justified.

Reducing the conditional probability of an MSLB event given reactor vessel overfill by as much as two orders of magnitude from the initial estimates, the risk reduction would be reduced by a factor of 23 to 157 man-rem over the life of the plant. Even with this sizable reduction in the conditional probability estimates for a steamline break (given overfill) and using overfill frequency estimates that are more in line with operating experience, the proposed staff resolution is still warranted for plants that do not have any automatic overfill protection.

Table B.1 summarizes the sensitivity of the risk estimates to changes in overfill frequency estimates and the probability estimates for MSLB events (given overfill conditions).

B. Westinghouse (W) Plants

In the BWR analysis, vessel overfill leading to an MSLB was the major contributor to risk. In PWRs, however, the core-melt frequency contribution associated with the overfill scenarios with only an MSLB is less significant. The major contributors to core-melt frequency for PWRs are overfill events that lead to an MSLB and a steam generator tube rupture (SGTR). In order to determine the probability for SGTR given a steamline break [P_{SGTR} given an MSLB], the probability estimates addressed as part of the staff's evaluation of USI A-3, A-4, and A-5 were used. These estimates were modified by the MSLB frequencies associated with the overfill-event frequencies developed by this review. The total risk contribution associated with the overfill event scenarios was calculated by the following:

$$\text{Risk} = \left(KP_{OF}\right)\left(P_{OA}\right)\left(P_{FP}\right)\left(P_{MSLB}\right)\left(P_{SGTR}\right)$$

given MSLB where K is the risk contribution estimated for the reference plant and the other terms are as defined previously in this appendix.

The estimated probability of control system, failure-induced, overfill events via the main feedwater control systems was calculated to be 2.7×10^{-8} event per reactor-year. This number is very low because of the highly reliable and redundant trip system that is used by all but three of the oldest Westinghouse-designed plants. This value is not contradicted by actual experience since there have been no identified, overfill events on Westinghouse plants to date. Although there was one overfill event at the Ginna plant in 1982, that event occurred as a result of a steam generator tube rupture, and not because of a control system failure. For the W PWR analysis, the estimated conditional probability of an MSLB during an overfill event was conservatively assumed to be 0.5 compared to a best-estimate value of 0.13 based on actual experiences for all BWR and PWR plants (i.e., 2 plants damaged/15 overfill events). Utilizing this operating experience, the overfill-induced MSLB frequency would be

$(2.7 \times 10^{-8})(0.9)(0.13) = 3.2 \times 10^{-9}$ event per reactor-year instead of 1.2×10^{-8} event per reactor-year used in the initial analysis summarized in Sections 3 and 4 of the present report. That is, the frequency is a factor of 3.75 less than the staff's initial estimates. The risk reduction to improve the existing overfill protection system (i.e., 2-out-of-3, steam generator, high-water-level system) would, therefore, also be reduced by a factor of 3.75. Because of the already insignificant risk reduction estimated for adding an additional independent channel, this additional reduction in risk strengthens the proposed resolution that no action is required to modify the existing W designs for overfill protection.

Even increasing the probability estimates for the overfill frequency by four orders of magnitude, the risk contribution would still not warrant any action and, therefore, would not change the proposed resolution for overfill protection for Westinghouse plants.

Table B.2 summarizes the sensitivity of the risk estimates to changes in overfill frequency estimates and the probability estimates for MSLB events (given overfill conditions).

C. Babcock and Wilcox (B&W) Plants

The methodology used on the Westinghouse plants (Section B) was applied to the B&W analysis. The estimated probability of control system, failure-induced, overfill events via the main feedwater, control systems was calculated to be 6.0×10^{-3} event per reactor-year. The actual number of overfill events identified by the LER search for B&W plants is 3 in approximately 110 reactor years (or 2.7×10^{-2} event per reactor-year). This is 4.5 times the initial estimates used in the analysis summarized in Sections 3 and 4 of the present report.

The probability of an MSLB (given overfill) was initially conservatively assumed to be 0.95. On the basis of actual experience, the best-estimate probability of an MSLB (given overfill) was determined to be 0.13, which is 7.3 times smaller than used in the initial estimates.

Using estimates based on actual plant experience, the overfill-induced LOCA frequency would be $(2.7 \times 10^{-2})(0.13) = 3.5 \times 10^{-3}$ event per reactor-year instead of 5.7×10^{-3} event per reactor-year, or a factor of 1.6 less than the initial estimates. The risk reduction to implement an additional independent feedwater trip on a steam generator, high-water level or to modify the existing design to incorporate a 2-out-of-4, steam generator, high-water-level, feedwater-trip system would therefore be reduced by a factor of 1.6 to 820 man-rem over the life of the plant. This change is not considered significant enough to modify the proposed resolution. Staff cost estimates for the proposed design modification are about $100,000 to $600,000 per plant, depending on which option the utility chooses. On the basis of the modified estimates, design modifications that cost $820,000 would still be justified.

It should be noted that if the probability of an MSLB (given an overfill) was further reduced by as much as 2 orders of magnitude, the risk reduction would not be significant enough to warrant a design change. For a 1-order-of-magnitude reduction in the MSLB probability, however, justification for a design modification would be marginal.

Table B.3 summarizes the sensitivity study.

D. Combustion Engineering (CE) Plants

The methodology used on the W plants (Section B) was also applied to the CE analysis. The estimated probability of control system, failure-induced, overfill events via the main feedwater, control systems was calculated to be 9.0×10^{-3} event per reactor year for one of the two overfill scenarios identified in Sections 3 and 4 of the present report and 4.4×10^{-4} event per reactor year for the other. The actual number of overfill events identified by the LER search for CE plants is 1 in approximately 125 reactor-years (or 8.0×10^{3} event per reactor-year) which was essentially the same as initially estimated for one of the events and 18 times greater than initially estimated for the other event.

The estimated probability of an MSLB (given overfill) was conservatively assumed to be 0.5. On the basis of actual experience, the best-estimate conditional probability of an MSLB (given overfill) was determined to be 0.13. This is 3.85 times smaller than used in staff estimates.

Using estimates based on operating experience, the overfill-induced LOCA frequency for each scenario would then be $(8.0 \times 10^{-3})(0.13) = 1.04 \times 10^{-3}$ event per reactor-year instead of 4.7×10^{-3} event per reactor-year, or a factor of 2.3 less than the initial estimates used in Sections 3 and 4 of the present report. The risk reduction to modify the existing design and incorporate a 2-out-of-4, steam generator, high-water-level, feedwater-trip system would, therefore, be reduced by a factor of 2.3 to a new estimated value of 248 man-rem over the life of the plant. This change is not considered significant enough to modify the proposed resolution. The estimate for this design modification is less than $100,000 per plant. On the basis of these estimates, design modifications that cost $248,000 would still be justified.

It should be noted that if the probability of an MSLB event (given overfill) was further reduced by an additional order of magnitude, the proposed design changes could not be justified.

Table B.4 summarizes the sensitivity of the risk estimates to changes in overfill and MSLB frequencies.

Table B.1 GE plants

Condition	Case 1	Case 2	Case 3
Overfill frequency events per year	3.38×10^{-3}	14.5×10^{-3}*	14.5×10^{-3}*
MSLB probability (given overfill)	9.5×10^{-1}	1.3×10^{-1}*	9.5×10^{-3}
Risk reduction (man-rem/ry)	3600	2400	157
Cost of proposed design fix	$100K	$100K	$100K
Proposed fix warranted	Yes	Yes	Yes

*Operating experience data: Case 1 - initial analysis; Case 2 - modified to reflect operating experience; Case 3 - reducing conditional MSLB failure probability by 2 orders of magnitude.

Table B.2 W plants

Condition	Case 1	Case 2	Case 3
Overfill frequency events per year	2.7×10^{-8}	2.7×10^{-8}	2.7×10^{-4}
MSLB probability (given overfill)	5.0×10^{-1}	1.3×10^{-1}*	5.0×10^{-3}
Risk reduction (man-rem/ry)	$<1.0 \times 10^{-4}$	$<1.0 \times 10^{-4}$	$<1.0 \times 10^{-2}$
Cost of proposed design fix	N/A	N/A	N/A
Proposed fix warranted	No	No	No

*Operating experience data: Case 1 - initial analysis; Case 2 - modified to reflect operating experience; Case 3 - reducing conditional MSLB failure probability by 2 orders of magnitude and increasing overfill frequency estimates by 4 orders of magnitude.

Table B.3 B&W plants

Condition	Case 1	Case 2	Case 3
Overfill frequency events per year	6.0×10^{-3}	2.7×10^{-2}*	2.7×10^{-2}*
MSLB probability (given overfill)	9.5×10^{-1}	1.3×10^{-1}*	1.3×10^{-3}
Risk reduction (man-rem/ry)	1340 to 1170	818 to 696	7.8 to 6.7
Cost of proposed design fix	$100K to $600K	$100K to $600K	$100K to $600K
Proposed fix warranted	Yes	Yes	No

*Operating experience data: Case 1 - initial analysis; Case 2 - modified to reflect operating experience; Case 3 - reducing conditional MSLB failure probability by 2 orders of magnitude.

Table B.4 CE plants

Condition	Case 1	Case 2	Case 3
Overfill frequency events per year	9.0×10^{-3}(OF1) 4.4×10^{-4}(OF2)	8×10^{-3}(OF1)* 8×10^{-3}(OF2)*	8×10^{-3}* 8×10^{-3}*
MSLB probability (given overfill)	5.0×10^{-1}	1.3×10^{-1}*	1.3×10^{-3}
Risk reduction (man-rem/ry)	570	248	2.48
Cost of proposed design fix	$100K	$100K	$100K
Proposed fix warranted	Yes	Yes	No

*Operating experience data: Case 1 - initial analysis; Case 2 - modified to reflect operating experience; Case 3 - reducing conditional MSLB failure probability by 2 orders of magnitude.

APPENDIX C

CONTROL SYSTEM DESIGN AND PROCEDURAL MODIFICATION FOR PROPOSED RESOLUTION OF USI A-47

As part of the resolution of USI A-47, "Safety Implications of Control Systems," the staff investigated control system failures that have occurred, or are postulated to occur, in nuclear power plants. The staff concluded that plant transients resulting from control system failures can be adequately mitigated by the operator, provided that the control system failures do not also compromise operation of the minimum number of protection system channels required to trip the reactor and initiate safety systems. A number of plant-specific designs have been identified, however, that do not provide adequate protection from transients leading to reactor core overheating or reactor vessel or steam generator overfill.

Reactor vessel or steam generator overfill can affect the safety of the plant in several ways: The more-severe scenarios could potentially lead to a steamline break and a steam generator tube rupture. The basis for this concern is the following: (1) the increased dead weight and potential seismic loads placed on the main steamline and its supports should the main steamline be flooded; (2) the loads placed on the main steamlines as a result of the potential for rapid collapse of steam voids resulting in water hammer; (3) the potential for secondary safety valves sticking open following discharge of water or two-phase flow; (4) the potential inoperability of the main steamline isolation valves (MSIVs), main turbine stop or bypass valves, feedwater turbine valves, or atmospheric dump valves from the effects of water or two-phase flow; and (5) the potential for rupture of weakened tubes in the once-through steam generator on B&W nuclear steam supply system (NSSS) plants due to tensile loads caused by the rapid thermal shrinkage of the tubes relative to the generator shell. These concerns have not been adequately addressed in plant designs because overfill transients normally have not been analyzed.

To minimize some of the consequences of overfill, early plant designs provided commercial-grade protection for tripping the turbine or relied on operator action to control water level manually in the event the normal-water-level, control system failed. Later designs, including the most recent designs, provide overfill protection which automatically stops main feedwater flow on vessel, high-water-level signals. These designs provide various degrees of coincident logic and redundancy, to initiate feedwater isolation, and to ensure that a single failure would not inhibit isolation. A large number of plants also provide safety-grade designs for this protection.

On the basis of the technical studies conducted by the staff and its contractors, the staff has concluded that certain actions should be taken by some plants to improve plant safety. These actions are described in the material that follows.

(1) GE Boiling-Water-Reactor Plants

(a) All GE boiling-water-reactor (BWR) plant designs should provide automatic, reactor vessel, overfill protection to mitigate main feedwater (MFW), overfeed events. The design for the overfill-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a reactor, high-water-level signal when required, even if a loss of power, or a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common-mode failures that could disable overfill protection and the feedwater control system, but would still cause a feedwater pump trip, are considered acceptable failure modes.

Plant designs with no automatic, reactor vessel, overfill protection should either:

(i) Upgrade their design by providing a commercial-grade (or better) MFW isolation system actuated from at least a 1-out-of-1 reactor vessel, high-water-level system, or

(ii) Demonstrate that the risk reduction in implementing an automatic, overfill-protection system is significantly less than the risk reduction estimated utilizing a generic plant. In determining the risk reduction, factors such as low plant power and population density should be considered.

In addition, all plants should also reassess their operating procedures and operator training and modify them if necessary to ensure that the operators can mitigate reactor vessel, overfill events that may occur via the condensate booster pumps during reduced pressure operation of the system.

(b) Technical specification for all BWR plants with main feedwater, overfill protection should include provisions to verify periodically the operability of overfill protection and should ensure that automatic, overfill protection to mitigate main feedwater, overfeed events is operable during power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. The technical specifications should include appropriate limiting conditions for operation (LCOs). These technical specifications should be commensurate with the requirements of existing plant technical specifications for channels that initiate protective actions. Plants that have previously approved technical specifications for surveillance intervals and limiting conditions for operation (LCOs) for overfill protection are considered acceptable.

Designs for Overfill Protection

Several different designs for overfill protection have already been incorporated into a large number of operating plants. The following discussion identifies the different groups of plant designs and provides guidance for acceptable designs.

Group I: Plants that have a safety-grade or a commercial-grade overfill protection system initiated on a reactor vessel, high-water-level signal based on a 2-out-of-3 or a 1-out-of-2 taken twice (or equivalent), initiating logic. The system isolates MFW flow by tripping the feedwater pumps.

This design is acceptable, provided that (1) the overfill protection system is separate from the control portion of the MFW control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems and that (2) the plant technical specifications include requirements to periodically verify operability of this system and identify the LCOs. Licensees of plants that already support these design features that have previously been approved by the staff should state this in their response. No additional staff review will be required for plants that fully conform to these guidelines. Licensees that need to modify their design and/or modify their technical specifications to conform to these guidelines should also state this in their response and should provide the modified design and or their modified technical specifications for review.

Group II: Plants that have safety-grade or commercial-grade, overfill-protection systems initiated on a reactor vessel, high-water-level signal based on a 1-out-of-1, 1-out-of-2, or a 2-out-of-2, initiating logic. The system isolates MFW flow by tripping the feedwater pumps.

These designs are acceptable provided conditions (1) and (2) stated for Group I are met. Plant designs with a 1-out-of-1 or a 1-out-of-2, trip logic for overfill protection should provide bypass capabilities to prevent feedwater trips during channel functional testing when at power operation.

Group III: Plants without automatic overfill protection.

The licensee should provide a design to prevent reactor vessel overfill. The adequacy of the design or its exclusion should be justified. The justification should include verification that the overfill protection system is separated from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overfill protection and the feedwater control system, but would still cause a feedwater pump trip are considered acceptable failure modes. The design should be submitted for staff review along with the appropriately modified proposed technical specifications.

(2) Westinghouse-Designed PWR Plants

(a) All Westinghouse plant designs should provide automatic, steam generator, overfill protection to mitigate MFW overfeed events. The design for the overfill protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a reactor, high-water-level signal when required, even if a loss of power, or a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common-mode failures that could disable overfill protection and the feedwater control system, but still would cause the feedwater pumps to trip are considered acceptable failure modes.

(b) Technical specifications for all Westinghouse plants should include provisions to periodically verify the operability of the MFW overfill protection and ensure that the automatic, overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. The technical specifications should include appropriate LCOs. These technical specifications should be commensurate with existing plant technical specification requirements for channels that initiate protective actions. Plants that have previously approved technical specifications for surveillance intervals for overfill protection are considered acceptable.

Designs for Overfill Protection

Several different designs for overfill-protection are already provided in most operating plants. The following discussion identifies the different groups of plant designs and provides guidance for acceptable designs.

Group I: Plants that have an overfill-protection system initiated on a steam generator, high-water-level signal based on a 2-out-of-4 initiating logic which is safety grade or a 2-out-of-3 initiating logic which is safety grade but uses one out of the three channels for both control and protection. The system isolates MFW by closing the MFW isolation valves and tripping the MFW pumps.

The design is acceptable, provided that (1) the overfill protection system is sufficiently separate from the control portion of the MFW control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems, and that (2) the plant technical specifications include requirements to periodically verify operability of this system and identify the LCOs. Licensees of plants that already have these design features and the associated approved technical specifications should state this in their response. No additional staff review will be required for plant designs that conform fully to these guidelines. Licensees that need to modify their design and or their technical specifications to conform fully to these guidelines should also state this in their response and provide their modified design and/or modified technical specifications for review.

Group II: Plants with a safety-grade or a commercial-grade overfill protection system initiated on a steam generator, high-water-level signal based on either a 1-out-of-1, 1-out-of-2, or 2-out-of-2 initiating logic. The system isolates MFW by closing the MFW control valves.

The staff finds that only one early plant falls into this group and, therefore, a risk assessment was not conducted. Considering the successful operating history of the plant regarding overfill transients (i.e., no overfill events have been reported), this design may be found acceptable, provided that (1) justification for the adequacy of the design on a plant-specific basis is provided and (2) technical specifications are modified to include requirements to periodically verify operability of this system and identify the LCOs. As part of the justification, the licensee should include verification that the overfill-protection system is separate from the feedwater-control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so

that a fire is likely to affect both systems. Common-mode failures that could disable overfill protection and the feedwater-control system, but would still cause a feedwater pump trip are considered acceptable failure modes.

Licensees should provide their justification and their modified technical specifications for staff review.

Group III: Plants without automatic overfill protection.

The licensee should provide a design to prevent steam generator overfill. The adequacy of the design or its exclusion should be justified. The justification should include verification that the overfill-protection system is separated from the feedwater-control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overfill protection and the feedwater-control system, but would still cause a feedwater pump trip are considered acceptable failure modes. The design should be submitted for staff review along with the appropriately modified proposed technical specifications.

(3) Babcock and Wilcox-Designed PWR Plants

(a) All Babcock and Wilcox plant designs should provide automatic, steam generator, overfill protection to mitigate MFW overfeed events. The design for the overfill-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a steam generator, high-water-level signal when required, even if a loss of power, or a loss of ventilation, or a fire in the control portion of the main feedwater control system should occur. Common failure modes that could disable overfill protection and the feedwater-control system, but would still cause a feedwater pump trip, are considered acceptable failure modes.

Plants that are similar to the reference plant design (i.e., Oconee Units 1, 2, and 3) should provide a steam generator, high-water-level, feedwater-isolation system that satisfies the single-failure criterion. An acceptable design would be to provide automatic MFW isolation by either (1) providing an additional system that terminates MFW flow by closing an isolation valve in the line to each steam generator (this system is to be independent from the existing overfill protection which trips the main feedwater pumps on steam generator, high-water level) or (2) modifying the existing overfill-protection system to preclude undetected failures in the trip system and facilitate online testing, or (3) upgrading the existing overfill-protection system to a 2-out-of-4 (or equivalent), high-water-level, trip system that satisfies the single-failure criterion.

(b) Technical specifications for all B&W plants should include provisions to periodically verify the operability of overfill protection and ensure the automatic, main feedwater, overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification. Technical specifications should include appropriate LCOs.

Designs for Overfill Protection

Several different designs for overfill protection are already provided on most operating plants. The following discussion identifies the different groups of plant designs and provides guidelines for acceptable designs.

Group I: Plants that provide a safety-grade, overfill-protection system initiated on a steam generator, high-water-level signal based on either a 2-out-of-3 or a 2-out-of-4 (or equivalent), initiating logic. The system isolates main feedwater (MFW) by (1) closing at least one MFW isolation valve in the MFW line to each steam generator and (2) tripping the MFW pumps.

This design is acceptable, provided that (1) the overfill protection system is sufficiently separated from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems. Common-mode failures that could disable overfill protection and the feedwater control system, but still trip the feedwater system are considered acceptable failure modes; and (2) the plant technical specifications include requirements to verify operability of this system periodically and identify LCOs. Licensees of plants that already have these design features and the associated approved technical specifications should state this in their response. No additional staff review will be required for plant designs that fully conform to these guidelines. Licensees that need to modify their design and or modify their technical specifications to conform fully to these guidelines should also state this in their response and provide their modified design and or modified technical specifications for review.

Group II: Plants that have a commercial-grade, overfill-protection system initiated on a steam generator, high-water level based on coincident logic that minimizes inadvertent initiation. The system also isolates MFW by tripping the MFW pumps.

This design may be found acceptable, provided that (1) the overfill-protection system is sufficiently separate from the feedwater control system so that it is not powered from the same power source, not located in the same cabinet, and not routed so that a fire is likely to affect both systems and (2) the design modifications are implemented per the guidelines identified above and that the plant technical specifications include requirements to periodically verify operability of this system and identify LCOs.

Licensees of plants that need to modify their design and or modify their technical specifications or design to conform fully to these guidelines should state this in their response and provide their modified design and technical specifications for review.

Plant designs that provide additional 1-out-of-1 or a 1-out-of-2, trip logic for overfill protection should provide bypass capabilities to prevent feedwater trips during channel functional testing when at power or during hot-standby operation. These technical specifications should be commensurate with existing plant technical specification requirements for channels that initiate protection actions.

Plant designs with no automatic protection to prevent steam generator dryout should upgrade their design and provide an automatic, protection system to

prevent steam generator dryout on loss of power to the control system. Automatic initiation of auxiliary feedwater on steam generator, low-water level is considered an acceptable design (the staff believes that only three B&W plants, i.e., Oconee 1, 2, and 3, do not have automatic, auxiliary feedwater initiation on steam generator, low water level).

On December 26, 1985, an overcooling event occurred at Rancho Seco Nuclear Generating Station, Unit 1. This event occurred as a result of loss of power to the integrated control system (ICS). Subsequently, the B&W Owners Group initiated a study to reassess all B&W plant designs, including, but not limited to, the ICS and support systems such as power supplies and maintenance. As part of the USI A-47 review, failure scenarios resulting from a loss of power to control systems were evaluated and the results were factored into these requirements. However, recommended actions for design modifications, for maintenance, and for any changes to operating procedures (if any) developed for the utilities by the B&W owners group will be coordinated with the NRC staff and provided separately.

D. Combustion Engineering-Designed [illegible]P Plants

(a) All Combustion Engineerig plants should provide an automatic, steam generator, overfill protection to mitigate main feedwater (MFW), overfeed events. The design for the overfill-protection system should be sufficiently separate from the MFW control system to ensure that the MFW pump will trip on a steam generator, high-water-level signal when required, even if a loss of power, or a loss of ventilation, or a fire in the control portion of the MFW control system should occur. Common failure modes that could disable overfill protection and the feedwater control system, but would still cause a feedwater pump trip are considered acceptable failure modes.

(b) Technical specifications for all Combustion Engineering plants should include provisions to verify periodically the operability of overfill protection and ensure that automatic, MFW, overfill protection is operable during reactor power operation. The instrumentation should be demonstrated to be operable by the performance of a channel check, channel functional testing, and channel calibration, including setpoint verification, and by identifying the LCOs. These technical specifications should be commensurate with existing plant technical specifications requirements for channels that initiate protection actions.

(c) All utilities that have plants designed with high-pressure-injection, pump-discharge pressures less than or equal to 1275 psi should reassess their emergency procedures and operator training programs and modify them, as needed, to ensure that the operators can handle the full spectrum of possible small-break, loss-of-coolant accident (SBLOCA) scenarios. This may include the need to depressurize the primary system via the atmospheric dump valves or the turbine bypass valves and cool down the plant during some SBLOCA. The reassessment should ensure that a single failure would not negate the operability of the valves needed to achieve safe shutdown. The procedure should clearly describe any actions the operator is required to perform in the event a loss of instrument air or electric power prevents remote operation of the valves. The use of the pressurizer PORVs to depressurize the plant during an SBLOCA, if needed, and the means to ensure that the R_TNDT (reference temperature, nil ductility transition) limits are not compromised should also be clearly described. Seven plants have

been identified that have high-pressure, injection-pump, discharge pressures less than or equal to 1275 psi that may require manual pressure-relief capabilities using the valves to achieve safe shutdown. They are: Calvert Cliffs 1 and 2, Fort Calhoun, Millstone 2, Palisades, and St. Lucie 1 and 2.

Designs for Overfill Protection

CE-designed plants do not provide automatic, steam generator, overfill protection that terminates MFW flow. Therefore, the utility should provide a separate and independent safety-grade or commercial-grade, steam generator, overfill-protection system that will serve as backup to the existing, feedwater, runback, control system initiated from steam generator, high-water-level sensors. Existing water-level sensors may be used in a 2-out-of-4 initiating logic to isolate MFW flow on a steam generator, high-water-level signal. The utility should submit a proposed design and the associated proposed technical specifications for staff review. The proposed design should ensure that (1) the overfill-protection system is separate from the feedwater-control system so that it is not powered from the same power source, is not located in the same cabinet, and is not routed so that a fire is likely to affect both systems (common-mode failures described above are considered acceptable) and (2) the plant technical specifications include requirements to periodically verify operability of the system and identify the LCOs. The information that should be addressed in the technical specifications is provided above.

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC, add Vol. No., if any)
NUREG-1218

2. TITLE AND SUBTITLE
Regulatory Analysis for Proposed Resolution of USI A-47
Safety Implications of Control Systems
Draft Report for Comment

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: March YEAR: 1988

5. AUTHOR(S)
A. J. Szukiewicz

6. DATE REPORT ISSUED
MONTH: April YEAR: 1988

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Engineering
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Same as 7, above.

11a. TYPE OF REPORT

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)
This report presents a summary of the regulatory analysis conducted by the NRC staff to evaluate the value impact of alternatives for the resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The NRC staff proposed resolution is based on these analyses and the technical findings and conclusions presented in NUREG-1217.

The staff has concluded that certain actions should be taken to improve safety in light-water reactor (LWR) plants. The actions recommended that certain plants upgrade their control systems to preclude reactor vessel/steam generator overfill events and to prevent steam generator dryout, modify their technical specification to periodically verify operability of these systems, and modify selected emergency procedures to ensure plant safe shutdown following a small-break loss-of-coolant accident.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS
Unresolved Safety Issue
A-47
Control Systems
Regulatory Analysis

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

*U.S. GOVERNMENT PRINTING OFFICE: 1988-202-292:80057