123 Main Street
White Plains, New York 10601
914 681.6950
914 287.3309 (Fax)

NewYorkPower Authority

James Knubel
Senior Vice President and
Chief Nuclear Officer

August 15, 2000
JPN-00-028

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001
Attn: Document Control Desk

Subject: James A. FitzPatrick Nuclear Power Plant
Docket No. 50-333
Response to NRC Question Number 6
Regarding the FitzPatrick Suppression Pool

References:

1. NRC letter, G. S. Vissing (USNRC) to J. Knubel dated June 22, 2000 regarding phone call of May 25, 2000.
2. NYPA letter, W. A. Josiger to USNRC dated June 30, 2000 (JPN-00-022) regarding response to NRC questions regarding the FitzPatrick Suppression Pool.

Dear Sir:

The attachments to this letter provide the Authority's response to question number 6 of Reference 1. The answers to the remaining questions were previously submitted as part of Reference 2. This information was originally requested by the NRC staff during a May 25, 2000 telephone conversation with Authority personnel.

The Authority makes no new commitments in this letter. If you have any questions, please contact Ms. C. Faison.

Very truly yours,

Jim Knubel
Senior Vice President and
Chief Nuclear Officer

cc: Next page

A001

cc: w/ att

Regional Administrator
U.S. Nuclear Regulatory Commission
475 Allendale Road
King of Prussia, PA 19406

Office of the Resident Inspector
James A. FitzPatrick Nuclear Power Plant
U.S. Nuclear Regulatory Commission
P.O. Box 136
Lycoming, NY 13093

Mr. Guy Vissing, Project Manager
Project Directorate I
Division of Licensing Project Management
U.S. Nuclear Regulatory Commission
Mail Stop 8 C2
Washington, DC 20555

Attachments:

1. Response to Question 6 of NRC Request for Information dated June 22, 2000

2. New York Power Authority Engineering Report JAF-RPT-MISC-03038, "Licensing & Design Basis Issues Concerning ADS & HPCI," Rev. 1.

Response to Question 6 of NRC Request for Information dated June 22, 2000

Q6. PASNY response and follow-up actions to service information letter (SIL-615). General Electric (GE) suggested that owners of GE Boiling Water Reactors (BWRs) evaluate the following if Automatic Depressurization System is not single failure proof:

(a) Demonstrate that the RHR system has the capacity to maintain the maximum suppression pool temperature below 170 degrees F during events for which High Pressure Coolant Injection (HCPI) is relied upon for long-term operation and reactor depressurization, and that the HPCI pump has adequate Net Positive Suction Head (NPSH) at the maximum calculated temperature, or

(b) Implement modifications to assure that the electrical power, controls and cabling for at least one ADS valve are physically separated from the electrical power, controls and cabling for the remainder of the ADS valves.

Submit only information developed in response to the above items in the SIL. (We are not requesting any modifications or any new evaluation.)

A6. The Power Authority in October 1997 requested General Electric to address questions on the design basis of HPCI and ADS as it pertained to JAF and hypothetical event scenarios involving the High Pressure Coolant Injection system and the Automated Depressurization System. In March 1998, General Electric issued SIL 615 based on the 10 CFR 21 evaluation performed by GE in response to NYPA's questions. The Authority developed an Engineering Report, JAF-RPT-MISC-03038 to address the issues raised by the Authority. This report also performed the evaluation specified in recommendation 1 of SIL 615. The first recommended action of GE SIL 615 states: "1. Review plant licensing bases to determine if consideration of the postulated single failure of the ADS function is appropriate for the plant." The conclusion of the NYPA's report 3038 is that JAF is within the Licensing and Design Basis of the plant and that no credible single failure within the licensing basis will result in the loss of the entire ADS function. Therefore the actions identified in the above question are not required to be addressed for JAF. However as part of the actions being taken by NYPA in response to our evaluation of this issue, analysis are in progress to determine the maximum suppression pool temperature with reliance on HPCI for long term cooling and reactor depressurization. A synopsis of the aforementioned report is provided below.

<u>Engineering Report JAF-RPT-MISC-03038 (From Section 1.0 "Purpose")</u>

Engineering Report JAF-RPT-MISC-03038 discusses hypothetical event scenarios involving the High Pressure Coolant Injection (HPCI) System and the Automatic Depressurization System (ADS). It identifies and summarizes the licensing and design basis issues concerning ADS and HPCI that resulted from consideration of the scenarios, and describes the process for evaluating and resolving these issues. The report clarifies and documents the licensing and design bases of the systems, at least to the extent necessary to resolve the Deficiency Event Reports (DERs) and to correct the Updated Final Safety Analysis Report and other design basis documents.

Engineering Report JAF-RPT-MISC-03038 makes a determination as to whether or not the issues raised concerning ADS and HPCI constitute non-compliance with the licensing and design basis of the plant. It then considers the likelihood of the hypothetical event scenarios.

Response to Question 6 of NRC Request for Information dated June 22, 2000

Engineering Report JAF-RPT-MISC-03038 then determines whether the likelihood is great enough to warrant changes to the plant, beyond what would be required to comply with the licensing and design basis, in order to further increase safety.

JAF-RPT-MISC-03038 Conclusion (From Section 4.0 "Conclusion")

The FitzPatrick plant ADS conforms to its design and licensing basis. The hypothetical scenario evaluated in this report is an insignificant contributor to risk and is outside the licensing basis of the plant. An electrical fault that destroys a wireway is not a single active component failure that is assumed in LOCA analysis. The NRC reviewed and approved the design of the FitzPatrick ECCS and the LOCA analyses of the plant.

Attachment 2 to JPN-00-028

New York Power Authority

Engineering Report JAF-RPT-MISC-03038, Rev. 1
"Licensing & Design Basis Issues Concerning ADS & HPCI"

NEW YORK POWER AUTHORITY
JAMES A. FITZPATRICK NUCLEAR POWER PLANT

LICENSING & DESIGN BASIS ISSUES CONCERNING ADS & HPCI

REPORT NO.: JAF-RPT-MISC-03038

FOR INFORMATION ONLY

PREPARED BY: _____ DATE: 11/12/99

REVIEWED BY: _____ DATE: 11/16/99

APPROVED BY: _____ DATE: 11/16/99

SYSTEM: 00 MISC

QA CAT: —

FILE #: 77-B-0160

COMP. PRINTOUT LOC: _____

© 1999

NEW YORK POWER AUTHORITY
JAMES A. FITZPATRICK NUCLEAR POWER PLANT

LICENSING & DESIGN BASIS ISSUES CONCERNING ADS & HPCI

REPORT NO.: JAF-RPT-MISC-03038

PREPARED BY: Original Signed by J. A. Gray, Jr. DATE: _____

REVIEWED BY: Original Signed by D. Ruddy DATE: _____

APPROVED BY: Original Signed by T. Dougherty DATE: _____

Vapiwala, Vinod

From: Gray, Jack
Sent: Wednesday, December 01, 1999 3:46 PM
To: Vapiwala, Vinod
Cc: Dougherty, Thomas; Ruddy, Daniel
Subject: JAF-RPT-MISC-03038 Rev. 1

Vinod,

The original hard copy of the subject report was hand carried to you today. Please enter into the document control system as appropriate and distribute copies to the following personnel:

J. Knubel / H. Salmon / M. Colomb / R. Deasy / T. Dougherty / D. Ruddy / J. Kelly / G. Thomas / G. Tasick / D. Burch / C. Faision / P. Kokolakis / G. Growchowski / A. Bartlik / P. McLaughlin / K. Charter / R. DenBlyker / J. Gray.

NYO JAF

Thanks.

Jack Gray

Hahn J TRAINING

REVISION SUMMARY SHEET

REV. NO.	CHANGE AND REASON FOR CHANGE
0	• Original issue
1	• Incorporation of additional information, corrections, and resolution of comments

TABLE OF CONTENTS

1.0 PURPOSE 6
2.0 STATEMENT OF THE ISSUES 7
3.0 APPROACH TO RESOLUTION OF THE ISSUES 9
4.0 SUMMARY AND CONCLUSIONS 10
5.0 SINGLE FAILURE CRITERION 13
5.1 Introduction 13
5.2 Summary and Conclusions 13
5.3 Single Failure Regulatory Requirements Applicable to FitzPatrick 14
5.4 FitzPatrick Single Failure Licensing Basis 23
5.5 Fitzpatrick Single Failure Design Basis 30
5.6 Specific Application of Single Failure Requirements to the ADS Wireway 33
6.0 ECCS FUNCTIONAL ANALYSIS 35
6.1 Design Evolution 35
6.2 HPCI/ADS Design Function 36
6.3 Emergency Core Cooling Systems Redundancy and Integrated Operation 38
6.4 Manual ADS/SRV Depressurization 40
7.0 CABLE SEPARATION 46
7.1 Separation & Installation Criteria 46
7.2. Routing of HPCI and ADS Cables 46
7.3. Conformance to Criteria 46
7.4. Containment Electrical Penetration Protection 47
8.0 PIPE BREAKS IN THE HPCI INJECTION PATH 48
9.0 QUALIFICATION OF THE CONDENSATE STORAGE TANK (CST), THE HPCI SUCTION LINE TO THE CST AND THE HPCI TEST RETURN LINE 50
10.0 – HPCI MISSION TIME 52
10.1 Introduction 52
10.2 Safe Shutdown 52
10.3 Original Licensing Basis of the HPCI System 54
10.4 Design Basis of the HPCI System 54
10.5 Industry Standards 55
10.6 HPCI & ADS Mission Times for Environmental Qualification Purposes 55
11.0 OPERATOR ACTIONS 58

TABLE OF CONTENTS

11.1 Technical Specification Requirements 58

11.2 Emergency Procedure Requirements 58

11.3 Operator Actions for Specific Line Breaks 59

12.0 SAFETY ASSESSMENT OF THE HPCI/ADS CONFIGURATION 62

12.1 Conclusion 62

12.2 Probabilistic Analysis 62

12.3 Deterministic Engineering Evaluation 62

13. 0 CONCLUSIONS AND RECOMMENDATIONS 64

13.1 Conclusions 64

13.2 Recommendations 68

14.0 CLOSURE OF DEVIATION/EVENT REPORTS (DERS) 77

14.1 DERs 97-701 & 1763 77

14.2 DERs 98-00999 & 01213 77

14.3 DERs 97-01226 & 01227 78

14.4 DER 98-01873 78

15.0 REFERENCES 79

APPENDIX A 89

APPENDIX B 94

HISTORICAL REVIEW OF FITZPATRICK LOCA ANALYSES 94

Large Break LOCA 95

Small Break LOCA (SBLOCA) 96

ACKNOWLEDGEMENT

Many people contributed their technical expertise, research, or draft input to this report. Others have reviewed and commented on the complete draft. The contributions of the following individuals are gratefully acknowledged. This does not imply their agreement with this report or its conclusions, either in whole or in part.

J. Adamson
A. Bartlik
S. Bischof
K. Brockwell
S. Carretta
J. Ellmers
W. Furnari
H. Chang
J. Circle
M. Harriman
T. Herrmann
N. Mathur
R. Schilling
G. Smith

1.0 PURPOSE

This report discusses hypothetical event scenarios involving the High Pressure Coolant Injection (HPCI) System and the Automatic Depressurization System (ADS). It identifies and summarizes the licensing and design basis issues concerning ADS and HPCI that resulted from consideration of the scenarios, and describes the process for evaluating and resolving these issues. This report clarifies and documents the licensing and design bases of the systems, at least to the extent necessary to resolve the Deficiency Event Reports (DERs) and to correct the Updated Final Safety Analysis Report and other design basis documents.

This report makes a determination as to whether or not the issues raised concerning ADS and HPCI constitute non-compliance with the licensing and design basis of the plant. It then considers the likelihood of the hypothetical event scenarios. The report then determines whether the likelihood is great enough to warrant changes to the plant, beyond what would be required to comply with the licensing and design basis, in order to further increase safety.

Additional issues concerning stratification and uneven heating of the suppression pool are beyond the scope of this report and are being addressed separately.

2.0 STATEMENT OF THE ISSUES

Several Deficiency Event Reports (DERs) were initiated which questioned the design functions and interdependency of ADS and HPCI. As these issues were researched and evaluated, other questions arose and additional DERs were written. The issues ultimately identified for resolution concerning ADS and HPCI are the following:

- the functional relationship of ADS to HPCI (functionally independent and redundant, or mutually dependent)
- the required electrical separation between ADS and HPCI (and if necessary within ADS itself)
- single failures to be postulated coincident with design basis events
- the small break mitigation capability of FitzPatrick ECC systems
- qualification of HPCI including mission times, operating temperatures, and HPCI suction line and Condensate Storage Tank (CST) design and construction
- pipe breaks in the HPCI injection path
- operator manual actions; and,
- documentation of the applicable licensing and design basis criteria.

The first major issue centered on the ability of ADS and HPCI to depressurize the reactor for small break loss of coolant accidents (LOCAs), particularly for breaks in the HPCI injection path with a coincident electrical fault in an ADS wireway. If HPCI and ADS were functionally redundant (i.e. perform identical functions) to each other, either system would have to be able to depressurize the reactor for small breaks. A LOCA/LOOP (loss of offsite power), with an electrical fault which destroys the wireway containing ADS (as the single failure), could make it impossible to depressurize the reactor before HPCI fails due to high suppression pool temperatures. If both HPCI and ADS were unavailable, reactor pressure would increase due to decay heat until one or more SRVs lifted to relieve pressure. This process would continue until the core uncovers and fuel damage results.

Conversely, according to the DERs, if HPCI required the assistance of one or more ADS valves to depressurize, HPCI and ADS would not be functionally redundant. If this were the case, then ADS would need to have redundant divisions; and, the existing arrangement of all ADS cabling in a single wireway would violate the design and licensing basis for cable separation.

These issues led to further questions concerning whether or not wireway failures must be postulated as single failures in LOCA analyses and whether a break could occur in the HPCI injection path that could prevent the entire HPCI flow from reaching the reactor vessel without depressurizing it. Questions were raised concerning the qualification of the Condensate Storage Tanks (CST) and the HPCI suction line to the CST. Other issues arose concerning what operator actions are appropriate and within the licensing basis for reactor depressurization

for small break LOCAs; and, NRC approval of the design and licensing basis of HPCI and ADS for FitzPatrick.

3.0 APPROACH TO RESOLUTION OF THE ISSUES

The issues concerning the licensing and design basis of HPCI and ADS are complex and interrelated. A common process was used to resolve the issues. As each issue was identified a Deficiency Event Report (DER) was completed and the Shift Manager (SM) was informed. As part of the DER process, an operability determination was made for the condition identified in the DER. When necessary, immediate corrective actions were identified and taken. The DER was also reviewed to determine if a report to the United States Nuclear Regulatory Commission (NRC) was required.

The next step was to identify or reconstitute the licensing and design basis requirements of both systems. This was done by reviewing the Code of Federal Regulations (CFR), NRC regulatory guidance documents, design specifications, generic reports and documents filed with the NRC on the FitzPatrick and other dockets. The Updated Final Safety Analysis Report (UFSAR), the Design Basis Document (DBD) for HPCI, and Nuclear Steam Supply System (NSSS) vendor topical reports were also examined.

Once the licensing and design basis was identified, then the event scenarios identified in the DER were reviewed to determine whether or not the existing design and installation of HPCI and ADS met the licensing and design basis. If potential non-conformances were identified, DERs were issued (or revised) to describe the condition and the DER review and evaluation process was re-entered.

Even though the existing design and installation were found to be in conformance with the design and licensing basis, the safety significance of the condition, postulated event or failure was evaluated further. The purpose of this evaluation was to determine if modifications to the plant, procedures or operations should be made to improve safety, even if they were not necessary to conform to the licensing and design basis. It should be noted that this effort went beyond what was required to demonstrate compliance with the licensing and design basis by determining the core damage frequency of the hypothetical scenarios. This is an additional evaluation performed as part of a very conservative approach to safety.

4.0 SUMMARY AND CONCLUSIONS

ISSUES CONCERNING THE AUTOMATIC DEPRESSURIZATION SYSTEM

Several questions have been raised with regard to the licensing and design bases of the Automatic Depressurization and High Pressure Coolant Injection Systems (ADS and HPCI). The principal concern is that the cables for the 7 ADS valves (as well as the remaining 4 SRVs) run in a single wireway and are therefore vulnerable to a single failure.

It has been hypothesized that one of the single failures that must be assumed coincident with a LOCA is an electrical fault that destroys all cables in a wireway. The hypothetical scenario is that a small break LOCA occurs in the HPCI injection path. A coincident electrical fault destroys the entire Division 1 wireway containing the ADS cables and possibly cables for Core Spray, LPCI and suppression pool cooling. Because a significant portion of suppression pool cooling is destroyed, HPCI (which is cooled by suppression pool water) fails due to elevated pool temperature before it can depressurize the reactor. This leaves no way to depressurize the reactor or add water to it, so the core uncovers and fuel damage results.

SUMMARY

ADS and HPCI are redundant high pressure Emergency Core Cooling Systems (ECCS) and are actuated by protection systems as defined in IEEE-279-1968 (i.e. all devices and circuitry from sensors to actuating device input terminals). ADS and HPCI are designed to function in conjunction with Core Spray (CS) and LPCI to automatically provide ECC and achieve safe shutdown in the event of a LOCA with a LOOP plus any single failure. ADS and HPCI perform the redundant high pressure ECCS function of reactor depressurization; i.e. either system is capable of depressurizing the reactor to the point where the low pressure ECCS can cool the core.

The FitzPatrick plant was designed and licensed to automatically achieve safe shutdown following any transient or accident. Safe shutdown was defined for FitzPatrick in the 1967 Draft General Design Criteria as hot shutdown. Hot shutdown is achieved by the insertion of the control rods and preventing or reversing the post accident rise in peak clad temperature (PCT). The increase in PCT has been terminated when the fuel has been covered for three fuel time constants or about thirty seconds. The FitzPatrick plant has met its licensing and design basis of automatically achieving safe shutdown when the control rods have inserted and either HPCI or ADS and a low pressure ECCS has kept the core covered for 30 seconds.

Safe shutdown is attained automatically – with no operator action. All protection system functions necessary for safe shutdown (reactor scram, reactor vessel and containment isolation and emergency core cooling) are automatically initiated and completed without manual action by the operator. The transition from safe (hot) shutdown to cold shutdown (which is called cooldown) assumes and requires manual actions by the reactor operators. These operator actions are assumed to begin ten minutes after the beginning of the accident. The FitzPatrick licensing basis is that once hot shutdown had been achieved with HPCI, the reactor operators would use manual SRV actuation (as required) to proceed to cold shutdown since this is the safest condition following an accident.

Nuclear power plants are licensed to design and analytical requirements. The ECCS are designed and installed in accordance with design requirements and analyzed in accordance with analytical requirements. IEEE-279 is a design standard and requires that protection systems be able to perform their design function (i.e. automatically actuate ECC systems) assuming an active or passive failure within the protection system. 10 CFR 50.46 and Appendix K is an analytical standard and requires that ECCS meet certain performance requirements assuming the failure of a single active component. In affect, the plant is designed and built in accordance with certain design assumptions and analyzed in accordance with different performance or analytical assumptions. Electrical separation is a design and not an analytical requirement.

The ADS and HPCI together meet the requirements of IEEE-279-1968, particularly the requirement to automatically actuate even assuming any active or passive failure in the protection system. ADS alone substantially meets IEEE-279 by itself since the ADS incident detection circuitry and ADS trip systems will generate an ADS actuation signal assuming the single failure. The ADS actuation circuits (from the outputs of the trip system to the actuating device input terminals) do not meet IEEE-279.

FitzPatrick ECCS and LOCA analyses are performed in accordance with 10 CFR 50.46 and Appendix K to 10 CFR 50, including the single failure criterion. This means that the FitzPatrick ECCS will perform their function assuming any single active component failure. (The failure of a battery is considered an active failure.) Wireway failures were considered in the design. The JAF configuration of ADS is different from the configuration in NEDO-10139, but the JAF ADS design has been determined to be as reliable as the NEDO-10139 configuration. An electrical fault that destroys a wireway is not a single active component failure that is assumed in LOCA analyses.

The FitzPatrick licensing basis also requires that safe shutdown be achievable assuming the complete non-deterministic loss of either HPCI or ADS. In the event of an assumed loss of HPCI, ADS will depressurize the reactor until the low pressure ECCS initiate and maintain core cooling. In the event of the assumed loss of the entire ADS, HPCI would provide core cooling and depressurize the reactor until the low pressure ECCS could inject and cool the

core. In this case, two divisions of suppression pool cooling would be available to ensure that the suppression pool temperature would not increase to the point where it would disable HPCI. This report recommends that a calculation be performed to confirm this.

The FitzPatrick ECCS and protection systems were reviewed and accepted by the NRC. The NRC required that the FitzPatrick (as well as the ADS of other BWRs of the same product line) be modified to be more resistant to single failures. The NRC did not require the ADS to have redundant divisions or to be "single failure proof". The NRC SER concluded that the ECCS and ADS were acceptable when compared to IEEE-279. The docketed record demonstrates that the NRC was familiar with the BWR 4 ADS design and was aware of its limitations.

The FitzPatrick ADS design and as-built configuration differs from that referred to in the UFSAR and NEDO-10139 and approved by the NRC. Design engineering is performing a Nuclear Safety Evaluation (NSE) of these differences to ensure that ADS is acceptable as installed.

This report concludes that the ADS meets the design and licensing basis of the plant (pending completion of the NSE referred to above and certain recommendations). However, NYPA performed a probabilistic safety assessment of the as-built ADS that concluded that no modifications are required to improve safety. A LOCA plus a LOOP plus an electrical fault that could destroy an ADS wireway was found to be an insignificant contributor to core damage frequency and several orders of magnitude below that which would require remedial action.

NYPA also commissioned a deterministic engineering evaluation of the ADS wireways to determine their susceptibility to damage or destruction. Based upon this evaluation, NYPA Design Engineering concluded that there is no credible external hazard or credible electrical fault that could prevent ADS from performing its safety function.

CONCLUSIONS

The FitzPatrick plant ADS conforms to its design and licensing basis. The hypothetical scenario evaluated in this report is an insignificant contributor to risk and is outside the licensing basis of the plant. An electrical fault that destroys a wireway is not a single active component failure that is assumed in LOCA analysis. The NRC reviewed and approved the design of the FitzPatrick ECCS and the LOCA analyses of the plant.

5.0 SINGLE FAILURE CRITERION

5.1 Introduction

It was difficult to determine the extent of the FitzPatrick plant's conformance to the single failure criterion (SFC) for many reasons. First, the term "single failure criterion" is loosely used and its definition is subject to interpretation. It is often referred to as "the single failure criterion", "a single failure", or "the single failure". Sometimes all three terms are used. Other terms such as "single active failure", "single passive failure", "single component failure", "passive component failure" and "single active component failure" are also used. These different terms are often used in the same document and are frequently used interchangeably.

Second, the terms are defined or interpreted in many different places including NRC regulations, codes and standards, NSSS vendor topical reports and plant specific FSARs and other licensing documents. These definitions and interpretations have different meanings depending upon the documents that contain them.

Third, the concept of single failure is more than 30 years old and evolved with time. Therefore, the meaning of the term single failure differs depending upon: the revision of the document that contains it; the specific nuclear plant to which it is applied; and, even the specific system within a plant to which it is applied.

Fourth, the failures assumed are different depending on the transient, design basis event or design basis accident being evaluated.

Fifth, although single failure might seem to be a relatively simple concept, it is very difficult to apply to nuclear safety-related systems which are very complex and which have even more complex interconnections and interdependencies. The NRC wrote in a Safety Evaluation Report (SER) for Dresden Station Units 1 & 2 and Quad Cities Station Units 2 & 3 (Ref. 5.1):

> "...The staff notes that the application of the SFC is difficult and ambiguous with respect to interconnected and interacting systems such as the ECCS."

5.2 Summary and Conclusions

This report addresses two single failure criteria: the single failure criterion as applied to protection systems; and, the single failure criterion as applied to LOCA analyses of Emergency Core Cooling Systems (ECCS). These two criteria are different for the FitzPatrick plant. They are defined by the NRC regulations, industry codes and standards and General Electric design standards in effect at the time the plant was designed, constructed and licensed.

The NRC regulation that governs the SFC for protection systems is 10 CFR 50.55a(h). It does not apply to FitzPatrick (and is therefore not part of its licensing basis) as explained in Section 5.3.1.1. The FitzPatrick licensing basis SFC for protection systems is IEEE-279-1968 and, for certain specific modifications, IEEE-279-1971 (See Section 5.4.1). The FitzPatrick plant protection systems meet these requirements.

No single active or passive failure will prevent the integrated operation of the ECCS from providing adequate core cooling (UFSAR 7.4.2.5.a). No single active or passive failure within the incident detection circuitry and trip systems will prevent the generation of an automatic initiation signal for ADS and HPCI. No single active or passive failure within the protection system will prevent the actuation of CS and LPCI. This capability does not apply to, and is not required for, manually initiated systems such as containment cooling.

The NRC regulations that govern the SFC for ECC systems are 10 CFR 50.46 and 10 CFR 50 Appendix K. These regulations do apply to the FitzPatrick plant, and therefore are part of the licensing basis, as described in Section 5.3.1.3. The FitzPatrick plant also meets these requirements. The ADS and HPCI systems meet these requirements together, since they are redundant high pressure ECC systems. HPCI does not meet the single active component failure criterion for LOCA analyses itself, since it has essential components that do not have a redundant counterpart. The ADS system does meet the single active component failure criterion for LOCA analyses by itself, since there are seven ADS valves (not all of which are required to perform the safety function).

5.3 Single Failure Regulatory Requirements Applicable to FitzPatrick

Regulatory requirements that are applicable to a nuclear power plant include NRC regulations; various types of NRC guidance documents; and, the licensing and design basis, which is described in the Updated Final Safety Analysis (UFSAR) and other licensing documents.

5.3.1 Single Failure Requirements of the Code of Federal Regulations

NRC regulations may be applicable to all nuclear power plants, or only plants of a particular design or vintage. Each regulation must be reviewed for its applicability to a particular plant. Although a regulation may not apply directly to a certain plant, that plant may be committed to meet the requirements of the regulation via commitments in the plant's licensing basis.

5.3.1.1. Protection Systems – 10 CFR 50.55a(h) (Ref. 5.27)

The requirement in 10 CFR 50.55a(h) for the design of protection systems to comply with IEEE-279 (the edition or revision in effect on the formal docket date of the construction application) is applicable to plants that received their Construction Permit (CP) after January 1, 1971. The FitzPatrick CP was issued on May 20, 1970. Therefore, the NRC regulation that mandates that protection systems comply with the SFC (as defined in IEEE-279) does not apply to the FitzPatrick plant.

Although 10 CFR 50.55a(h) does not apply to the FitzPatrick plant, a commitment to IEEE-279 is part of the licensing basis. The FitzPatrick plant is committed to, and its protection systems conform to, IEEE-279-1968 (and 1971 for certain modifications to the systems), as described in Sections 5.4 and 5.4.1. (The definition of protection system is stated in Section 5.4.1) Therefore, although 10 CFR 50.55a(h) does not apply, the FitzPatrick plant complies with the regulation.

5.3.1.2. General Design Criteria – 10 CFR 50 Appendix A

The FitzPatrick plant was not specifically licensed to the General Design Criteria (GDC) as described in References 5.28 and 5.29. However, the FitzPatrick plant is committed to portions of the 1967 (draft) and 1971 versions of the General Design Criteria (Refs. 5.2 and 5.3 respectively).

5.3.1.2.1. Draft General Design Criteria – 1967

The NRC published a proposed rule in the Federal Register on July 11, 1967 (Ref. 5.2). The proposed rule included a new Appendix A to 10 CFR 50 which contained General Design Criteria for Construction Permits. The following statement preceded the proposed rule:

> "**The Commission expects that the** provisions of the proposed amendments relating to **General Design Criteria** for Nuclear Power Plant Construction Permits **will be useful as interim guidance** until such time as the Commission takes further action on them." (Emphasis added.)

The proposed rule contained several GDC that dealt with single failures. Draft GDC 20 – Protection Systems Redundancy and Independence stated:

> "Redundancy and independence designed into **protection systems** shall be sufficient to assure that **no single failure** or removal from service **of any component or channel will result in loss of the protection function.**" (Emphasis added.)

GDC 39 – Emergency Power for Engineered Safety Features stated:

> "Alternate power systems shall be provided...to permit the functioning required of the engineered safety features. As a minimum, the **onsite power system and the offsite power system shall each, independently, provide the capacity assuming a failure of a single active component in each power source.**" (Emphasis added.)

GDC 41 - Engineered Safety Features Performance Capability stated:

> "**Engineered safety features** such as emergency core cooling and containment heat removal systems **shall provide ... the required safety function assuming a failure of a single active component.**" (Emphasis added.)

These Draft GDC clearly state that protection systems must provide the protection function with "any single failure" and that onsite and offsite power systems, emergency core cooling systems and containment heat removal systems must provide their safety function "assuming a failure of a single active component".

Although these Criteria were issued as "interim guidance" (Ref. 5.2), they were incorporated into the FitzPatrick licensing basis. The Draft GDC concerning protection systems is met by compliance with the requirements of IEEE-279-1968 (Ref. 5.4) as described in Section 5.4.1. IEEE-279-1968 also provides the definition of protection systems that GDC 20 addresses. The GDC concerning single active component failures was eventually incorporated into NRC regulations 10 CFR 50.46 (Ref. 5.7) and Appendix K to 10 CFR 50 (Ref. 5.8). The FitzPatrick plant meets these requirements as described in Section 5.3.1.3.

5.3.1.2.2. Final General Design Criteria – 1971

The GDC were under development when the United States Atomic Energy Commission (AEC) was reviewing the FitzPatrick application for an Operating License. Section 16.6 of the Updated Final Safety Analysis Report (UFSAR) contains an evaluation of the FitzPatrick plant to the GDC. These GDC became effective on May 21, 1971 – nearly a year after the FitzPatrick construction permit was issued and, about a year and a half after the conceptual design of the plant was complete. This evaluation is very brief and general and does not describe the extent of compliance, or non-compliance, with the GDC. In addition, the evaluation is qualified and limited by the following statement that immediately precedes it:

> "Based on our understanding of the intent of these criteria, it was concluded that the James. A. **FitzPatrick** Nuclear Power Plant **conformed with the intent of the AEC General Design Criteria** for

Nuclear Power Plants **to the maximum extent possible** consistent with the state of design and construction at the time of issuance of these criteria." (Emphasis added.)

GDC 34 – Residual heat removal states:

"A system to remove residual heat shall be provided."

And:

"Suitable redundancy in components and features...shall be provided... to assure that the system safety function can be accomplished, assuming a single failure."

GDC 35 – Emergency core cooling states:

"A system to provide abundant emergency core cooling shall be provided."

And

"Suitable redundancy in components and features...shall be provided... to assure that the system safety function can be accomplished, assuming a single failure."

GDC 38 – Containment heat removal states:

" A system to remove heat from the reactor containment shall be provided."

And

"Suitable redundancy in components and features...shall be provided to assure that...the system safety function can be accomplished, assuming a single failure."

Single failure is defined in 10 CFR 50 Appendix A – General Design Criteria for Nuclear Power Plants (Ref. 5.3) as follows:

"A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions." (Emphasis added.)

A footnote to Appendix A says:

> "Single failures of passive components in electrical systems should be assumed in designing against a single failure. The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single failure are under development".

The Introduction to the GDC states:

> "The development of these General Design Criteria is not yet complete. For example, some of the definitions need further amplification."

And

> " The minimum acceptable redundancy and diversity of subsystems and components within a subsystem, and the required interconnection and independence of the subsystems have not yet been developed or defined. (See Criteria 34, 35, 38, 41, and 44.)"

Essentially what these statements taken together mean is that the specific design presented by each license applicant was reviewed and approved by the AEC or NRC on a case-by-case basis.

The FitzPatrick plant does not meet GDC 34 because the shutdown cooling mode of the Residual Heat Removal System has components which do not have redundant counterparts. It apparently does meet GDCs 35 and 38. The plant should be reviewed and the UFSAR updated to describe the extent of compliance with the 1971 GDC (See Recommendation 13.2. 7).

5.3.1.3 Acceptance Criteria for Emergency Core Cooling Systems – 10 CFR 50.46 and ECCS Evaluation Models - 10 CFR 50 Appendix K

The NRC requires that LOCAs be analyzed in accordance with 10 CFR 50.46 and Appendix K (Refs. 5.7 and 5.8). These rules were preceded by an Interim Acceptance Criteria (IAC) of the AEC (the agency that preceded the NRC). The IAC was published in the Federal Register on June 29, 1971 (36FR12247) and was subsequently amended and published on December 18, 1971 (36FR24082) (Refs. 5.9 and 5.16). The IAC as amended provided criteria for analyzing ECCS LOCA performance. Following extensive rulemaking hearings (Docket No. RM-50-1), the IAC was modified and published as 10 CFR 50.46 and Appendix K.

10 CFR 50.46 (Ref. 5.7) was published on January 4, 1974 and became effective on February 4, 1974. It specifies acceptance criteria for light-water reactor emergency core cooling systems. The five acceptance criteria are specified in

terms of fuel related parameters. They are the peak cladding temperature (PCT); maximum cladding oxidation; maximum hydrogen generation (due to the chemical reaction between the cladding and steam or water); maintaining the core in a coolable geometry; and, long term cooling. The regulation requires the calculation of fuel response to LOCA conditions using an "acceptable evaluation model". 10 CFR 50 Appendix K describes the features of an acceptable model (Ref. 5.8). This regulation was, and still is, applicable to the FitzPatrick plant.

The FitzPatrick plant was initially licensed on October 17, 1974 (for the first core) to the Interim Acceptance Criteria (Ref. 5.9). In the original pre-license plant design, the Low Pressure Coolant Injection (LPCI) system was vulnerable to a single injection valve failure and a single failure in the loop selection logic. The LPCI system was modified in order to eliminate these single failure vulnerabilities and, to be able to meet the acceptance criteria of Appendix K without derating the plant. The NRC reviewed and approved the licensing and design basis of the ECC systems, which was revised with this modification and the application of Appendix K. All subsequent cores have been licensed to the final (1974) 10 CFR 50.46 and Appendix K (Refs. 5.7 and 5.8).

The NRC approvals of the FitzPatrick ECCS are based on General Electric (GE) models and calculations that the NRC has reviewed (for FitzPatrick as well as many other plants). These models were based on the assumption of a single active component failure (including failure of a battery) in an ECC system.

General Electric (GE) published the licensing topical report NEDO-10329 titled "Loss-of-Coolant Accident & Emergency Core Cooling Models for General Electric Boiling Water Reactors" in April 1971 (Ref. 5.17), which described the GE methodology for performing LOCA analyses of both large and small breaks. The AEC Interim Acceptance Criteria of June 29, 1971 specifically endorsed NEDO-10329 and the single failure criterion of the NEDO in the following statement:

> "The combination of systems used for analysis should be derived from a failure mode and effects analysis, using the single failure criteria as indicated in Table 2-1 of the topical report "Loss-of-Coolant Accident and Emergency Core Cooling Models for General Electric Boiling Water Reactors," NEDO-10329."

GE actively participated in the rulemaking hearings, which followed publication of the IAC and resulted in the final rule. On April 16, 1973 the AEC issued the "Concluding Statement of the Regulatory Staff" (Ref. 5.18). The Concluding Statement specified that:

> "The **combination of emergency core cooling subsystems assumed to operate** in analyses **shall be derived** from a failure modes and effects analysis, **using the single failure criteria.**" (Emphasis added.)

The Concluding Statement also stated that NEDO-10329 is an acceptable model for GE BWRs that have jet pumps and use a 7 x 7 fuel array. FitzPatrick has jet pumps and was using 7 x 7 fuel (now obsolete) at the time. FitzPatrick was also explicitly identified in the NEDO. The Concluding Statement also says that the onsite source of electrical power must also be subject to the conservative assumption of the "worst single failure". (Ref. 5.18, page 220)

The AEC Commissioners themselves issued a concurring opinion on the rulemaking (Docket No. RM-50-1) on December 28, 1973 (Ref. 5.19). They affirmed the staff opinion, defined the content of the rule, established an implementation schedule and provided the AEC staff with directions for implementation. The rule stated then, as it does now, that:

> "An analysis of possible failure modes of ECCS equipment and of their effects on ECCS performance must be made. In carrying out the accident evaluation the **combination of ECCS subsystems assumed to be operative shall be those available after the most damaging single failure of ECCS equipment** has taken place." (Emphasis added.)

The AEC requested specific information about the FitzPatrick plant's compliance with the IAC. AEC Question 6.5 in the Original FSAR (Ref. 5.31) says in part:

> "**Provide curves** of peak clad temperature...**for the various combinations of ECC subsystems evaluated by using the single failure criterion** indicated in Table 2-1 of...NEDO-10329. A discussion should be included for the ECC subsystem combinations used in the evaluation." (Emphasis added.)

NEDO–10329 (Ref. 5.17) identifies the FitzPatrick plant and the LOCA model applicable to it (Table 2-1). Given the fact that large break LOCAs are the limiting accidents, they receive most of the attention. The NEDO states that the low pressure systems provide adequate protection for all but very small breaks, for which they require the assistance of the high pressure systems (ADS and HPCI for FitzPatrick). The NEDO goes on to state the following about the ECCS:

> "...**the assumption of single systems operating** (which was done in the bar chart analysis) **is unrealistic** and was simply done to give an idea of the relative protection offered by each of the systems. Thus, the main body of **our analytical effort is directed toward** the more realistic transients involving **combinations of systems.**" (Emphasis added.)

NEDO-10329 also states:

> "Since the purpose of this report is to discuss how analyses are done, the reasons for choosing the combinations of systems for analysis will not be

discussed in detail. At the minimum, the ability to meet the single-failure criterion is demonstrated."

The NEDO provides a table of assumed single failures that are all active components. This table also shows the failure of either HPCI or ADS. It also says, in a footnote to the table, that the high pressure systems (ADS and HPCI) are "additional failures arbitrarily applied to the 1967 Product Line plants." No explanation is given for this statement and the analyses presented in Appendix B of the NEDO are based on the combinations of systems operable after assuming single active component failures. (One possible explanation is that the failure of either ADS or HPCI could be due to the assumption of the failure of the corresponding station battery, which was subsequently added to the FitzPatrick licensing basis by the AEC). As noted above, the AEC approved this NEDO.

A telephone conference call was held between representatives of GE and NYPA on July 30, 1998 (Ref. 5.20). The GE personnel on the call were P. Marriott, G. Sozzi, D. Robare and G. Thacker. These gentlemen have many years of experience in licensing, engineering and power uprate analyses within GE. (Mr. Marriott was formerly Manager, Emergency Core Cooling Systems Engineering and approved NEDO-20566 [Ref. 5.21]). None could account for the footnote to the table in NEDO-10329 concerning "additional failures". None of these gentlemen could remember ever seeing or hearing about a LOCA analysis that included the assumption of a wireway failure. None of them were aware of any requirement for LOCA analyses to assume such a failure.

NEDO-10329 (Ref. 5.17) and subsequent LOCA analyses prepared by GE for the FitzPatrick plant are based on an assumed failure of a single active component. This includes NEDO-20566, "General Electric Company Analytical Model for Loss-of-Coolant Analysis in Accordance with 10CFR50 Appendix K (January 1976)" and NEDO–21662, "Loss-of-Coolant Accident Analysis Report for James A. FitzPatrick Nuclear Power Plant (Lead plant)" and subsequent revisions all dated July 1977 (Refs. 5.21 and 5.22).

The current FitzPatrick LOCA analysis NEDC–31317P Revision 2 James A. FitzPatrick Nuclear Power Plant SAFER/GESTR-LOCA Loss-of-Coolant Analysis (April 1993) is based on the assumption of a single active component failure (Ref. 5.23). It also continues to refer to NEDO-20566A (Ref. 5.21) as demonstrating compliance with Appendix K Criterion 5 – Long Term Cooling.

Each and every one of the FitzPatrick LOCA analyses were based on single active component failures and the use of combinations of various ECC subsystems. All of these LOCA analyses were reviewed and approved by the AEC or NRC.

NRC documents, such as SECY-83-472 Emergency Core Cooling System Analysis Methods (Ref. 5.25), show that the NRC considers and has always

considered Appendix K analyses to include "the assumption of the worst single active failure".

The NRC evaluated the FitzPatrick ECCS during its review of the application for an Operating License. In its November 20, 1972 Safety Evaluation Report (SER) (Ref. 5.12) the NRC wrote:

> "The ECCS subsystems are provided of such number, diversity, reliability, and redundancy that, even **if any active component of the ECCS fails** during a loss-of-coolant accident, **inadequate cooling of the reactor core will not result.**" (Emphasis added.)

And:

> "We conclude that the design of the FitzPatrick emergency core cooling system is acceptable and meets the requirements of the AEC interim acceptance criteria based on analyses using the G.E. evaluation model acceptable to the Commission and described in Appendix A, part of the Commission's Interim Policy Statement....

The model referred to in the Interim Policy Statement is that provided in NEDO-10329 (Ref. 5.17), and described above.

These conclusions were reconfirmed in a December 27, 1974 AEC Order for Modification of License (Ref. 5.33) and Amendments 8, 14, 26 and 30 to the FitzPatrick Operating License and Technical Specifications (Refs. 5.34 through 5.37).

The 1975 edition of the Standard Review Plan (SRP) NUREG-75/087 (Ref. 5.26) addresses "single active component" failures in Sections 3.6.1 (eight citations), 6.3 (two citations), 15.1.5, 15.2.6, 15.6.1, and 15.6.5 (two citations). The SRP identifies single failure as "single active failure" at least fifteen (15) separate times in sections on piping failures, ECCS, and accident analysis.

Therefore, ECCS are evaluated based upon their ability to perform their system safety function, even in the event of a single active component failure.

5.4 FitzPatrick Single Failure Licensing Basis

In addition to requirements contained in applicable regulations, the FitzPatrick plant must comply with the various licensing commitments contained in the Operating License Application, the UFSAR, NRC Safety Evaluation Reports (SERs) and other docketed licensing correspondence with the NRC. The UFSAR contains numerous references to IEEE-279, IEEE-279-1968, IEEE-279-1971 and the IEEE Proposed Criteria for Nuclear Power Plant Protection Systems (IEEE 279 as amended). The majority of the UFSAR references to

IEEE-279 are made in Section 7.0 - Instrument and Control, or elsewhere in regard to I&C or electrical systems. These statements are sometimes global and often do not identify the revision of IEEE-279 that is applicable: "Safety systems have been designed to meet the single failure criteria of IEEE-279" (UFSAR 1.5.6.1.4).

Sometimes these statements commit specific portions of the FitzPatrick plant design to specific revisions of IEEE-279. For example, the Reactor Protection System, Primary Containment & Reactor Pressure Vessel Isolation & Control System and ECCS instrumentation and controls are similar to those of the Vermont Yankee plant but there are minor differences. UFSAR 7.1.5.1 states:

> "The requirements for single failure and other criteria of IEEE-279-1971 were explicitly applied in the design of the circuit changes, and IEEE-279-1971 was backfitted wherever feasible, all as described below."

USFAR 7.1.5.1 then briefly describes specific modifications made to the plant that are covered by this statement including modifications to the ADS. The UFSAR contains a partial description of the resulting ADS design, which is configured as follows:

> The solenoids which actuate the ADS valves are normally powered from the A battery, with an automatic swapover to the B battery on loss of power from the A battery. (Each ADS valve is equipped with a second solenoid that is powered from the B battery and can only be controlled from a panel on the 300 foot elevation of the Reactor Building.)
>
> The ADS A trip system is permanently powered by the A battery. The ADS B trip system is normally powered by the B battery with an automatic swapover to the A battery on loss of power from the B battery. Both A and B trip systems independently send actuation signals to all ADS valves.

The UFSAR requires updating to resolve inconsistencies in references to this standard as well as to correct some conflicting statements. This is a recommendation of this report (Recommendation 13.2.4). Nevertheless, the UFSAR as well as other docketed information indicate that the safety related plant protection systems (which are defined in Section 5.4.1) were to be designed to withstand a single active or passive failure as described in IEEE-279-1968 (Ref. 5.4).

There are numerous references to single failure, single active failure, and the SFC throughout the UFSAR. There are also a few references to passive failures. These references are often general and applied to entire systems by name or classification without regard to mechanical, fluid, electrical or I&C systems or components – although there are exceptions. Unlike statements that refer to IEEE-279, these statements often don't define what is meant by single failure.

As noted above, the UFSAR requires updating to clarify these statements and this updating is addressed in Recommendation 13.2.4.

5.4.1. Single Failure Requirements of IEEE-279 – Nuclear Power Plant Protection Systems

The 1968 and 1971 versions of IEEE-279 (Refs. 5.4 and 5.5 respectively) are very similar. However, the FitzPatrick plant is committed to the 1968 IEEE-279, which states in Section 1.0 – Scope:

> "These Criteria establish minimum requirements for the safety-related functional performance and reliability of protection systems..."

and

> "For the purposes of these Criteria, the nuclear power plant protection system encompasses all electric and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protection function. These signals include those that actuate reactor trip and ...engineered safeguards..."

Section 4.1 states that:

> " the protection system shall...automatically initiate appropriate protective action ... for the full range of conditions and performance enumerated in 3(g), 3(h) and 3(l). "

Section 3 states that:

> "The design basis shall document as a minimum, the following:
> ... (h) the malfunctions, accidents or other unusual events (e.g., fire, explosion, missiles, lightning, flood, earthquake, wind, etc.) which could physically damage protection system components ... and for which provisions must be incorporated to retain necessary protection system action..."

A footnote to Section 3 further states:

> "The development of the specific information to be used in fulfillment of the above requirements is not within the scope of these Criteria."

This means that the protection system (which actuates ECCS) must be designed to accommodate events that are specified in IEEE-279-1968 and must be defined elsewhere. For example, the FitzPatrick design basis does not include design requirements for explosions inside the plant. It does include design requirements for protection from extreme winds and missiles. The phenomenon

and events for which protection systems must perform their intended function and meet the single failure criterion are beyond the scope of IEEE-279-1968.

IEEE-279-1968 Section 4.2 "Single Failure Criterion" states:

> "Any single failure **within the protection system** shall not prevent proper protection when required." (Emphasis added)

The meaning of this is clear. The single failure occurs "...within the protection system..." There is no mention of any type of failure external to the protection system itself.

Therefore, IEEE-279 applies to the protection systems which actuate systems such as ECCS and not the ECCS piping and fluid components themselves. It requires that the phenomena and events for which the protection systems must be designed be specified in the design basis; and, that the single failure to be accommodated is assumed to occur within the protection system itself. This is consistent with Regulatory Guide 1.53 (Ref. 5.6) and Appendix 7.1-B of the Standard Review Plan (Ref. 5.39), although the FitzPatrick plant is not committed to either document. This is also consistent with General Design Criteria 20 through 24 (Ref. 5.3).

ANSI/ANS 52.1-1983 Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants (Ref. 5.13) states:

> "The single failure criterion requires that the plant be capable of achieving...emergency core and containment heat removal...given an initiating occurrence plus an independent single failure of a nuclear safety-related component..."

And further:

> "The single failure shall be assumed only in the safety-related components that are needed to respond to the initiating occurrence..."

This standard, issued almost ten years after the FitzPatrick plant went into operation, requires that containment heat removal systems meet the single failure criterion. This standard was not a requirement for the FitzPatrick plant as described in Section 5.5.2 of this report.

In UFSAR Section 1.5.6.1.4 and 7.1.5.1, statements are made that safety-related I&C and electrical systems (particularly the Reactor Protection System, the Primary Containment and Reactor Vessel Isolation and Control System and the control systems that actuate ECCS), will still perform their protective function assuming a single active or passive failure. Based upon the meaning of protection system and single failure in IEEE-279-1968 and our general knowledge of the ECCS systems, these statements are correct and protection

systems that actuate the low pressure ECCS systems meet the single failure criterion.

ADS and HPCI have redundant instrument and control logic and redundant logic power supplies, so together ADS and HPCI meet the single failure requirements for protection systems specified in IEEE-279. The NRC recognized and formally concluded that the FitzPatrick Protection Systems are acceptable with regard to the independence of redundant channels when compared to IEEE-279-1968 in its November 20, 1972 SER (Ref. 5.12). The NRC SER states:

> "Our review of the instrumentation and controls encompassed the reactor protection and control system and the engineered safety features. The Commission's General Design Criteria (GDC) and IEEE Std 279-1968, ' Criteria for Protection Systems for Nuclear Power Generating Stations' served as the basis for evaluating the adequacy of these designs."

and

> "We have reviewed various schematic diagrams to confirm conformance with the design and have reviewed the installation at the site."

and in writing of the plant Protection Systems:

> "We have reviewed the cable installation design, routing and identification criteria relating to the preservation of the independence of redundant channels. We have found that these criteria and their implementation are acceptable."

The UFSAR must be updated, as noted above, for clarification and as part of a process to document the design and licensing basis of the ECCS. As part of this update and clarification IEEE-603 should be reviewed for applicability to the FitzPatrick design.

5.4.2 NEDO-10139 Compliance of Protection Systems to Industry Criteria: General Electric BWR Nuclear Steam Supply System (Ref. 5.10)

NEDO-10139 documents GE's comparison of emergency core cooling systems to GE's interpretation of IEEE-279. The NEDO does not apply to containment cooling systems.

In describing the ECCS control and instrumentation, UFSAR 7.1.5.3 states:

> "...a comprehensive comparison of the Reactor Protection System with the design requirements of IEEE-279-1968 has been assembled into a topical report, "Compliance of Protection Systems to Industry Criteria: General Electric BWR Nuclear Steam Supply System" **(GE/NEDO 10139)**.

The results of this analysis show that the BWR Reactor Protection Systems, which will produce protective actions during and after a postulated reactor Loss-of-Coolant-Accident meet the design requirements of IEEE-279-1968.

The topical report illustrates the basis for the analysis and **presents the designer's interpretation of IEEE-279-1968 design requirements in those cases where an exact fit of the requirements to the intended protective function is not achieved.**

The design of the JAF Reactor Protection System, however, was performed prior to the issue and effective date of the IEEE-279-1971 and thus was adequate to meet the then effective IEEE-279-1968." (Emphasis added.)

Taken together with the statements in UFSAR 7.1.5.1 which are quoted in Section 5.3.1 above, this means that the high pressure ECCS (ADS and HPCI) were designed in accordance with IEEE-279-1968 except for the logic that automatically transfers power for the ADS solenoids and trip system B from one battery to another. This portion of the ADS logic was designed in accordance with IEEE-279-1971 (Ref. 5.5).

The UFSAR does not explicitly say that the ADS and HPCI instrument and control logic was designed and installed in accordance with NEDO-10139, however this is implied. In fact, there are differences between the ADS system described in the NEDO and the one installed in the FitzPatrick plant. The NEDO describes the actuation circuits for the ADS valves as emerging from the ADS cabinet (presumably located in the equivalent of the FitzPatrick Relay Room) in independent metal conduits which enter the drywell through separate penetrations.

The FitzPatrick ADS cables from the Control Room to the Relay Room should be verified to be installed in accordance with the NEDO or evaluated in accordance with Recommendation 13.2.3. From the Relay Room cabinet, the FitzPatrick ADS cables run in a common open cable tray with other safety related and non-safety related cables, and enter the drywell through a common penetration. Inside the drywell, the cables share a common junction box. Design electrical engineering should prepare a Nuclear Safety Evaluation (NSE) to formally document the acceptability of the differences between the existing FitzPatrick configuration and NEDO-10139. (See Recommendation 13.2.3).

An inspection during the 1998 refueling outage identified ADS cables in the drywell which were not in conduit. This was corrected during the outage. See Recommendation 13.2.18.

ADS and HPCI are physically separated in the plant to provide protection from external hazards such as pipe whip, jet impingement, missiles and fires. For any

postulated event, physical separation ensures that only one high pressure ECCS subsystem (either ADS or HPCI) would be damaged and the other would remain operable.

Running the cable in open trays rather than separate conduit may make the cables more susceptible to external hazards and electrical faults. Therefore, a study was performed (Ref. 5.14) of the ADS wireways. Based upon this study, NYPA Design Engineering concluded that there are no credible external hazards or electrical faults that could damage the ADS cables over the entire run from the Control Room to the drywell penetration and prevent ADS from performing its safety function. See Section 12.3 for further details.

5.4.3 Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems" (Ref. 5.6)

Regulatory Guides are not legally binding requirements. They describe methodologies that are acceptable to the NRC for meeting requirements that are binding. The FitzPatrick plant as a whole is not committed to conform to RG 1.53, which specifies IEEE-379-1972 (Ref. 5.30) as an acceptable method for meeting IEEE-279-1971 (Ref. 5.5). (Individual modifications may have been made in accordance with RG 1.53.) Section 5.4.1 describes the licensing basis of the FitzPatrick plant with regard to the 1968 and 1971 versions of IEEE-279 (Refs. 5.4 and 5.5).

5.4.4 Single Failures During Transients and Postulated Accidents

Nuclear power plants are designed to withstand the effects of various postulated occurrences. The probabilities of these occurrences vary depending on the type of plant, its location and design. They are postulated to occur so that the plant will be designed so that, if they do occur, the health and safety of the public will be protected.

The FitzPatrick plant was designed for postulated occurrences that are classified and described in Chapter 14 of the UFSAR, as either Abnormal Operational Transients (transients) or Accidents. Transients are occurrences which are expected to happen during the life of the plant and which challenge the first two radioactive material barriers – the fuel cladding and the reactor coolant pressure boundary. Accidents require functioning of the engineered safeguards and are generally not expected to happen during the life of the plant. Transients and accidents have different acceptance criteria. The acceptance criteria for transients are more stringent than for accidents since there is a greater likelihood that they will occur.

Section 14.4.2 of the UFSAR states:

> "Abnormal operational transients may be the result of single equipment failures or single operator errors that can reasonably be expected during any mode of plant operation. The following types of operational single failures and operator errors are identified: ... 4. Any electrical failure..."

Therefore single electrical failures were assumed to occur and, the resulting events were identified as transients and evaluated. These evaluations are described in UFSAR Sections 14.2, 14.4 and 14.5.

Accidents are grouped into classes as described in Chapter 14 of the UFSAR. UFSAR 14.4.3 states that:

> "The accidents resulting in potential radiation exposures greater than any other accident considered under the same general accident assumptions are designated design basis accidents and are described in detail in this chapter.
>
> To incorporate additional conservatism into the accident analyses, consideration is given to the **effects of an additional, unrelated, unspecified fault in some active component** or piece of equipment. Such a fault is **assumed to result in the malfunction of a device which is intended to mitigate the consequences of the accident.** The assumed result of such an unspecified fault is restricted to such relatively common events as an electrical failure, instrument error, motor stall, breaker freeze-in, or valve malfunction. **Highly improbable failures,** such as pipe breaks, **are not assumed to occur coincident with the assumed accident.**" (Emphasis added.)

Section 14.4.3 of the original FSAR contains the same statements except that the word maloperation is used in lieu of the word malfunction. Both the original FSAR and the UFSAR wording are very similar to and appear to be based upon General Electric Nuclear Safety Criterion 1.21, "Single Additional Failure Criterion" (Ref. 5.38). (See Section 5.5.1.)

There are four Design Basis Accidents (DBAs). These are loss-of-coolant accident (LOCA); main steam line break (MSLB) outside of secondary containment; refueling accident; and, control rod drop accident. ECCS would only be needed to cope with a LOCA or a MSLB. The assumptions used in evaluating these accidents are contained in UFSAR Sections 14.6.1.3.1 and 14.6.1.5.1 respectively. Electrical faults in raceways are not mentioned anywhere in these sections or in Section 14.4.3 and therefore are not a single active component failure assumed in LOCA analysis. Electrical faults in raceways are also not identified as an assumed failure in UFSAR Section 14.6.1.3.3, which discusses evaluation of containment response to a LOCA. However, all failures which occur as a direct result of the DBA (consequential failures) are considered in the accident analyses.

5.5 Fitzpatrick Single Failure Design Basis

5.5.1. GE Nuclear Safety Criterion 1.21, "Single Additional Failure"

GE developed a series of technical requirement documents to ensure that GE's design philosophy concerning safety was incorporated into specific plant designs. Nuclear Safety Criterion (NSC) No. 1.21 (Ref. 5.38), was issued on January 31, 1968, probably as a result of the NRC's Draft GDC which were issued in mid-1967. NSC 1.21 states:

> "**In the analysis of a Design Basis Accident (DBA), it shall be assumed that there exists an additional, unrelated, hidden fault** in some piece of equipment or some service. **This fault will result in the misoperation of a device which is intended to mitigate the consequences of the DBA**" (Emphasis added.)

and

> "For the purposes of this criterion, the hidden fault shall be assumed to be a relatively common one such as an electrical failure, instrument error, motor stall, breaker freeze-in, or valve misoperation. **The more improbable types of failure will not be assumed, such as a battery failure** or rupture of the reactor process system simultaneously with an unrelated DBA." (Emphasis added.)

As described in Section 5.4.4, this GE NSC appears to be the basis for Sections 14.4.3 of both the Original FSAR and the UFSAR. The NSC preceded both and followed a few months after the NRC published the Draft GDC in 1967 (Ref. 5.2) (See Section 5.3.1.2.1.) The NRC and ACRS reviewed the Original FSAR as part of the their review of the application for the Operating License. The ACRS asked that the ADS system be modified to ensure that the ADS would perform its design function even in the event of a failure of a station battery, which was its power source. The NRC then required that the failure of a station battery be added to the single active failures assumed coincident with a design basis accident. As a result, this failure became the only passive failure assumed coincident with a design basis accident. As a result the ADS was modified as described in Section 5.4 above. (AEC approval of the final design is described in Section 5.6 below.)

5.5.2. Equipment and Cable Design Separation

The UFSAR contains criteria for the design and installation of cables for instrumentation and control, AC power and DC power. UFSAR 7.1.9 states:

"The design and installation criteria which provide for preserving the independence of Reactor Protection Systems, engineered safety feature systems, and Class 1E electrical systems through physical arrangement and separation of system circuits are presented in Section 8.5."

UFSAR Sections 8.6.3 and 8.7.3 for AC and DC systems respectively also refer to UFSAR Section 8.5. Section 8.5.4.2 – Cables and Raceways states:

"The arrangement of cables and raceways is designed to preserve the independence of redundant Reactor Protection System and engineered safeguard circuits and conforms to the following:

Physical Separation (for Redundancy)

...redundant cables are run in separate cable trays or conduit which are physically separated... Therefore, an event which might damage the cables in one set of trays or conduit will not affect the redundant...cables in the other set of cable trays or conduit.

Intermixing of Nonsafeguard Cabling with Engineered Safeguard Cabling.

Cables for nonsafeguard service may be run in the same raceway with the engineered safeguard cabling... All nonsafeguard cabling is of the same quality as the safeguard cabling and is installed in accordance with the same criteria as the safeguard cabling to ensure that the **nonsafeguard circuits do not compromise the safeguard circuits.**" (Emphasis added.)

Therefore, hazards external to Engineered Safeguards such as a missiles, pipe breaks, or fires would not damage redundant subsystems such as HPCI and ADS. This was assured by physical separation of the subsystems and their raceways. However, certain events, such as pipe breaks and fires, are not assumed to occur coincidentally with a LOCA and vice versa.

The NRC transmitted Appendix A to Branch Technical Position APCSB 9.5-1 "Guidelines for Fire Protection for Nuclear Power Plants Docketed prior to July 1, 1976" to NYPA in a letter dated September 30, 1976 (Ref. 5.32). Appendix A stated:

"Postulated fires... need not be considered concurrent with other plant accidents or the most severe natural phenomenon."

GE Specification 22A2989 Rev. 1, "Electrical Equipment Separation for Safeguards Systems" (Ref. 5.15), which is still in use at FitzPatrick, also addresses this subject:

"The objective of this specification is to set forth a coherent and definitive set of criteria for separation of wiring, cabling, and electrical control and power supply equipment to achieve true independence of safeguards functions compatible with the redundant equipment provided. The resulting installation should satisfy the 'single failure criterion' and assure an optimum level of operating reliability."

This specification contains a Section 4.1 - Single Failure Criterion. The first paragraph of 4.1.1 states:

"Single failure criterion is defined in accordance with Paragraph 4.2 of IEEE-279, and further clarified and limited below. Design Basis Events shall include the following:

4.1.1.1. Electrical fires in wireways .... and

4.1.1.2. Gross failures of electrical equipment in any single compartment..."

This section also identifies earthquakes, environmental factors, and hazardous locations as "design basis events". It concludes:

4.1.1.6. No single design basis event shall disable an automatic protective function, i.e. ...Engineered Safeguards Systems."

Section 4.4 states:

"Electrical equipment and wiring for...the Engineered Safeguards Subsystems (ESS) shall be segregated into separate divisions...such that **no single credible event is capable of disabling sufficient equipment** to prevent reactor shutdown, removal of decay heat from the core, or to prevent closure of the Nuclear Steam Supply Shutoff valves in the event of a design basis accident." (Emphasis added.)

Section 3.1.1.3 defines Engineered Safeguards Systems (ESS) as:

"That combination of **subsystems which take automatic action to provide the cooling necessary to limit or prevent melting of fuel cladding** in the event of a design basis accident. These systems include the following:

a. Core Spray System (CSS)
b. Automatic Depressurization System (ADS)
c. High Pressure Coolant Injection System (HPCI)
d. Residual Heat Removal System (RHR)
e. Emergency Equipment Cooling Water (EECW)" (Emphasis added.)

[EECW is ESW – Emergency Service Water at the FitzPatrick plant.]

The subsystems that take automatic action to provide cooling of the fuel cladding do not include the suppression pool cooling mode (SPC) of the RHR system. The SPC mode of RHR is manually initiated by the reactor operators and is assumed (for accident analysis purposes) to occur ten (10) minutes after the accident begins.

The GE specification appies to ADS and HPCI and the low pressure injection (LPCI) mode of RHR and not to the suppression pool cooling mode of RHR. In the highly unlikely event of the destruction of the ADS wireway, the HPCI system would provide the Engineered Safeguard function and the requirements of both the UFSAR and the GE specification would be met.

The requirements of the UFSAR and the GE specification would still be met even if destruction of the ADS wireway resulted in the loss of shutdown cooling and/or the partial loss of suppression pool cooling. This is because the FitzPatrick licensing basis for safe shutdown after an accident is hot shutdown. Even so, FitzPatrick can achieve cold shutdown with the loss of one division of RHR, including the loss of shutdown cooling. This is discussed in Section 10.2.

Separation prevents events such as electrical fires and gross failure of electrical equipment from damaging cables of redundant subsystems of low pressure ECC systems. The specification does not say that electrical fires and other events are single failures that must be assumed coincident with a LOCA.

Cables are also separated by division, segregated by voltage, service derated and equipped with over-current protection, to prevent electrical interaction as described in UFSAR 7.1.9 and 8.5.4.2. UFSAR 8.5.4.2 states: "Cables are sized and installed so as to limit the temperature rise of conductors to within the emergency temperature rating of the cable for any expected over-load condition."

5.6 Specific Application of Single Failure Requirements to the ADS Wireway

One or more of the DERs described in Appendix A identify several hypothetical scenarios in which a small break LOCA occurs, HPCI injects but is unable to handle the break, and a single wireway failure due to an electrical fault disables ADS. HPCI is unable to handle the break for one of the following reasons depending on the scenario: 1. The break is in the HPCI injection path and HPCI flow goes out the break without depressurizing the reactor; or, 2. The break is very small and HPCI cycles on and off keeping the fuel covered but not depressurizing the reactor. In the second case the contents of the CST tanks are injected and HPCI suction swaps to the suppression pool. The suppression pool heats up until HPCI (which is cooled by the pumped fluid) fails. The smaller the break, the longer HPCI will function. HPCI qualification, operability and mission time are described in Sections 9 and 10.

The FitzPatrick ADS incident detection circuitry and trip systems meet the single failure requirements for protection and ECC systems of the Draft GDC, the UFSAR and IEEE-279. The ADS actuation circuits (the circuits from the trip system output to the ADS actuation solenoids) do not conform to IEEE-279. The AEC specifically reviewed the ADS design and explicitly requested a modification so that it would not be susceptible to a single failure of its power supply. This request was also made of other plants. The AEC then approved the ADS modification in its November 20, 1972 SER (Ref 5.12):

> "...the ADS valves. The power supply to these valves is automatically transferred between redundant busses. We have determined that this design satisfies the single failure criterion and is consistent with previously approved 1967 product line BWR plants. We have concluded that it is acceptable."

Based upon Sections 5.3 through 5.5 above and the AEC SER quoted here and in Section 5.4.1, the ADS system meets the single active component failure criterion for LOCA analyses and substantially meets the single failure criterion for protection systems. It can accomplish its safety function assuming a single active component failure and a single active or passive failure in the incident detection circuitry and trip systems. ADS does not meet the single failure criterion for protection systems by itself since the actuation circuits do not meet IEEE-279.

Section 7.4.3.3.2 of both the Original FSAR and the UFSAR describe the ADS initiating signals and logic. These two sections were compared and the Original FSAR description of "trip system" was changed to "actuation system" in the UFSAR. This revision appears to have been made as an editorial change. However, it may be incorrect terminology which conflicts with the codes and standards applied to the system. This should be reviewed as part of Recommendation 13.2 4.

6.0 ECCS FUNCTIONAL ANALYSIS

6.1 Design Evolution

The evolution of the ADS and HPCI systems can provide insight into the intended system functions and relationship between systems. The conceptual design of the BWR/3 core cooling system did not include HPCI. Instead, it relied on ADS, an isolation condenser, and low pressure core cooling systems. It was intended that the redundancy provided within the ADS system design would satisfy the depressurization requirements. The redundancy existed in the form of a combination of manual or automatic actuations of relief valves (11 in the case of FitzPatrick) located on the four main steam lines in the drywell. NRC review of this design (Ref. 6.1) identified that it was inadequate to mitigate the effects of a small break LOCA due to the potential for a common mode failure that could disable the entire ADS system. Consequently, a high pressure makeup system was considered necessary and the HPCI system was added. Adding a HPCI system created a separate subsystem within ECCS that enhanced the diversity and added redundancy to eliminate the common failure mode concern (Ref. 6.1).

The HPCI system was the preferred system for mitigating small breaks, because it kept the core covered and prevented fuel heatup. Small break LOCA analyses were performed assuming HPCI was unavailable. This resulted in loss of inventory followed by ADS actuation. This in turn maximized core uncovery and peak clad temperature, which resulted in a more conservative analysis.

For the small break accident scenarios postulated at that time, the HPCI system was capable of depressurizing the vessel without assistance from ADS or the SRVs (Ref. 6.2 and Ref. 5.10 page 3-1). The original design of the HPCI System was based on the core cooling evaluation models and design criteria that existed in the late 1960's. The HPCI System design criterion was to prevent clad melt for small breaks with HPCI available in conjunction with three of four LPCI pumps and with one of two Core Spray Systems, with no credit for ADS. This old basis became no longer meaningful, since ECCS analysis models and assumptions were changed to meet 10 CFR 50.46 which was published after the HPCI System was designed (Ref. 6.3).

The HPCI response to small breaks without the use of ADS/SRVs, was described in the 1979 GE NEDO-24708 (Ref. 6.4). That analysis showed the reactor response to long-term HPCI operation for several classes of Recirculation suction line break sizes, 0.005 ft^2, 0.08 ft^2, and 0.2 ft^2. For the 0.005 ft^2 break, the break flow rate is small compared to the capacity of the HPCI flow. For the 0.08 ft^2 break, the break flow approximately equals the HPCI flow. For these two breaks, the analysis shows that reactor pressure oscillates below the SRV setpoint for many hours at a pressure too high to make use of the low pressure ECCS systems. Without using ADS or manual SRV actuation to depressurize the vessel for these break sizes, the low pressure systems cannot be used. This would put greater reliance on the single HPCI pump for long-term cooling as

opposed to the higher flow low pressure ECCS pumps. However, a full complement of suppression pool cooling equipment is available since only single active component failures are assumed for LOCA analyses (as described in Section 5.3.1.3). Therefore, it is expected that the plant can be safely cooled down without exceeding HPCI operating temperatures. This will be verified as per Recommendation 13.2.1.

6.2 HPCI/ADS Design Function

"Nuclear Safety Criteria for Boiling Water Reactors", Criterion 7.1, (Ref. 6.5) states:

> "Emergency Core Cooling Systems shall be provided which will operate to cool the reactor core when coolant is lost through any design basis break size of the nuclear system process barrier."

GE Design Specification for High Pressure Coolant Injection System (Refs. 6.6 and 6.7) specify HPCI requirements as:

> "The HPCI System shall allow for complete plant shutdown by maintaining sufficient reactor water inventory until the reactor is depressurized to a level where the low pressure coolant injection system or core spray system can be placed into operation."

GE Design Specification for the Nuclear Boiler System (Ref. 6.8) specifies ADS requirements as:

> "Relief valves used for automatic primary system depressurization under assumed loss-of-coolant accident conditions shall automatically open and remain open below their preset closing pressure under such conditions. The open signal is based on simultaneous signals from high drywell pressure [a modification to the logic deleted this input signal], low reactor water level and non-operation of the High Pressure Coolant Injection (HPCI) system for which these relief valves shall be backup. By remaining open, the relief valves shall reduce the reactor pressure to the point where Residual Heat Removal (RHR) and/or the core spray systems can adequately cool the core. In addition, the relief valves shall be utilized, in the event the main condenser is not available, as a heat sink after reactor shutdown, to relieve steam generated by core decay heat to the suppression pool. Relief valve operation shall be manual from the main control [*sic*] to hold the desired primary system pressure."

Current Technical Specification Bases, Section 3.5.C (Ref. 6.9), defines the HPCI system function as:

"The High Pressure Coolant Injection System is provided to adequately cool the core for all pipe breaks smaller than those for which the LPCI or Core Spray Systems can protect the core."

Current Technical Specification Bases, Section 3.5.D (Ref. 6.10) defines the ADS system function as:

"The relief valves of the ADS are a backup to the HPCI subsystem. They enable the Core Spray or LPCI Systems to provide protection against the small pipe break in the event of HPCI failure, by depressurizing the reactor vessel rapidly enough to actuate the Core Spray or LPCI Systems."

"Nuclear Safety Criteria for Boiling Water Reactors", Criterion 7.1, (Ref. 6.5) states:

"The number, diversity, and redundancy of emergency core cooling systems shall provide a high probability of the core being adequately cooled following a loss-of-coolant accident. Preferably two independent techniques or phenomenological methods of cooling shall be employed."

UFSAR Section 6.2 (Ref. 6.14,) establishes the Safety Design Bases as (in part):

"The Emergency Core Cooling Systems (ECCS) are designed with diversity, reliability, and redundancy to provide adequate core cooling of the reactor core under abnormal and accident conditions."

"In the event of a LOCA, the ECCS are designed to remove residual heat, including stored heat and heat generated due to radioactive decay, such that excessive fuel clad temperature is prevented."

"The ECCS provide for continuity of core cooling over the complete range of postulated break sizes in the Reactor Coolant Pressure Boundary piping."

In order to satisfy the Safety Design Bases, the FSAR Safety Evaluation (Ref. 6.15, Section 6.5) says it relies upon four systems (HPCI, ADS, CS and LPCI) which comprise the ECCS. Throughout the Safety Evaluation it is stated that the plant's ability to meet the design criteria and the safety design bases is dependent on:

"the manner in which ECCS operates to protect the core..."

"the ECCS removes the residual and decay heat from the reactor core..."

UFSAR Section 6.3 (Ref. 6.16) refers to:

"...the redundant capability of the integrated ECCS."

It also references functional aspects of ECCS like,

"...the low pressure portions of ECCS..."

"...the reliability and diversity of ECCS..."

In conjunction with system design criteria and design specifications, these references to ECCS make it quite clear that ECCS includes the functions of HPCI, ADS, CS, and LPCI. Documentation shows, from a functional point of view, that ECCS has been regarded as a single system with several subsystems fulfilling different emergency core cooling functions. ECCS, therefore, is an integrated collection of subsystems designed to meet the collective function of core cooling.

ECCS is routinely regarded and identified by its individual subsystems, HPCI, ADS, LPCI, and CS, with separate unique functions in the plant. However, separating any single subsystem from ECCS to determine its ability to meet the overall safety functions and design criteria may be inappropriate. ADS, for example, is incapable of meeting the ECCS function to inject water to remove decay heat, as LPCI is incapable of depressurizing the reactor. It is the integrated ECCS that meets the safety functions and design criteria for all conditions.

6.3 Emergency Core Cooling Systems Redundancy and Integrated Operation

Computer modeling and analysis demonstrates that the ECCS design criteria, of preventing peak clad temperatures of greater than 2200 °F, is satisfied across the entire spectrum of possible liquid or steam line break sizes. This is accomplished by two different modes of core cooling, even in the event of the loss of normal auxiliary power. The redundant capability of the ECCS is sufficient for all size line breaks up to and including the double-ended design basis break. The individual ECC subsystems also meet the ECCS design criteria, without assistance from other subsystems, over certain specific ranges of break sizes in the Reactor Coolant System. Their integrated performance provides adequate and timely core cooling over the entire spectrum of LOCAs, up to and including the Design Basis LOCA, even with concurrent loss of offsite AC power. (Ref. 6.15)

The manner in which the ECCS operates to protect the core is a function of the rate at which coolant is lost from the break in the Reactor Coolant Pressure Boundary. The HPCI System is designed to provide adequate reactor core

cooling for small breaks when the reactor is at high pressure. The injection of coolant, taken from the condensate storage tanks or the suppression pool, allows the reactor pressure to slowly decrease until it reaches a point where the LPCI and Core Spray Systems can be initiated (Ref. 6.15). (EOP-2 Rev. 4 requires defeating the automatic transfer function of the suction to the suppression pool on high torus water level.)

When the HPCI System begins operation, the reactor depressurizes more rapidly than would occur if HPCI were not initiated due to the condensation of steam by the cold water pumped into the reactor vessel. As the reactor vessel pressure continues to decrease, the HPCI System momentarily reaches equilibrium with the flow through the break. Continued depressurization causes the break flow to decrease below the HPCI System flow and the liquid inventory begins to rise. (Ref. 6.15)

If the break in the Reactor Coolant Pressure Boundary is of such a size that the loss-of-coolant exceeds the capacity of the HPCI System, Reactor Coolant System pressure drops at a rate fast enough to allow the Core Spray System and LPCI to cool the core. Automatic depressurization is provided to automatically reduce Reactor Coolant System pressure if a break has occurred and the HPCI System and other water addition systems do not maintain vessel water level. Rapid depressurization of the Reactor Coolant System is desirable to permit flow from the Core Spray and LPCI Systems to enter the vessel, so that the rise in peak cladding temperature is limited. When the Automatic Depressurization System is actuated, the flow of steam through the valves provides a maximum energy removal rate while minimizing the corresponding fluid mass loss from the reactor vessel. Thus, the internal energy of the saturated fluid in the reactor vessel is rapidly decreased causing pressure reduction. The Automatic Depressurization System functions and is analyzed in conjunction with LPCI or Core Spray. ADS, together with the LPCI and Core Spray Systems, provides the backup for the HPCI System. (Ref. 6.15)

If, for a given size break, the HPCI System has the capacity to makeup all the coolant lost from the Reactor Coolant System, flow from the low pressure portions of the ECCS is not required for core protection until the Reactor Coolant System pressure has decreased below approximately 150 psig. This pressure is well within the range of the LPCI and Core Spray Systems so that water continues to be pumped into the reactor vessel. (Ref. 6.15)

Capability for cooling exists over the entire spectrum of break sizes. This is true even with the concurrent loss of normal and reserve power, the unavailability of one of the high pressure systems (HPCI or Automatic Depressurization) and the unavailability of one of two redundant divisions of the low pressure systems (Core Spray and LPCI).

6.4 Manual ADS/SRV Depressurization

This section discuses the licensing basis of manual depressurization. However, EOP-3 and EOP-4 require the operators to override the ADS signal and manually depressurize in a controlled manner, unless the EOPs direct otherwise.

"Nuclear Safety Criteria for Boiling Water Reactors", Criterion 4.5, (Ref. 6.17) provides criteria for operator judgement and response to potentially serious accident situations:

> "Facilities for manual actuation of safeguards shall be provided in the control room so that operator judgement and action is possible, yet reserved for the remedy of a deficiency in the automatic actuation of the safety equipment."

"Nuclear Safety Criteria for Boiling Water Reactors", Criterion 7.1, (Ref. 6.5) states:

> "For at least the first few minutes following the rupture, automatic instrumentation of the Reactor Protection Systems shall assess the prevailing conditions and automatically select and operate appropriate cooling systems. ... This will give the plant operators some time to make plans for manual action if necessary. Ten minutes is suggested as a minimum time."

In response to a request by the AEC, a special study was conducted concerning the effects of a postulated pipe break in high energy lines outside the primary containment. This study, "Effects of a High Energy Piping System Break Outside Primary Containment" (Ref. 6.18), includes a special shutdown procedure in the event of a Main Steam or Feedwater line break. The procedure specifies manual actuation of ADS:

> "On indication that the HPCI system failed to start, the operator can manually reduce reactor pressure using the automatic depressurization system (ADS)."

It also recognizes the impact of repeated SRV blowdown on suppression pool temperature:

> "The suppression pool temperature will increase with repeated relief valve blowdown. Suppression pool temperature will be controlled by manually initiating the residual heat removal system and RHR service water system in the suppression pool cooling mode."

NEDO-24708 (Ref. 6.19) analyzes the systems' response to various accidents and transients. In the event of a small break LOCA and in conjunction with other system failures, including complete loss of the high pressure systems, this document includes manual initiation of ADS (manual operation of one or more ADS SRVs) to allow low pressure systems to mitigate the accident and maintain core cooling.

> "The operator should verify that automatic ECCS actuations occur when the levels are at the trip points. The operator should be prepared to manually actuate ECCS during a suspected LOCA if automatic actuation is not achieved."
>
> "If the pool temperature reaches [F], then manually depressurize the vessel to below [150 psig] using one or more SRVS."
>
> "If vessel pressure increases ... then depressurize the vessel in the following order of preference: 1) condenser, - 2) one or more SRVs to the pool, - or 3) manual ADS initiation."
>
> (Brackets indicate that plant specific values should be inserted for that parameter.)

NEDO-24708 describes many different scenarios - some of which involve multiple equipment failures or other degraded conditions outside the licensing basis of the FitzPatrick plant. In some cases actuation of the ADS was assumed. In others, the use of manual actuation of the SRVs was credited in response to these conditions. Postulated accidents with typical assumed failures were analyzed without manual operator actions for at least the first ten minutes.

In a NRC letter dated December 3, 1979 (Ref. 6.20) regarding an evaluation of the small break LOCA operator guidelines, the NRC confirmed agreement and acceptance of the actions contained in the guidelines, Section 3.1.1.2 of NEDO-24708, by stating:

> "We have completed our review of these guidelines, have determined that they have been modified in accordance with our agreements and conclude, therefore, that they are acceptable."

In a 1980 response to NRC questions regarding ECCS response to a small break LOCA (Ref. 6.21), GE answered, in part:

> "The small break **operator guidelines** in NEDO-24708, in addition, **explicitly provide for manual depressurization** in the event of low reactor water level **with high pressure systems unable to maintain level for any reason.**" (Emphasis added.)

The NRC issued a Generic Letter on January 8, 1980 (Ref. 6.22) which described their audit of small break LOCA emergency procedures and operator retraining at JAF and other plants. The purpose of the NRC audit was to review the implementation of the NRC approved operator guidelines developed by the GE BWROG as set forth in NEDO-24708. Manual initiation of ADS (manual operation of one or more ADS SRVs) to mitigate the effects of a small break LOCA was mentioned several times in the Generic Letter. Hence, manual actuation of the SRVs to relieve pressure is part of the mitigation strategy reflected in Emergency Operating Procedure EOP-02 (Ref. 6.23).

GE report, NEDC-24361-P, "Suppression Pool Temperature Response" (Ref. 6.25), evaluated the use of manual ADS actuation for small break accident mitigation by saying:

> "The ADS system is modeled by fully opening six SRVs in the ADS mode. The ADS system may be actuated manually on high suppression pool temperature (120F)."

This acceptance of manual depressurization to supplement HPCI and ADS appears in the Safety-Related Functional Analysis (SRFA), Safe Shutdown Evaluation (UFSAR Section 12.2A.6) (Ref. 6.26). The SRFA is a systematic analysis that identifies consistently and clearly the safety-related equipment functions required for the mitigation of each accident and abnormal operational transient specified in Chapter 14 of the Updated Final Safety Analysis Report (UFSAR). The SRFA was accepted and incorporated in the UFSAR via Nuclear Safety Evaluation JAF-SE-88-052 (Ref. 6.27). It should be noted that the level of detail presented in this Nuclear Safety Evaluation has been questioned and a review to determine the adequacy of the evaluation is necessary. (See Rec. 13.2.11.)

The Safety-Related Functional Analysis (SRFA), Safe Shutdown Evaluation (UFSAR Section 12.2A.6) (Ref. 6.26) says:

> "For small pipe breaks inside the primary containment, pressure relief is effected by the nuclear system pressure relief systems that transfer decay heat to the suppression pool."
>
> "After completion of the automatic safety-related functions of the above equipment, manual operation of at least one low pressure ECCS, the RHR System suppression pool cooling mode and ADS or relief valves (controlled depressurization) are required to maintain containment pressure and fuel cladding temperature within limits during extended core cooling."

The use of relief valves in conjunction with HPCI operation, as stated in the SRFA and UFSAR, is consistent with the November 1972 AEC Safety Evaluation Report (Ref. 5.12):

> "They [the SRVs] can be operated by remote manual controls at pressures below the set point to control coolant system pressure."

Use of SRVs is also consistent with the post-LOCA assumption of a single active component failure, which means that an adequate number of SRVs will always be available.

Also in FSAR Section 12.2A.7 (Ref 6.28) it says:

> "In State C, in which the reactor vessel head is on and the system can be pressurized, operation of relief valves or ADS in conjunction with any of the ECCS and the RHR suppression pool cooling mode (both manually operated) can be used to maintain water level and remove decay heat."

A GE topical report (NEDO-10189) on common mode failures in protection and control instrumentation (Ref. 6.29) discusses the response to pipe breaks inside primary containment coincident with the failure to sense ECCS initiating conditions such as high drywell pressure:

> "If the break were in the HPCI line, operator action would be required (in the event of failure to sense high drywell pressure) to initiate controlled depressurization. The operator would have numerous indications of the condition - loss of feedwater, low water level, scram, isolation, high drywell temperature, HPCI not operating, and drywell radiation alarms. If no credit is taken for operator action until 10 minutes after the time of the break (a requirement of APED-4600, Criterion 7.1, Ref. 6.5), the effects would be no worse than if depressurization were initiated automatically by high drywell pressure and low water level."

NEDO-10189 (Ref 6.29) concludes by saying:

> "For small steam line breaks in the HPCI steam supply lines, either failure to sense high drywell pressure, or failure to sense low water level will not result in high cladding temperatures even though both high pressure systems (HPCI and automatic depressurization) are inoperable. With proper operator action to initiate depressurization, the consequences will be no worse, over the spectrum of break sizes, than if the system had operated automatically."

Manual relief valve actuation is accomplished via a switch for each valve from the control room that bypasses ADS control logic (Ref. 6.30). It does, however, use the same power supply and cabling run to the solenoid valves. In addition, independent remote shutdown switches exist that are credited for compliance with 10 CFR 50.48 and Appendix R (Ref. 6.31). These remote manual switches provide further redundancy to the system by utilizing totally separate power supplies, relays, cabling (from the remote shutdown panel to the relief valve solenoid valves) and solenoid valves, different than those used in the ADS logic circuit. This equipment is used to provide a redundant means for mitigating the effects of a fire in the control room, relay room, cable spreading room and certain other areas, which could disable ADS and other vital equipment. The hardware associated with this modification was purchased seismically and environmentally qualified and may be QA Category I (although the drawings indicate otherwise). Therefore, it might possibly be used to mitigate a LOCA, however, explicit credit cannot be taken for its use without further analysis and the evaluation of required operator actions. EP-11 Rev. 0 (Ref.6.32) has been issued to permit use of the remote ADS control panel if the SRVs cannot be opened from the control room.

A description of long term operation of HPCI operation was requested in FSAR Question 4.19. The response to the question acknowledged that long term HPCI operation was possible but that the operator would, if necessary, reduce the vessel pressure in an orderly manner. Additionally, the response recognized that if the CSTs were unavailable to provide relatively cool makeup water to the vessel, the operator would not consider going into a prolonged period of hot standby conditions and would initiate cooldown of the reactor immediately. These statements indicate that the NRC (AEC) was aware that while HPCI is capable of operating for a long period of time, manual depressurization would be used in conjunction with HPCI operation.

Additional recognition of operator action is presented in the original FSAR, Section 14.6.5, "Main Steam Line Break Accident", where it is stated that:

> "After the main steam line isolation valves are closed, the reactor can be cooled by operation of any of the normal or Emergency Core Cooling Systems".

The use of manual actuation of the SRVs to depressurize the vessel is widely accepted as a viable means for accident mitigation. It is an integral part of the ECCS design of interdependent subsystems. Manual actuation, however, cannot be relied upon to supplant the role of the auto-initiated design features of the ECCS for at least ten minutes following the onset of the LOCA (Ref. 6.5).

This is reiterated in NEDO-24951, "BWR Owners' Group NUREG-0737 Implementation: Analyses and Positions Submitted to the USNRC" (Ref. 6.33). Section 8 of the NEDO describes the short and long term phases of an accident and the operator actions required to respond to each. The plant response during the short term phase of an accident (large or small break) is completely automatic. The short term phase ends when core-uncovery and heatup have been terminated by automatic operation of the Emergency Core Cooling systems. No operator actions are credited during the short term phase. As noted above, this is generally assumed to be the first ten minutes of the accident. Typical LOCA analyses, which do not involve degraded conditions beyond the licensing basis, end at ten minutes. The longest analysis cited in this report ends at 1000 seconds, or less than 17 minutes.

The long term phase begins as soon as the core-uncovery and heatup has been terminated. At this point adequate short term core cooling has been established without operator action. Paragraph 2.6 of Section 8 of NEDO-24951 states:

> "BWR emergency system design is based on the assumption that **long term control of the reactor will be completely dependent upon operator actions**. This long standing design philosophy has been consistently applied to reactor control following both non-LOCA transient events (such as turbine trip) and also to the complete spectrum of credible loss of coolant accidents. A good example of this philosophy is the **complete manual control of the multiple operations required to establish the long term post-LOCA containment cooling functions. Post-LOCA containment cooling is** a key safety function since it prevents overpressurization and is thus **required to support the long term cooling of the core.**" (Emphasis added.)

Therefore, long term cooling and achieving cold shutdown are completely dependent upon operator actions. The use of SRVs for depressurization during the cooldown is in keeping with this design philosophy.

7.0 CABLE SEPARATION

7.1 Separation & Installation Criteria

Separation and installation criteria are defined in JAF-RPT-ELEC-02075 Rev 1, Design Criteria for Independence of Redundant Electrical Circuits (Ref. 7.1).

These criteria are based on the basic premise that redundant systems obtain their redundancy by being divided into two channels having physical separation. Physical separation requires separate raceways and criteria define the minimum separation distances required between the raceways.

The criteria allow non-safety related cables to be run in safety-related raceways, provided once entering such a raceway they never leave it to run in a redundant safety-related raceway. However, they may leave to enter a non-safety related raceway.

The criteria define different service classes of cables and raceways and require the service classes to match. However 600 V power and low voltage control and alarm cables may be mixed in the same raceway provided certain additional criteria are met.

7.2. Routing of HPCI and ADS Cables

HPCI and ADS cables are run separately from each other consistent with the HPCI and ADS systems being considered functionally redundant. HPCI is installed as a Division II system and ADS as a Division I system. (This applies to the automatic operation of ADS.)

There is a remote manual system associated with the ADS system that operates through a separate set of solenoids. The cabling for the remote manual system runs separate from that for the automatic system. The remote manual system is installed as a Division II system.

Cabling for each of the seven (7) ADS valves and four (4) SRVs is run in common raceways and enters the drywell through a common penetration.

7.3. Conformance to Criteria

The separation of the HPCI and ADS cabling meets the design basis separation criteria since HPCI and ADS are functionally redundant with regard to depressurization.

The cabling for all of the ADS valves is run in common raceways and enters the drywell through a common penetration. In other words, ADS cabling is not separated into redundant channels. Furthermore, the common raceways are shared with multiple non-safety-related cables. If ADS were required to be redundant this would not be permitted by the design basis separation criteria.

7.4. Containment Electrical Penetration Protection

The ADS system cables enter the drywell through penetration X101B. None of the cables that share raceways and enter the drywell together with the ADS cables through this penetration will be damaged as the result of a cable failure within the drywell, even allowing for a single failure. This is because these cables fall into one or more of the following categories:

- The short circuit current is below the continuous rating.
- They have dual levels of overcurrent protection.
- They are QA Cat I circuits and are designed not to fail as the consequence of a design basis event. As a result, if they were to fail that would be the single random failure and their single level of protection is presumed to operate correctly.

An Electrical Penetration Coordination Study (Ref 7.2) was performed and one cable was found to be an exception to the discussion. This cable was modified to bring it into conformance as described in NSE JAF-SE-98-017. Ref. 7.2 concluded that, after this modification, there are no post-LOCA failures of cables or loads in the drywell, which will result in an overcurrent condition that will damage a containment electrical penetration. Therefore, no such failure can propagate beyond the penetration and damage cables outside the drywell. In other words, electrical failures that could result from the LOCA (i.e. consequential failures) have been adequately addressed in the design of the plant.

A 1998 refuel outage inspection found that ADS cables in the drywell were not completely run in conduit. The plant was modofied to correct this. (See Recommendation 13.2.18.)

8.0 PIPE BREAKS IN THE HPCI INJECTION PATH

DER-97-1763 describes the plant response to a hypothetical break in the "B" Feedwater line with a break flow of 4250 gpm – equivalent to HPCI flow capacity. This break, with both a specific size and a specific location has not been demonstrated to be physically possible. This section of the report describes how the hypothetical break was evaluated and determined to be mechanistically not credible. Also, the licensing basis of FitzPatrick takes credit for ADS when the break is too large for HPCI alone or if HPCI fails (for whatever reason) to handle the break. (UFSAR 4.4.5)

As a result of this hypothetical break plus hypothetical total failure of ADS, it is postulated that all of the HPCI flow would be diverted to the break and would not reach the reactor vessel. The HPCI injection flow would not increase the water inventory in the vessel and would not depressurize the reactor. Decay heat would increase the reactor vessel pressure until the pressure exceeded the SRV setpoint and the SRV, operating in the safety mode, would lift and relieve the pressure. This would reduce the water inventory in the vessel and would ultimately result in core uncovery and fuel damage. A break on the "A" Feedwater line was not examined since HPCI flow would reach the reactor vessel for such a break.

The hypothetical break could be the result of a crack in a pipe or weld, or the failure of a branch connection. The HPCI injection path, including the "B" Feedwater line, was evaluated to determine if such a break was credible. Calculations were performed to determine the leakage rate of critical crack lengths for a circumferential and a longitudinal break in either the Feedwater line or the HPCI injection line (Ref. 8.1). The results of the calculation are as follows*:

Pipeline	Circumferential Break		Longitudinal Break	
	Critical Crack Length (in.)	Leakage Rate (GPM)	Critical Crack Length (in.)	Leakage Rate (GPM)
18"-FW	10.74	35.4	9.61	17.4
12"-FW	8.54	23.3	5.78	8.9
10"-HPCI	7.54	20.4	4.48	5.6

*Note that Section 4.7 of Ref. 8.3 and Ref. 8.4 identify the minimum leak rate from any crack large enough to propagate rapidly as 150 gpm, still well below the postulated break flow rate. The source of the 150 gpm value is GEAP-5587 (Ref. 8.5).

As the crack grows beyond the critical size, the pipe can be expected to experience sudden failure or a break (Ref. 8.2). Such a failure is uncontrolled and very unlikely to result in a particular size break with a flow of 4250 gpm. Therefore, it can be concluded that a postulated break of a size equivalent to the HPCI injection capacity is not a credible break.

As shown above, the leakage rates from critical size radial or longitudinal cracks in the Feedwater lines or the HPCI injection line range from approximately 6 gpm to 35 gpm. If such a crack were to occur without propagating beyond the critical size, HPCI capacity (4250 gpm) would be more than adequate to ensure makeup flow to the vessel. Additionally, cracks within this range would be easily detected by leak detection systems (which can detect as little as 5 gpm) prior to propagation of the break (Ref. 8.7). The leak detection system would allow operators time to take appropriate compensatory actions before a pipe break.

To result in a LOCA, the postulated break would have to occur between the reactor vessel and Feedwater check valve NRV-111B in line 14-W25-902A-3A. As stated above, a break in the line itself would not result in a break of the size in question. However, there are connections to the Feedwater line downstream of the check valve. These connections were reviewed (Ref. 8.6) and it has been determined that no connections greater than ¾ " exist between the check valve NRV-111B and the reactor vessel. A total failure of one of these connections will result in a leak of approximately 200 gpm. Therefore, a failure of one of these connections cannot result in a break of the size in question.

Based on the above information, a postulated break with break flow equivalent to HPCI makeup capacity (in the "B" Feedwater line) is not a credible event. This is also true of the "A" Feedwater line, which has a three (3) inch RCIC connection which could be postulated to fail. However, in this case the RCIC break would be isolated from the reactor vessel by a feedwater check valve and the HPCI flow would reach the core.

Additional reviews were originally recommended (Rec. 13.2.17 was withdrawn) to verify that a recirculation pump seal failure or valve packing failure could not result in a "break" of the specified size. This is unnecessary since the recirc pump has dual seals (either of which will withstand reactor pressure if the other fails). The seals are equipped with seal leak detection which alarms in the control room and the pump is equipped with a throttle bushing to limit leakage in the unlikely event that both seals fail. The pump can also be isolated from the reactor coolant system. Valves are equipped with a lantern ring and a leakoff connection. In either case, HPCI would inject into the reactor vessel.

9.0 QUALIFICATION OF THE CONDENSATE STORAGE TANK (CST), THE HPCI SUCTION LINE TO THE CST AND THE HPCI TEST RETURN LINE

DERs 97-01226 & 1227 concerned a letter to the NRC (JPN-97-003) which stated that the automatic transfer of the HPCI suction line from the CST to the suppression pool was not required, except for initiating events which could render the CST unavailable. The letter concluded that the transfer function under thermal pressurization conditions, as postulated in GL 96-06, is not required.

HPCI pump suction is normally aligned to the CSTs to provide a source of reactor quality water in the event of reactor isolation or a small break LOCA. Each tank has a capacity of 200,000 gallons, with 100,000 gallons per tank reserved for HPCI and RCIC operation. This reserve capacity is adequate to support HPCI and RCIC operation for up to 16 hours (8 hours per tank) in the event of reactor isolation without a break (Ref. 9.1). To ensure that this source of water would be available when required, a portion of each tank is below grade, providing protection from natural phenomena such as earthquakes, tornadoes, and missiles (Ref. 9.4 and 9.1, Sections 2.1.1.7, 3.3.1.3).

The HPCI pump suction line to the CSTs is also below grade, and, as stated in Ref. 9.2, Section 2.1.1.1(f), "must meet Class I earthquake requirements". (See also Refs. 9.6 and 9.7). The seismic criteria applied to buried pipe was discussed in response to AEC Question 12.6 (Ref. 9.3).

The HPCI test return line, which would be used if operating HPCI in the pressure control lineup, is mostly below grade providing protection from natural phenomena. The line splits into two lines below grade near the tanks. Each line rises above grade near its tank and returns the test water to the upper portion of each tank. Each line is unprotected from grade level to the top of the tank. No documentation regarding the design criteria applied to this line could be located. If credit were to be taken for operation of HPCI in the pressure control lineup, this line would have to be evaluated and upgraded to QA Category I. There are no plans to credit this lineup of HPCI operation at this time.

During a Master Equipment List review in the late 1980's, the CSTs and the HPCI pump suction line were downgraded from QA Category I. A review is currently underway to confirm that the CSTs and the line still satisfy QA Category I requirements (See Rec. 13.2.20). Additional research to locate the original design, purchase and installation documents is required to fully support the QA Category I classification.

The reserve portion of the CST and the HPCI suction line to it were originally QA Category I and are unlikely to have been modified since their declassification since they are below grade. This equipment must be reevaluated and reclassified as QA Category I (Rec. 13.2.20). HPCI is normally aligned to the CST and this is assumed in LOCA analyses and the EOPs. If the equipment is not returned to QA Category I status: either HPCI must be realigned to the

suppression pool; or, the LOCA analysis must be redone to account for the delay in switching the HPCI suction from the tank to the suppression pool at the start of the LOCA. Although technically feasible, neither of these options is considered beneficial.

Pressure locking of the valves in the HPCI suction line has been evaluated. Qualitative assessment has concluded that the HPCI system safety function would not be jeopardized. However, because of uncertainty in the qualitative assessment, NYPA performed a quantitative assessment of the potential for pressure locking. Due to the design features (solid wedge gate valves, SS seats) of the valves in this penetration, the valves have sufficient leakage to prevent this phenomenon.

A calculation (JAF-CALC-HPCI-02968, Rev. 0) determined the leakage rate based on the maximum heatup rate of the water inside the piping between 23MOV-57 and 23MOV-58. The leakage rate that equates to the rate of volumetric increase due to thermal expansion is roughly 120% of the acceptable leakage rate for a new single valve in this penetration. Since there are two valves that form the pressure boundary for this section of piping, this represents roughly 60% of the acceptable leakage rate for this penetration with new valves at their maximum allowable leakage. There are no Appendix J leakage testing requirements for these valves because they are water sealed.

This evaluation was performed in accordance with constraints imposed by the NRC in Ref. 9.5. NRC leakage rates will require testing, perhaps on a periodic basis. A temporary operating procedure (TOP-281, Rev. 0) was prepared and a Nuclear Safety Evaluation (JAF-SE-98-027) PORC approved to collect the necessary information for further evaluation. This testing established that the actual leakage was more than 300 times greater than required to prevent pressure locking (JAF-RPT-HPCI-03080). Procedure AP-05.07, Maintenance and Post-Work Testing (ISI), was revised to ensure that any future valve maintenance that could change this requires testing to confirm that the leakage remains above the threshold for pressure locking.

NYPA's response to Generic Letter 96-06 was revised as a result of an NRC Request for Additional Information. This response was also revised to incorporate the above information (Ref. 9.8).

10.0 – HPCI MISSION TIME

10.1 Introduction

A small break in the HPCI injection path has been hypothesized coincident with the destruction of an ADS raceway due to an electrical fault. Since this raceway contains other safety related cables, one division of Residual Heat Removal Service Water (RHRSW) could be lost, as well as a portion of the RHR equipment which is used in the suppression pool cooling mode. In this hypothetical scenario, the water supply in the Condensate Storage Tanks (CSTs) is eventually depleted and HPCI suction would automatically switch to the suppression pool (unless the automatic swapover is bypassed). Due to the reduced suppression pool cooling capability, HPCI (which is cooled by the pumped fluid) is hypothesized to fail before it alone can depressurize the reactor. Core uncovery and fuel damage could result.

Existing documentation does not specify exactly how long HPCI is assumed to operate post-LOCA. For a large break LOCA, HPCI is not required at all. For smaller breaks, its mission time depends on the size of the break and the other assumptions of the evaluation. None of the existing small break LOCA analyses quantified HPCI operating time. HPCI is usually assumed to fail in small break analysis since HPCI failure results in the highest peak cladding temperature and therefore results in the most conservative evaluation. Analyses which do show HPCI operable usually terminate at 10 minutes or 1000 seconds.

Although HPCI operating time is not quantified, information exists which can be used to deduce the mission time of HPCI as envisioned by the system designers.

It should be noted that the design basis of HPCI calls for HPCI to have the capability of cooling the core and depressurizing the reactor (with no assistance from ADS) until the low pressure ECCS can be used. (This is addressed in Section 6.1 and Recommendation 13.2.1.) This discussion demonstrates that the original design intent was to use both HPCI and ADS (SRVs in the manual mode) to reach cold shutdown following a small break LOCA. FitzPatrick reaches hot shutdown with no operator actions as described below.

10.2 Safe Shutdown

The FitzPatrick plant was designed and licensed to achieve safe shutdown following any transient or accident (and certain other licensing basis events, e.g. station blackout). Safe shutdown was defined in the 1967 Draft General Design Criteria (Ref. 5.2) as hot shutdown. Criterion 28 – Reactivity Hot Shutdown Capability states that:

"At least two of the reactivity control systems provided shall independently be capable of making and holding the core subcritical from any hot standby or hot operating condition."

Safe shutdown was considered hot shutdown for Fitzpatrick and other plants of the same vintage (Ref. 10.1). An electronic (Folio) search of the current UFSAR shows that the capability to achieve safe shutdown is used when describing the ECC systems. The term "cold shutdown" is used in only three ways in the UFSAR. It is used to describe the capability of the control rods to hold the core subcritical in cold shutdown; to describe the capability of the Standby Liquid Control System to hold the core subcritical in cold shutdown; and, for the plant to have the capability and procedures to allow achieving cold shutdown from outside the control room.

Section 1.2 of the UFSAR contains definitions of Achieving Shutdown, Cooldown and Shutdown Mode. These definitions make it clear that shutdown means that the reactor is more than one rod subcritical and that the reduction of reactor coolant system temperature and pressure is considered Cooldown.

For the FitzPatrick plant, safe shutdown is Hot Shutdown. Hot Shutdown is achieved once HPCI has actuated, restored level, and is maintaining level. The transition from Hot Shutdown to Cold Shutdown is considered Cooldown (UFSAR 1.2).

This is confirmed by the fact that safe shutdown must be obtainable assuming various single failures; and, the FitzPatrick plant shutdown cooling system is vulnerable to single failures, including single active component failures. This would not have been acceptable design if the plant had been licensed for cold shutdown. The NRC has continued to recognize the fact that older plants were licensed for hot shutdown in the wording used in subsequent regulations such as Appendix R to 10 CFR 50. Appendix R uses the term "safe shutdown" and allows 72 hours to repair damaged equipment that is needed to achieve cold shutdown (Ref. 10.2).

The FitzPatrick plant has the capability to achieve cold shutdown without the use of the RHR system in the shutdown cooling mode. This is the Alternate Shutdown Cooling Mode which consists of depressurizing with the SRVs and injecting with LPCI (Ref. 10.19). The vessel refloods and two-phase flow leaves the reactor vessel and returns to the suppression pool via the SRVs.

Hot shutdown from any normal operating state is achieved by the insertion of the control rods and automatic actuation of the ECCS. At that point, operator action may be taken to ensure long term core cooling and containment cooling. This is discussed further below.

10.3 Original Licensing Basis of the HPCI System

The original HPCI system licensing basis is described in Section 6.5.3 of the Original FSAR (Ref. 10.3). Although this basis has been superceded by the requirements of 10 CFR 50.46 and Appendix K, it indicates that HPCI only needed to operate for a brief period of time to perform its intended safety function. Section 6.5.3 of the Original FSAR states:

> "The upper limit of the HPCI system capability [is] defined as the largest break for which the HPCI system can protect the core for a period of at least 1000 sec[onds]..."

This limit is illustrated in Figure 6.3-1 of the Original FSAR (and also Figure 6.3-1 of the UFSAR).

Although HPCI is now expected to have the capability to depressurize the reactor without help from the ADS system, the original licensing basis shows that HPCI was expected to have a short operating time. In fact, HPCI was credited with successfully mitigating the break if it could do so for only 1000 seconds.

10.4 Design Basis of the HPCI System

NEDO-10329 "Loss-of-Coolant Accident & Emergency Cooling Models for General Electric Boiling Water Reactors" (Ref. 10.4) states:

> "A small break is characterized by the maintenance of nucleate boiling until virtually all the stored energy in the core is removed before a deterioration in cooling capability, which for small breaks occurs when water level drops and uncovers the core region."

And

> "It can be seen that, as long as core flow is sufficiently high to maintain nucleate boiling for approximately three fuel time constants (about 30 seconds), essentially all of the stored energy can be removed from the fuel."

And

> "The small break...is known... that sufficient core flow is maintained at least until the stored energy has been removed from the core."

Thus, HPCI fulfills its mission as soon as it begins injecting and maintains the core covered. At that point, the core is being adequately cooled and hot shutdown has been achieved. The operators can then take manual actions for the transition to cold shutdown.

GE Auxiliary Systems Data Book (ECC) Document 257HA791 Rev. 6 (Ref.10. 5) describes the FitzPatrick ECCS – LPCI, Core Spray, HPCI and ADS. It states:

> "One full Core Spray System is required for long term core cooling (beyond 10 minutes after the accident)...."

It is clear that, for most small break accidents, HPCI was expected to operate for a short period of time until the operators could begin to cool down to cold shutdown.

10.5 Industry Standards

ANSI/ANS 52.1-1983 and ANSI/AND 58.9-1981 (Refs. 10.6 and 10.7) both state that:

> "...for the purposes of design of the emergency core cooling and containment spray systems, the short term shall be considered to terminate upon transfer of these systems to the long term cooling mode."

ANS 58.9 further states:

> " For BWRs, the long term cooling mode starts when the suppression pool cooling commences."

For BWRs, including FitzPatrick, the suppression pool cooling mode is manually initiated and is assumed for analysis to begin at 10 minutes following the LOCA. (In all likelihood, use of the EOPs would shorten this time period.) These are newer standards that have not been specifically applied to the FitzPatrick plant. However, they clearly demonstrate that it is recognized that once the ECCS have automatically actuated and have established core cooling, it is appropriate to credit operator action to provide for long term decay heat removal and protection of the containment. Therefore, it is reasonable to assume and to take credit for operator actions to depressurize the reactor and not remain at elevated temperatures and pressures. This is discussed further in Sections 6 and 11.

10.6 HPCI & ADS Mission Times for Environmental Qualification Purposes

Per 10 CFR 50.49 (Ref. 10.8), safety related electrical equipment and certain non-safety related and post-accident monitoring equipment are required to be environmentally qualified to mitigate design basis accidents (DBAs) and design basis events (DBEs) that create harsh environments. The Environmental Qualification Component List Validation Project clarified what plant components are required to be environmentally qualified and established the bases for qualification (Ref. 10.9). Appendix C of the report contains a set of matrices titled "System Safety Functions vs. Events" that define the safety functions performed

by each system that are required to mitigate the DBEs that create harsh environments. Appendix D of the report contains a set of matrices titled "System Safety Functions vs. Operating Times" that document the expected operating times for each system safety function.

The matrices developed during the EQ Component List Validation Project were incorporated into Attachments 2, 3 and 4 of JAF Procedure No. EDP-20 (Ref. 10.10). These Attachments are periodically updated based on new or revised design basis documentation.

10.6.1 HPCI Post-LOCA System Operability Requirements

Per Reference 10.10, Appendix C, System Safety Function (SSF) 23a, High Pressure Core Cooling was required to mitigate a LOCA or Rod Drop Accident (RDA). JAF-SE-96-069 (Reference 10.11) states that the HPCI system is not required to mitigate a RDA, therefore EDP-20, Attachment 2 was revised and deleted this requirement.

The post-accident required operating time for SSF 23a was determined to be eight hours (Ref. 10.10, Appendix D). The basis for the 8-hour operating time was originally documented in EQ Reference No. 101, in the form of an EDP-3 Design Review of the EDP-20 evaluation performed on HPCI System Essential Electrical Components, approved April 6, 1987 (Reference 10.12). Per the attached evaluation, the most conservative event for determining HPCI operating time was determined to be a small break LOCA (<0.1 ft^2). For this accident, HPCI alone can provide adequate make-up to maintain reactor pressure and level. At the time this evaluation was performed in April 1987, F-AOP-39 required the reactor to be shutdown manually per F-OP-65, and established a maximum cool down rate of 60°F/hr (now 80° F/hr). Therefore, the time to cool down from 545°F to 212°F before switching over to low pressure cooling systems was calculated to be 5.55 hours. For conservatism, 2.45 hours was added to arrive at the 8-hour duration. At higher cool down rates the minimum cool down period would be shorter, and the HPCI operating time would be less than 8 hours. The cooldown rate could be as short as 3.3 hours based on the maximum cooldown rate of 100° F/hr, as limited by the Technical Specifications (Ref. 10.18). Therefore, the HPCI essential electrical components required to operate to provide HPCI are required to be environmentally qualified for 8 hours. The technical evaluation demonstrating qualification of HPCI essential electrical components was documented in EQ Reference No. 335 (Ref. 10.13).

The HPCI essential electrical components were subsequently deleted from the JAF EQ Program per EDP-20 evaluation based on JAF-CALC-HPCI-00820 (Ref. 10.14) because operation of the HPCI system following a small break LOCA would not be challenged by any harsh environmental conditions resulting from the postulated accident.

10.6.2 HPCI Post-HELB System Operability Requirements

Per Reference 10.10, Appendix C, certain components in the HPCI system are required to function to isolate a HPCI/RHR steam line break in the Reactor Building based on high area temperature (SSF 23b), high steam flow (SSF 23c), or low steam pressure (SSF 23d). Therefore, the HPCI system would be rendered inoperable by design (Ref. 10.12). Additionally, a RCIC or RWCU line break may also trip the HPCI steam line automatic isolation circuitry on high area temperature and isolate the HPCI steam line. The post-accident required operating time for these safety functions is 1 hour (Ref. 10.10, Appendix D).

Following a postulated HELB in the Reactor Building, the operator may initiate a reactor scram. However, no postulated HELBs outside Primary Containment will cause an automatic reactor scram (Ref. 10.15). A main steam line break (MSLB) is considered one of the Design Basis Accidents – not a HELB. Manual operation of the HPCI system may be used to maintain reactor water level if available, however this is not the design basis of the HPCI system (Ref. 10.12). Other safety related systems would be available to shutdown and cool down the reactor.

The maximum post-accident required operating time for the HPCI System essential electrical components to mitigate a LOCA was originally determined to be 8 hours, which is based on mitigation of a small break LOCA (< 0.1 ft^2). The post-accident required operating time for certain HPCI components required to mitigate a HELB in the Reactor Building is 1 hour.

10.6.3 ADS Post-Accident System Operability Requirements

Per Reference 10.10, Appendix C, SSF-02a, manual or automatic depressurization is required to mitigate a LOCA, RDA, MSLB and a Reactor Building HELB. The safety related electrical equipment required to perform this safety function are the SRV solenoid valves.

The required post-accident operating time for SSF-02a was determined to be 100 days (Ref.10.10, Appendix D). The 100 day operating time is based on NUREG 0737, Task II.K.3.28. The EQ Qualification Bases Documentation states that the original design bases for ADS would result in depressurization in 6 - 24 hours following a small break LOCA, however the operating time was conservatively increased to 100 days based on NUREG-0737 (Reference 10.12). It should be noted that the duration of a large break LOCA (≥ 0.5ft^2) was conservatively determined to be 1 hour for environmental qualification purposes (Ref. 10.16). The acceptability of a 1-hour post-LOCA required operating time for large breaks was evaluated in JAF-SE-96-016 (Ref. 10.17).

11.0 OPERATOR ACTIONS

11.1 Technical Specification Requirements

The FitzPatrick Technical Specifications (TSs) have always contained suppression pool temperature limitations for normal and off-normal conditions. The original TS contained TS 3.7.A.1.a which gives a temperature limit of 95° F during normal operation. The original TS 3.7.A.d specified a maximum temperature of 130° F during HPCI, RCIC or relief valve operation. Failure to meet the Tech Spec meant that the reactor had to be brought to cold shutdown within 24 hours. The 130° F limit was based on a DBA LOCA pool temperature increase of 40° F and a final pool maximum temperature of 170° F. This requirement was to ensure stable steam condensation.

The NRC modified the FitzPatrick TS in Amendment 16 dated March 29, 1976. This amendment retained the 95° F limit for normal operation as TS 3.7.A.1.c (1) and added three other limits in TS 3.7.A.c (2), (3) and (4). TS 3.7.A.c (2) provides pool temperature limits for testing. TS 3.7.A.c (3) and (4) specify pool temperature limits that require that the reactor be scrammed at 110° F and depressurized (at normal cooldown rates) at 120° F.

These suppression pool temperature limits apply during accidents and the requirement to depressurize at 120° F is contained in EOP Support Procedure EP-1 (Ref. 11.1). Therefore, unless restrained by the EOPs for conditions outside of the FitzPatrick design and licensing basis, the reactor depressurization would begin at a maximum pool temperature of 120° F.

11.2 Emergency Procedure Requirements

Our current EOP generic guidelines (EPG Rev. 4) provide basic "ground rules" for operator actions. (Emergency Procedure Guidelines/Severe Accident Management Guidelines Rev. 1 were implemented following the October 1998 refueling outage.) Some of these rules include:

- "...operator actions are keyed to certain plant parameters or symptoms. Actions are specified as appropriate to restore and maintain these key plant parameters to within limits which define safe plant conditions."

- "The operator actions specified are consistent with the manner in which control room operators actually operate plants..."

- "...the EPGs address a spectrum of conditions including those more severe as well as those less severe than were considered in developing the design basis."

- " Although guidance is provided for responding to plant conditions which may extend to and beyond the design basis of the plant, there is no intent or proposal to extend any design basis beyond that which is currently established."

- "Operator actions, limits, and action levels are based on realistically bounding best-estimate engineering calculations as opposed to traditional licensing or design-basis analytical methods and assumptions."

- "The best possible operational guidance is specified, irrespective of licensing or design-basis assumptions or commitments..."

11.3 Operator Actions for Specific Line Breaks

The scenarios described in the DERs involve the assumption that ADS will not automatically operate, but SRVs would function on pressure or could be opened by manual operator action. Loss of offsite power is also assumed, leaving only power from vital busses. Based on direction provided in the EOPs and training provided to the FitzPatrick operators in their use, operator responses to certain type pipe breaks can be expected. These events and the expected operator actions are described below.

11.3.1 Feedwater System Break

Operators are trained to respond to many variations of breaks and degraded RPV injection capability. There is a scenario available that involves a severe Feedwater injection line rupture in the steam tunnel. By choosing Feedwater Line B for this problem, HPCI injection into the RPV is also removed because HPCI injects via Feed line B. In this case RPV water level would rapidly drop to well below 177 inches above the top of active fuel (TAF) requiring use of EOP-2, RPV Control. If the operating history of the core resulted in a significant decay heat generation rate, the remaining high pressure injection systems (Reactor Core Isolation Cooling - RCIC, Control Rod Drive - CRD, and Standby Liquid Control - SLC) might not be able to reverse the level trend. This is because steam mass is released from the reactor pressure vessel (RPV) to control pressure by the Main Turbine Bypass Valves (BPVs) or the SRVs.

Operators would be expected to:

- Perform initial scram response actions – assuming a successful scram
- Bypass automatic ADS actuation
- Stabilize RPV pressure between approximately 900 – 1080 psig with BPVs or SRVs. Depending on the event and power history, RCIC, SRVs, main steam line drains, Reactor Water Cleanup or other equipment may be used. The worst case for this scenario would be an inability to use

BPVs. SRVs or other means would then be initially used manually to establish pressure control. Torus water temperature would rise to greater than 95° F and could approach 120° F, but would not threaten the Heat Capacity Temperature Limit.

- Stabilize RPV water level with one or more remaining high quality, high pressure injection systems (in this case RCIC, CRD). The preferred level range is 177 to 222.5 inches above the TAF; if this is not possible then directions are to maintain level greater than zero inches above the TAF. This degradation would permit use of SLC as an additional high pressure injection source.

Once RPV pressure is stabilized with SRVs, RPV pressure control protocol per EOP-2 requires initiation of a cooldown at less than 100° F per hour. The equipment used would depend upon the event and what is available. This could be delayed by the Shift Manager pending some higher priority action or temporary shortage of control room Reactor Operators, but it is expected to be started in a timely manner and not delayed just because the reactor is stable at that pressure. The actual rate would depend on the specific event and is established by the Shift Manager.

EOP-2 would permit use of the previously mentioned high pressure RPV injection systems to maintain level above the TAF even if normal values could not be achieved. However, if level continued to decrease, ADS would be overridden and low pressure systems would be prepared for an eventual Emergency RPV Depressurization (using SRVs to the torus). This would be directed when RPV level reached the TAF, provided a source of injection water is available. If a crew recognized that emergency depressurization was likely to be required, then EOP-2 would permit a rapid depressurization at greater than 100° F per hour to the main condenser (if the main steam isolation valves were open) using the BPVs or other means identified in the EOPs. However, the minimum acceptable performance for operating crews would be to conduct the SRV Emergency Depressurization at the TAF per EOP-8. Restoration of RPV level would be with low pressure ECCS.

Torus conditions are controlled by EOP-4. When the suppression pool temperature limit of 95° F is exceeded then all available torus cooling is required using the RHR System. At 110° F, EOP-4 requires the operators to scram the plant and enter EOP-2 to avoid exceeding the Boron Injection Initiation Temperature (BIIT). (If the BIIT is exceeded boron injection is required.) EOP-4 then requires the operators to maintain the plant below the Heat Capacity Temperature Limit. For a successful scram scenario, this limit would not be threatened and normal torus cooling and the expected RPV cooldown and depressurization would place the reactor and containment in their lowest energy state in a reasonable amount of time.

11.3.2 Small Break (less than the capacity of HPCI)

The basic sequence of events of this accident would be similar to the previously described, only under much less severe conditions. Under some previous assumptions: (1) a successful scram and (2) degraded BPV response, and adding (3) the small break inside the primary containment the expected sequence of operator actions would be as follows:

- Scram response per AOP-1
- RPV pressure stabilization below 1080 psig – using the main condenser and BPVs if available, or SRVs with heat addition to the torus, along with that from the small break
- RPV water level control using HPCI, which would have automatically initiated at greater than 2.7 psig drywell pressure.

In this case the amount of available injection is more than necessary for the steam being removed by the break and also by RPV pressure control. EOP-2 directions for RPV level begin with a range of 177 to 222.5 inches above the TAF. In order to preclude HPCI tripping multiple times on high level followed by manual or auto restarts, operators would be expected to control RPV level by controlling the injection rate. For HPCI this is accomplished by reducing the injection rate to a value matching steam usage (such that the RPV water level is maintained at a steady level). HPCI controls provide multiple acceptable ways to accomplish this as long as turbine RPM remain above a minimum value (2100 rpm). If the injection rate could not be dropped enough to stop the level rise then:

- RCIC could be used instead of HPCI, or
- HPCI could still be cycled on and off between 177 and 222.5 inches above TAF.

In either event the operators are expected to actively attempt to control water level within an acceptable range.

For RPV pressure, it would again be expected that a cooldown would be commenced in accordance with EOP-2. Torus water temperature would be controlled as described above.

EOPs are symptom oriented and independent of any particular event. They are developed to direct operators to take appropriate actions to control RPV and primary containment parameters in response to a wide range of occurrences within and outside of design bases. By virtue of training to implement the EOPs in a knowledgeable manner, licensed operators can be expected to manage suppression pool temperatures appropriately after a LOCA.

12.0 SAFETY ASSESSMENT OF THE HPCI/ADS CONFIGURATION

12.1 Conclusion

The hypothetical failure of a wireway coincident with a LOCA and a LOOP is not a credible event. This is true even though no credit is taken for HPCI injection, HPCI recirculation, Reactor Core Isolation Cooling (RCIC) injection, RCIC recirculation, Control Rod Drive (CRD) injection, backfeeding from the 345 kV lines, restoration of offsite power, or use of the alternate shutdown panels. No credit is taken for the RHR steam condensing mode, although this is a function of the RHR system.

12.2 Probabilistic Analysis

A probabilistic analysis has been performed to evaluate the core damage frequency of a small break LOCA coincident with a loss of offsite power and an electrical fault in a raceway (Ref. 12.1). The core damage frequency contributions of each event are:

- the frequency of a small break LOCA is 3.00×10^{-3} per year
- the unavailability of offsite power is 2.47×10^{-4} and,
- the probability of a sustained electrical fault on a cable with a 24 hour vulnerability is 3.12×10^{-6}.

A mission time of 24 hours was assumed for the vulnerability of SRV cables to electrical faults. The event probabilities are multiplied by the LOCA frequency since they are hypothesized to occur simultaneously. This gives a core damage frequency of **2.31×10^{-12}** per year. When compared to the IPE core damage frequency of **2.4×10^{-6}** per year, this particular scenario is insignificant. This is true even if the loss of offsite power were not considered. In that case, the core damage frequency would be **9.36 E-9.**

The overall contribution of the hypothetical scenario is several orders of magnitude below that which would require remedial action in accordance with EPRI guidelines (Ref.12.2).

12.3 Deterministic Engineering Evaluation

The licensing and design basis of the FitzPatrick electrical systems, and specifically the requirements for cables and raceways, permit the intermixing of safeguard (safety related) and non-safeguard (non-safety related) cabling. UFSAR Section 8.5.4.2 states:

> "Cables for nonsafeguard service may be run in the same raceway with the engineered safeguard cabling, provided that the voltage levels are in

the same range. All nonsafeguard cabling is of the same quality as the safeguard cabling and is installed in accordance with the same criteria as the safeguard cabling to ensure that the nonsafeguard circuits do not compromise the safeguard circuits."

Since non-safety related circuits are designed and installed to the same general electrical criteria as safety related circuits, it is unlikely that the cable will overheat and damage adjoining cables. Therefore even if failures of non-safety related cables cannot be absolutely precluded, they are unlikely. This is also consistent with NRC requirements for assumptions to be made for accident analysis. The NRC requires that non-safety related equipment be assumed to be unavailable during a LOCA. Non-safety related equipment is not assumed to fail destructively unless the failure is a consequence of the accident.

Although not required to demonstrate conformance to the licensing and design basis, the Authority employed an engineering consultant to evaluate the ADS wireway(s) in question and to determine if there are any credible electrical faults or external hazards that could prevent the ADS from performing its design function. Based upon the consultant's report (Ref. 5.14), NYPA Design Engineering concluded that there are no credible failures that could destroy the wireway for the ADS cabinet to the SRV solenoids, with the exception of 93 cables. Design Engineering has evaluated 85 of the cables and concluded that they do not present a fault that could prevent ADS from performing its safety function. The remaining 8 cables were evaluated as part of an operability assessment (A.1.2.3 of this report). Design Engineering concluded that the maximum credible fault involving these cables would not prevent ADS from functioning. (See Recommendation 13.2.24).

Therefore, even though not required by the design or licensing basis, no credible internal or external hazard to the ADS wireways will prevent ADS from performing its safety function.

13. 0 CONCLUSIONS AND RECOMMENDATIONS

13.1 Conclusions

13.1.1 Wireway Failures Coincident with LOCAs

The single failure criterion for ECCS does not require electrical faults that damage entire wireways to be postulated coincident with LOCAs.

Events external to safety related systems were considered in the design of the plant. These postulated events included earthquakes, missiles, extreme weather phenomena, and electrical faults in wireways. The separation criteria defined in GE design specifications ensured that no single postulated event could result in the loss of redundant divisions. Success in handling such an event means that no more than a single division is damaged or destroyed and that the plant could be safely shut down with safety related equipment.

Section 5.5 describes how electrical fires in wireways factor into the plant design. They are considered design basis events and the success criterion is that "No single design basis event shall disable an automatic protective function, i.e. Engineered Safeguards Systems." Wireway fires are not single failures that must be assumed during a LOCA. There is no regulatory requirement to assume wireway failures (resulting from any cause) as a single active component failure coincident with LOCAs.

A GE specification deals with this subject and is discussed in Section 5.5.2 of this report.

13.1.2 Single Failure Assumptions for LOCA Analyses

Single active component failures are the only single failures that are postulated to occur coincident with LOCAs. No other type of single failure needs to be considered coincident with LOCAs.

The only single failures that are assumed coincident with LOCAs are single active component failures. (Other types of failures in other systems are precluded or mitigated by design.) Single active component failures are assumed in BWR LOCA models approved by the NRC. The NRC, in the Interim Acceptance Criteria for Emergency Core Cooling Systems (Ref. 5.16), stated that:

> "The combination of systems used for analysis should be ... as indicated in Table 2-1 of ... NEDO-10329."

This table is largely based on single active component failures. Subsequent NRC documents, such as SECY 83-472 (Ref. 5.25), confirm that the NRC means that single failures for LOCA analyses are single active component failures.

As applied to the FitzPatrick, this means that ADS or SRVs operated manually will always be available following a LOCA. The number assumed available is identified in the SAFER/GESTR LOCA analysis (Ref. 5.23).

LOCA models used for FitzPatrick are based on the assumption of single active component failures coincident with a LOCA, beginning with the NEDO-10329 model (Ref. 5.17). The failure of a station battery is also assumed. NEDO-10329 and subsequent GE LOCA models are generic to one or more classes of BWRs. They have been reviewed and accepted by the AEC and NRC on a generic basis. The NRC has further accepted the application of each model and the specific single active component failures assumed in the analysis, for every BWR core reload (thirteen for FitzPatrick alone).

13.1.3 NRC (AEC) Review and Acceptance of the ADS Design

The AEC concluded that the FitzPatrick Protection Systems, which include the ADS instrument and control logic, are acceptable when compared to the General Design Criteria and IEEE-279-1968.

Section 5.3.1.3 discusses the NRC criteria for ECCS systems as well as the single failure criterion as used in 10 CFR 50 Appendices A and K. This NRC finding is consistent with the NRC definitions as written in these regulations, as well as subsequent NRC applications of the term "single failure criterion".

The AEC based this conclusion on reviews of ADS schematic diagrams and the ADS installation in the plant (Refs.13.6, 13.7, 13.8 and 13.9). This review included a modification to the ADS design originally requested by the Advisory Committee on Reactor Safety. This modification to the ADS power supply logic adds a feature that will automatically transfer power for the ADS actuation circuits and the B trip system to a redundant power supply in the event of a failure of its normal power supply.

13.1.4 Redundancy and Interdependency of ADS and HPCI

HPCI and ADS perform the redundant ECCS function of depressurizing the reactor following small break LOCAs.

HPCI and ADS are identified in GE design specifications as redundant systems, are physically separated accordingly and have always been regarded as redundant for the FitzPatrick plant. (It should be noted that inadequate physical

separation of HPCI and ADS cables was discovered early in plant life and corrected by modification).

HPCI was added to the BWR 4 design in response to concerns about common mode failure of ADS valves. HPCI injects coolant into the vessel and keeps the fuel covered for small break LOCAs. This ensures adequate core cooling and keeps the calculated peak cladding temperature (PCT) within acceptable limits. The ADS ensures adequate core cooling for small break LOCAs by depressurizing the reactor so that low pressure ECC systems can inject water and cool the core. The core is uncovered in the process and the fuel heats up until the low pressure systems inject and terminate the heatup. This results in a PCT higher than the PCT that occurs when HPCI is available.

GE was questioned about the ability of HPCI to depressurize the reactor without assistance from ADS. GE did tests to demonstrate that HPCI could depressurize the reactor without assistance and summarized them in APED-5608 (Ref.13.1). However, GE has always considered the ECCS to be an integrated combination of systems and has always analyzed them as functioning in combination with each other. Since single active component failures (and a station battery failure) are the only failures considered in LOCA analyses, ADS valves are always assumed to be available and the analysis takes credit for them. In addition, the failure of HPCI is the limiting failure for small break since it forces the use of ADS which results in a higher PCT.

For these reasons, GE LOCA analyses (depending on the event) sometimes show ADS and HPCI functioning together (Refs. 5.17, 5.21, 5.22 and 5.23). This does not mean that HPCI requires the assistance of ADS – only that such assistance is available and credited in calculations of PCT and other ECCS acceptance criteria.

13.1.5 Credibility of the Hypothetical HPCI Line Break

A break in the HPCI injection path that will prevent HPCI flow from reaching the reactor, without depressurizing the reactor, is not credible. No physical mechanism exists for a break of this size to occur in the HPCI injection path.

Section 8.0 shows that there is no credible physical break in the "B" Feedwater line, or the HPCI line itself, that will give a break sized to equal the HPCI flow rate. The break will either be well within HPCI capability or will result in sudden failure or a break of the pipe.

13.1.6 Credibility of the Hypothetical Scenario of Small Break and ADS Wireway Failure

The core damage frequency of a small break LOCA coincident with a loss of offsite power and an electrical fault in a wireway is 2.31 x 10^{-12} per year. When compared to the IPE of 2.4 x 10^{-6} per year, this particular scenario is insignificant.

Section 12.1 describes a probabilistic analysis of the hypothetical scenario. This analysis shows that the probability of the scenario is so small that it need not be considered.

It should be noted that no credit is given for the use of Reactor Core Isolation Cooling (RCIC) or the completely independent remote shutdown panel from which the SRVs can be manually operated even if the wireway is destroyed. Inclusion of these in the analysis would result in a calculated core damage frequency several orders of magnitude <u>less</u> than 10^{-12}, which itself is considered insignificant.

13.1.7 UFSAR Descriptions of ADS, HPCI and LOCA Analyses

The UFSAR descriptions of ADS, HPCI, design basis events, design basis accidents and LOCA models are unclear and must be updated.

This report, in part, was necessary because the UFSAR descriptions of the ECCS, design basis events, design basis accidents and accident analyses were not as clear or thorough as they could be. The information in this report should be used as the basis for a Nuclear Safety Evaluation for upgrading the UFSAR (see Recommendation 13.2.4).

13.1.8 Condensate Storage Tank (CST) and HPCI Suction Line

The HPCI suction line to the CSTs and the below-grade portion of the CSTs must be reclassified as nuclear safety-related and QA Category I.

HPCI is aligned to take suction from the CSTs following a LOCA. This was part of the original design and is currently part of the FitzPatrick LOCA analysis. The EOPs also rely on this lineup (see Recommendation 13.2.20).

13.1.9 GE Services Information Letter (SIL) No. 615 – ADS/HPCI Functional Redundancy

GE SIL No. 615 is not clear with regard to the depressurization capability of HPCI and the redundancy or interdependency of HPCI and ADS.

The conclusions reached in this report do not agree with some of the statements in the SIL. The SIL seems to imply that ADS is needed to assist HPCI. This report concludes that it is available but not required. See Recommendation 13.2.15.

13.1.10 NYPA Letter (JPN-97-003) to the NRC Concerning GL 96-06 Thermal Pressurization

JPN-96-06 contains erroneous conclusions about the need for, and potential timing of, the transfer of HPCI suction from the CST to the suppression pool.

The subject letter concludes that the transfer of the HPCI suction from the Condensate Storage Tank to the suppression pool will not be needed after significant heating of the suppression pool has occurred. This is not correct for some accident scenarios. The EOPs also credit use of the CSTs. The letter was updated. See Recommendation 13.2.14.

13.2 Recommendations

13.2.1 Small Break Suppression Pool Cooling Capability

Verify that the full complement of equipment for suppression pool cooling can maintain the suppression pool temperature within required limits for small break LOCAs of any size. (ACTS-99-42695)

This report concludes that wireway failures need not be postulated coincident with a LOCA. Therefore, even in the hypothetical event of a small break and a complete loss of ADS, a full complement of equipment for suppression pool cooling would remain operable. This same complement of equipment is capable of removing decay heat from the core and cooling containment following a large break LOCA. Following a small break LOCA, the stored energy and decay heat are deposited in containment at a slower rate and over a longer period of time (both depending on the size of the break). Therefore, the full complement of equipment for suppression pool cooling should be able to cope with a small break LOCA of any size. This should be verified – if necessary using realistic RHR heat exchanger fouling factors.

13.2.2 Redundancy and Single Failure Criterion as Applied to FitzPatrick

Redundancy and the single failure criterion should be defined as they are applied to the FitzPatrick plant for onsite and offsite electrical power systems. (ACTS-99-42696)

This report addresses the issue of single failure as it specifically applies to FitzPatrick protection and ECC systems. This report documents the following conclusions: (1) protection systems were designed to perform their intended function even assuming a single active or passive failure within the system; (2) only single active component failures of ECCS equipment (and failure of a station battery) are assumed in LOCA analyses; and, (3) wireway failures are not assumed as single active component failures in LOCA analyses.

Electrical power systems were not specifically reviewed as part of this evaluation, nor addressed in this report. However, the conclusion regarding wireway failures also applies to electrical power systems, i.e. failures of electrical power wireways are not assumed coincident with a LOCA. The evaluation of electrical power systems should be extended to include the redundancy and single failure capabilities designed into the system.

13.2.3 An Engineering Analysis and Nuclear Safety Evaluation (NSE) for As - built ADS Cable Routing and Installation

An engineering analysis and NSE should be prepared to evaluate and resolve the discrepancy between the UFSAR which describes ADS as conforming to NEDO-10139 and the actual installation which does not (the ADS cables are not routed in independent conduit). (ACTS-99-42697)

The UFSAR implies that the ADS system conforms to NEDO-10139 (Ref. 5.10). That document states that the ADS circuits are run in independent conduits from the cabinet to the containment where they enter the drywell through separate penetrations. In the FitzPatrick plant, the ADS cables are run in a common open wireway with non-safety related cables and they enter the drywell through a single electrical penetration.

An engineering analysis should be performed to assess the acceptability of the as-built configuration both inside and outside the containment. The UFSAR should be updated as required.

13.2.4 UFSAR Corrections and Clarifications

The UFSAR contains errors, inaccuracies and vague statements that must be corrected. (ACTS-99-42702)

Information contained in this report as well as information uncovered in researching the issues it addresses conflicts with the UFSAR. The UFSAR must be revised to resolve these during the next update, as required by 10 CFR 50.71e (Ref. 13.2). The update should include the items identified in Ref. 13.3.

13.2.5 References to Regulations, Regulatory Documents, Codes and Standards in the UFSAR

Dates, editions or revisions should be added to all regulatory and technical document citations in the UFSAR. (ACTS-99-42703)

The UFSAR contains many references to NRC regulations, Regulatory Guides, and industry codes and standards. Some of these documents are referenced without a revision, edition or date. These should be added since they are needed to specify the exact requirements that apply to FitzPatrick.

13.2.6 Conformance to NRC Regulations and Regulatory Documents

The UFSAR should be updated to fully and clearly describe the dates or revisions of NRC regulatory requirements and guidance applicable to FitzPatrick and the extent of conformance to them, particularly the General Design Criteria (GDC), NRC regulations and Regulatory Guides. (ACTS-99-42704)

FitzPatrick was designed and constructed to various regulatory requirements and guidance that have been superceded by those widely in use today. This includes even the most fundamental NRC requirements such as the GDC, ECCS licensing and design criteria and LOCA models and evaluations. As these regulatory criteria evolved, FitzPatrick was often compared or evaluated to requirements that superceded those to which the plant was built. This has resulted in confusion that gave rise to some of the issues addressed in this report.

13.2.7 Availability of Documents Referenced in the UFSAR

Copies of all documents referenced in the UFSAR should be obtained and placed in permanent Authority archives. (ACTS-99-42705)

A few documents referenced in the UFSAR had to be obtained outside the Authority. A complete list of all documents referenced in the UFSAR should be compiled and copies of the documents obtained. This is being done for the

Technical Specifications as part of the Improved Technical Specification (ITS) Project. See Recommendation 13.2 8 for review and approval of these documents.

13.2.8 Review and Acceptance of Documents Referenced in the UFSAR

All generic and topical documents referenced in the UFSAR should be formally reviewed and accepted by the Authority in accordance with appropriate procedures regardless of their age. (ACTS-99-42746)

As noted in Recommendation 13.2.6, the UFSAR refers to documents that have become part of the design basis of the plant but had to be obtained outside the Authority. Some of these documents include topical reports for GE LOCA models that have become part of the current FitzPatrick licensing and design basis. These documents or reference to them were accepted by the Authority in accordance with the process or procedure employed at the time. Prior to using these documents again, they should receive a documented review and approval in accordance with current Authority procedures.

13.2.9 Licensing Basis Documents for Design Basis Events, Transients and Accidents

Licensing Basis Documents (LBDs) should be developed for Design Basis Events (DBEs), Transients and Design Basis Accidents (DBAs) and should be used to update the UFSAR (especially Section 12.2) and the Design Basis Documents (DBDs). (ACTS-99-42706)

Section 12.2 of the UFSAR describes DBEs, Abnormal Operational Transients (AOTs) and DBAs to some extent. A more detailed and extensive document or documents should be developed to fully describe these. The LBDs should identify the postulated occurrences (DBAs, DBEs & AOTs) for which the plant was designed and licensed. The LBDs should specify both the assumptions used in evaluating the occurrences as well as the "success criteria" for coping with each one. This information is needed to address licensing basis issues such as the ones addressed in this report.

13.2.10 Generic NRC Regulatory Licensing and Design Requirements

NRC regulatory requirements that apply to the entire plant design, that apply to many systems or that have cross-disciplinary application should be described in Licensing Basis Documents (LBDs). (ACTS-99-42713)

Many NRC regulatory requirements and commitments have broad and general application to plant design. Some of these are best captured in "topical" LBDs (such as the DBD for fire protection) based on the subject rather than in many DBDs for individual systems. Requirements in this category include containment isolation, single failure, design basis accidents, LOCA models, etc.

13.2.11 UFSAR Section 12.2 – Safety Related Functional Analysis (SRFA)

The Nuclear Safety Evaluation (NSE) and the SRFA should be reviewed and, if necessary, supplemented with additional information. (ACTS-99-42716)

The NSE which evaluated and accepted the Safety Related Functional Analysis has been described by several engineers as lacking sufficient detail. The appropriate engineering manager should review the SRFA and the NSE to determine if they should be upgraded. If determined to be necessary, the upgrade should be performed.

13.2.12 Procedure for Resolving Topical Licensing and Design Basis Issues

A process should be developed and implemented for resolving licensing and design basis issues, such as the ones addressed in this report. (ACTS-99-42719)

The process for resolving the issues, such as those addressed in this report, could be improved substantially. This would make resolution of future issues quicker, more efficient and more economical.

13.2.13 Indian Point 3

Appropriate personnel should review these recommendations for their applicability to Indian Point 3. (ACTS-99-42717)

Some of these recommendations might apply to Indian Point 3. Appropriate personnel should review these recommendations to ensure that similar situations either don't exist at Indian Point 3 or are corrected.

13.2.14 NYPA Letter to the NRC Concerning Thermal Pressurization

JPN-97-003 should be revised to correct erroneous information concerning thermal pressurization as it applies to the transfer of HPCI suction from the CST to the suppression pool.

The subject letter contains information that has recently been determined to be incorrect (See Conclusion 13.2.14). A revision to this letter has been sent to the NRC (Ref. 13.4). Testing committed to in the letter was being tracked by ACTS Item 98-34168 and has been completed (Ref. 13.10). This recommendation is completed.

13.2.15 General Electric (GE) Service Information Letter (SIL) No. 615

The Conclusions of this report and DER 98-01213 are inconsistent with the recommendations of SIL No. 615. GE should be asked to resolve the inconsistencies.

GE SIL No. 615 is not clear with regard to the functions of HPCI and ADS (See Conclusion 13.1.9). The SIL seems to imply that ADS is needed to assist HPCI. This report concludes that ADS is available but not required.

This recommendation is withdrawn and need not be completed. This report addresses the issue raised in the SIL and can be used to document closure of the SIL. Sending a letter to GE is unnecesary and is unlikely to result in changes to the SIL, which was written for generic applicability.

13.2.16 DER 98-00999 Concerning GE RHR Service Water Temperature Analysis

DER 98-00999 indicates that there are errors in GE RHR Service Water Temperature Analysis Report (Ref. 13.5). GE should be asked to correct these errors. (ACTS-99-42721)

The GE report includes general statements about the temperature limits of cooling water for the HPCI pump (e.g., the ability of the pump to operate with cooling water above 140°F). Analyses should be done to verify the statements or they should be corrected.

13.2.17 Reactor Recirculation Pump Seal Failure

The rate of loss of reactor coolant due to a recirc pump seal failure is not known. This should be determined to ensure that it could not create a break that could divert all of the HPCI flow.

This recommendation is withdrawn and need not be completed. Leakage through a recirc pump seal would be indicated and alarmed in the Control Room and operators can take action to isolate the leak. In the event of gross failure of both seals, a breakdown bushing would limit leakage. Also, HPCI flow would reach the reactor vessel.

13.2.18 ADS Cables in the Drywell

A Nuclear Safety Evaluation should be performed on the as-built configuration of the ADS cables in the drywell to determine if it is acceptable as is or needs to be modified.

A recent inspection determined that certain ADS/SRV cables in the drywell are not encased in conduit, as specified in the plant design basis. This was corrected during the 1998 refuel outage. This Recommendation has been completed.

13.2.19 RHR Steam Condensing Mode

Use of the RHR steam condensing mode has been restricted to events in which the EOPs are entered. Some valves used in this mode may be disabled in normal operation or may not be tested appropriately. A review of changes to the steam condensing mode equipment and procedures should be made to ensure that it would be available if needed.

The RHR steam condensing mode can be used post-accident to remove energy from the reactor and deposit it directly into the ultimate heat sink, rather than the torus. This can be done without using RCIC, or together with RCIC if it is available.

13.2.20 Reclassification of the HPCI Suction Line

The HPCI suction line and Condensate Storage Tank (below grade portion) were declassified from Category I to Category II. This reclassification

should be reversed and the equipment reclassified in accordance with the original design basis of the plant. (ACTS-99-42722)

The subject equipment was designed and installed as Category I, and credit is still taken in accident analyses for it. It was reclassified in error. The equipment should be evaluated and reclassified and the documentation corrected.

13.2.21 Relationship of the Emergency Operating Procedure (EOPs) to The Technical Specification and Licensing Basis

The UFSAR should be updated to clearly define the relationship between the EOPs and the licensing basis of the plant.

The UFSAR identifies EOPs (Section 13.8.2.2) but does not describe how they relate to requirements of the Technical Specifications and the licensing and design basis of the plant. For example, the EOPs allow the operators to depressurize the reactor after an accident using different criteria (or limits) than contained in the Technical Specifications. However, this does not mean that the EOPs supercede the Technical Specifications.

13.2.22 Cooling Water for the HPCI Pump

Consideration should be given to providing a safety-related source of cooling water to the HPCI pump other than the pumped fluid.

The HPCI pump is cooled by the pumped fluid. As the suppression pool heats up (above 140°F) this jeopardizes HPCI pump operability. A cost benefit analysis should be prepared for providing a different source of safety-related cooling water to the pump. (For example, the cooling water return line from a crescent area cooler might possibly be routed through the HPCI pump cooler). This would extend the operable range of the HPCI pump from 140°F to the suppression pool temperature at which adequate NPSH would not be available.

13.2.23 Quality of Non Safety-Related Cable

The original FSAR and the UFSAR state that non safety-related cable is of the same quality and installed in accordance with the same criteria as safety-related cable. This should be verified.

13.2.24 Control and Instrumentation Cables Routed with ADS Cables

93 nonsafety-related cables are routed with ADS cables. 85 of these have been evaluated to ensure that they are not an exposure hazard to the ADS cables. The remaining 8 cables have been evaluated for operability. However, they are not properly protected and should be evaluated to determine if modifications are warranted.

13.2.25 Administrative Controls on Cables in ADS Wireways

EPM evaluated the cables in the ADS wireways for their potential to damage the ADS cables (Ref. 5.14). This evaluation is valid only as long as the ADS wireway configuration doesn't change, or it is updated as changes occur. Procedural controls should be put in place to ensure that the configuration isn't changed or that the evaluation be updated if it is.

14.0 Closure of Deviation/Event Reports (DERs)

This report provides information related to the DERs described in Appendix A. Several DERs can be closed following approval of this report. Others can be closed after this report is approved and when Recommendations made in this report are implemented.

14.1 DERs 97-701 & 1763

DER 97-701 stated that the HPCI system might not be capable of depressurizing the reactor without assistance. It also stated that the ADS system was susceptible to a single raceway failure. Finally it stated that it was not appropriate to rely on ADS and HPCI together for small breaks, since they are redundant systems.

This report concludes that the HPCI system is capable of depressurizing the reactor without assistance (Conclusion 13.1.4). Implementation of Recommendation 13.2.1 will verify this.

Wireway and raceway failures need not be postulated as a single failure coincident with a LOCA (Conclusion 13.1.1).

DER 97-701 can be closed after approval of this report and Recommendation 13.2.1 is completed.

The scenario described in DER 97–1763 is based on the supposition that wireway failures are single failures in LOCA analyses and that a break exactly equivalent to the HPCI flow rate can occur. Wireway failures need not be postulated as single failures coincident with a LOCA (Conclusion 13.1.1). The hypothetical break and overall scenario are not credible (Conclusions 13.1.5 and 13.1.6).

DER-97-1763 can be closed upon approval of this report.

14.2 DERs 98-00999 & 01213

DER 98-0999 states that the GE RHR Service Water temperature analysis is in error concerning HPCI operability and that calculations necessary to demonstrate that the suppression pool can be adequately cooled for small breaks have not been done.

DER 98-0999 is correct concerning the temperature analysis, which should be corrected (See Recommendation 13.2.16). Calculations concerning suppression pool cooling capability will be verified (Recommendation 13.2.1).

DER 98-0999 can be closed after approval of this report and Recommendations 13.2.16 and 13.2.1 are completed.

DER 98-01213 states that GE SIL No. 615 is technically incomplete. This report reaches the same conclusion although not necessarily for the same reasons (Conclusion 13.1.9). The recommendation to notify GE of the Authority's findings (Recommendation 13.2.15) has been withdrawn.

DER 98-01213 can be closed after approval of Revision 1 of this report.

14.3 DERs 97-01226 & 01227

These DERs correctly identify errors in a letter to the NRC (Conclusion 13.1.10). These errors are being addressed at this time.

DERs 98-1226 & 1227 can be closed after approval of this report and Recommendation 13.2.14 is complete.

14.4 DER 98-01873

This DER (dated Aug. 10, 1998) states that the SAFER/GESTR LOCA analysis takes credit for Division A & B systems operating at the same time and that this is not consistent with pre-Appendix K analysis. The DER also states that with the loss of a cable tray, less equipment will be available than was assumed available in the LOCA analysis.

This report concludes that the loss of cable trays need not be postulated coincident with a LOCA (Conclusion 13.1.1). This report also describes the acceptability of the FitzPatrick LOCA analysis and the extent of HPCI/ADS redundancy and physical separation (Conclusions 13.1.2 and 13.1.3).

DER 98-01873 can be closed after approval of this report.

15.0 REFERENCES

1.0 PURPOSE

None

2.0 BACKGROUND

None

3.0 APPROACH TO RESOLUTION OF THE ISSUES

None

4.0 EXECUTIVE SUMMARY

4.1 NYPA memo, S.S. Zulla to J. Gray, concerning the ADS Protection System Boundary, dated May 6, 1999 (SSZ-99-04).

5.0 SINGLE FAILURE CRITERION

5.1. NRC Safety Evaluation by the Office of Nuclear Reactor Regulation Relating to Postulated Battery Power Supply Failure and ECCS Requirements, Commonwealth Edison Company Quad Cities Station Units 1 and 2, Dresden Station Units 2 and 3, Docket Nos. 50-254/265 and 50-237/249, dated October 13,1988.

5.2. Appendix A to 10 CFR 50, "General Design Criteria for Nuclear Power Plants", July 11, 1967.

5.3. Appendix A to 10 CFR 50, "General Design Criteria for Nuclear Power Plants", May 21,1971.

5.4. IEEE-279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," effective August 30, 1968.

5.5. IEEE-279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations."

5.6. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," issued June 1973.

5.7. 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light water nuclear power reactors", February 4, 1974.

5.8. Appendix K to 10 CFR 50, "ECCS evaluation models", February 4, 1974.

5.9. "Criteria for Emergency Core Cooling Systems for Light Water Power Reactors", Interim Policy Statement, June 29,1971.

5.10. "Compliance of Protection Systems to Industry Criteria: General Electric BWR Nuclear Steam Supply System", NEDO-10139, June 1970.

5.11. NRC Letter, Roger S. Boyd of the AEC to A. P. Bray of General Electric, December 13, 1971.

5.12. AEC "Safety Evaluation of the James A. FitzPatrick Nuclear Power Plant," Docket No. 50-333, November 20, 1972.

5.13. ANS 52.1-1983 "Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants".

5.14. "The Automatic Depressurization System Cable Separation Issue and Failure Modes and Effects Analysis for the James A. FitzPatrick Nuclear Power Plant," EPM Intermediate Report, Rev. 1, Feb. 1, 1999, JAF-RPT-MISC 03086.

5.15. GE Specification 22A2989 Rev. 1, "Electrical Equipment Separation for Safeguards Systems", April 22, 1971.

5.16. "Criteria for Emergency Core Cooling Systems for Light Water Power Reactors", December 18, 1971.

5.17. "Loss-of-Coolant Accident and Emergency Core Cooling Models for General Electric Boiling Water Reactors," NEDO-10329, April 1971."

5.18. "Concluding Statement of the Regulatory Staff, Public Rulemaking Hearing On: Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled nuclear Power Reactors", Docket No. RM-50-1.

5.19. "Opinion of the United States Atomic Energy Commission in the Matter of Rulemaking Hearing: Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled nuclear Power Reactors", Docket No. RM-50-1.

5.20. Record of Telephone Conference Call of July 30, 1998, GE to NYPA, dated July 31, 1998 (GPL-98-038).

5.21. NEDO-20566 General Electric Company Analytical Model for Loss-of-Coolant Analysis in Accordance with 10CFR50 Appendix K (January 1976).

5.22. NEDO–21662 Loss-of-Coolant Accident Analysis Report for James A. FitzPatrick Nuclear Power Plant (Lead Plant) and subsequent revisions all dated July 1977.

5.23. James A. FitzPatrick Nuclear Power Plant SAFER/GESTR-LOCA Loss of Coolant Accident Analysis, NEDC-31317P Rev. 2, April 1993.

5.24. NRC Letter, Robert A. Purple to George T. Berry of NYPA, April 16, 1975.

5.25. "Emergency Core Cooling System Analysis Methods ", SECY-83-472, November 17, 1983.

5.26. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", LWR Edition, September 1975, NUREG-75/087.

5.27. 10 CFR 50.55a(h), "Protection systems", August 24, 1972.

5.28. NYPA memo, J. Gray to R. Rajaram dated September 8, 1992 (JAG-92-162), concerning the Applicability of the 1967 Draft GDC to JAFNPP.

5.29. NYPA memo, R. Rajaram/N. Mathur to J. Gray dated November 13, 1992 (CM-JAF-92-221), concerning the Applicability of AEC/NRC General Design Criteria (GDC).

5.30. IEEE-379-1972, "IEEE Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear power generating Station protection Systems", June 22, 1972.

5.31. Original FSAR, Question 6.5.

5.32. NRC letter, Karl R. Koller to George T. Berry (NYPA), dated September 30, 1976, transmitting Appendix A to Branch Technical Position APCSB 9.5-1.

5.33. AEC Order for the Modification of License for the James A. FitzPatrick Power Station, December 27, 1974, Section 4.0 and Status Report Sections 4.4.1 and 5.5.

5.34. Amendment 8 to the FitzPatrick Operating License, January 15, 1976.

5.35. Amendment 14 to the FitzPatrick Operating License, March 12, 1976.

5.36. Amendment 26 to the FitzPatrick Operating License, August 8, 1977.

5.37. Amendment 30 to the FitzPatrick Operating License, September 16, 1977.

5.38. APED 4600, Nuclear Safety Criteria for Boiling Water Reactors, Criterion No. 1.21, Single Additional Failure Criterion, January 31, 1968.

5.39. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800."

6.0 ECCS FUNCTIONAL ANALYSIS

6.1. 1 EAS 75-0688, "JAF HPCI System Design Bases Document", Section 1.2.1.

6.2. LER 79-056 Attachment, NYPA letter to Safety Review Committee, dated 11/28/79, Subject: "Inoperability of HPCI & ADS Systems Simultaneously Due to Single Failure at JAFNPP and its impact on Plant Safety".

6.3. EAS 75-0688, "JAF HPCI System Design Bases Document," Section 5.2.

6.4. NEDO-24708, Additional Information Required for NRC Staff Generic Report on Boiling Water Reactors, August 1979.

6.5. APED 4600, Nuclear Safety Criteria for Boiling Water Reactors, Criterion No. 7.1 "Reactor Core Cooling Following Coolant Loss", Rev. 2, 2/28/69.

6.6. 22A1362, GE Design Specification, "High Pressure Coolant Injection System", Rev. 5, Section 4.0.

6.7. 22A4313, GE Design Specification, "High Pressure Coolant Injection System", Rev. 0, Section 4.0.

6.8. 22A1437, "GE Design Specification for the Nuclear Boiler System", Rev. 3, 10/30/70, Section 4.2.2.3, pg. 4.

6.9. JAF Current Technical Specification Bases, Section 3.5.C, pg. 128, (Amendment 217).

6.10. JAF Current Technical Specification Bases, Section 3.5.D, pg. 128, (Amendment 217).

6.11. GEK-1 6636, "High Pressure Coolant Injection Subsystem", Section 1-2, pg. 1 –1.

6.12. GEK-34628A, "Automatic Depressurization Subsystem", Section 3-4, pg. 3-1.

6.13. JAF FSAR, "Safety Objective", Section 6.1.

6.14. JAF FSAR, "Safety Design Bases", Section 6.2.

6.15. JAF FSAR, "Safety Evaluation", Section 6.5.

6.16. JAF FSAR, "Summary Description", Section 6.3.

6.17. APED 4600, Nuclear Safety Criteria for Boiling Water Reactors, Criterion No.4.5, "Operator Judgement and Response", Oct. 15, 1965.

6.18. JAF Special Report, "Effects of a High Energy Piping System Break Outside Containment", May 3, 1973.

6.19. NEDO-24708, Additional Information Required for NRC Staff Generic Report on Boiling Water Reactors, "Operator Guidelines" Section 3.1.1.2, August 1979.

6.20. NRC letter to GE BWR Owner's Group, dated Dec. 3, 1979, Subject: "Evaluation of Small-Break Loss-of-Coolant Accident Guidelines."

6.21. RHB-008-80, February 21, 1980, GE response to NRC, Subject: "Response to Questions Posed by Mr. C. Michelson", pg. 7.

6.22. Generic Letter Jan. 8, 1980, "Summary of B&OTF Audits of Small Break LOCA Emergency Procedures and Operator Retraining at Selected GE BWR Operating Plants."

6.23. EOP-02 Rev. 5, JAF Emergency Operating Procedure, "RPV Control."

6.24. PWM-7928, 9/20/79 transcript between the NRC and GE, Subject: "Discussion of ECCS Design Bases with NRC," Sept. 20, 1979.

6.25. NEDC-24361-P, "Suppression Pool Temperature Response", August 1981, pg. 4-3.

6.26. JAF FSAR, "Safety-Related Functional Analysis", Section 12.2A.6, pg. 7 & 8.

6.27. JAF-SE-88-052, "JAF QA Classification Program Update", April 15, 1988.

6.28. JAF FSAR, "Safety-Related Functional Analysis", Section 12.2A.7, pg. 18.

6.29. NEDO-10189, "An Analysis of Functional Common-Mode Failures in GE BWR Protection and Control Instrumentation", July 1970.

6.30. NYPA Drawing. 1.83-38, 791 E453 SH2, Rev. L, "Elementary Diagram – Auto Depressurization System

6.31. ESK-11AAM, DC Elementary Diagram ADS Relief Valve 02ADS-RV-71, SOV-71A2.

6.32. EP-11 Rev. 0, "Alternate Depressurization Using SRVs from 02ADS-71".

6.33. NEDO-24951, "BWR Owners' Group NUREG-0737 implementation: Analyses and Positions Submitted to the NRC", June 1981.

7.0 CABLE SEPARATION

7.1 Design Criteria for Independence of Redundant Electrical Circuits, JAF-RPT-ELEC-02075 Rev.1

7.2 Electrical Penetration Coordination Study Summary, JSED-APL-95-009 Rev. 5, March 18, 1998.

8.0 PIPE BREAKS IN THE HPCI INJECTION PATH

8.1 PEP-HYC-98-0170, H.Y. Chang / J.V. Brunetti to J. Gray, Leakage Rates of Critical Crack Lengths for Feedwater and HPCI Lines, dated July 22, 1998.

8.2 UFSAR, Section 16.3.2.2.3.1.

8.3 "AEC, Safety Evaluation of the James A. FitzPatrick Nuclear Power Plant, Docket No. 50-333, November 20, 1972.

8.4 Supplement 5 to the FSAR, Question 4.27.

8.5 Reactor Primary Coolant System Rupture Study, Quarterly Progress Report No. 11, October-December 1967, GEAP-5587, March 1968.

8.6 NYPA e-mail, Glenroy Smith to J. Gray, July 17, 1998.

8.7 UFSAR Section 4.10.

9.0 QUALIFICATION OF THE CONDENSATE STORAGE TANK

9.1 Condensate, Feedwater and Feedwater Control Systems 006/033/034 Design Basis Document, Rev. 1.

9.2 High Pressure Coolant Injection System 023 Design Basis Document, Rev. 0

9.3 Original FSAR, Question 12.6.

9.4 JDED-98-0052, D. Huwe to N. Mathur, "Review of HPCI Suction and Test Return Lines for Possible Upgrade to QA Category I. requirements", dated January 28, 1998.

9.5 "Meeting with NEI and Licensees to Discuss Generic Letter (GL) 96-06, 'Assurance of Equipment Operability and Containment Integrity During Design-Basis Accident Conditions'", dated November 22, 1996, Attachment 1, Q6).

9.6 EAS 75-0688, "JAF HPCI System Design Bases Document", Section 2.1.

9.7 GE Design Specification 22A4313, "High Pressure Coolant Injection System", Rev. 0, Section 4.9.3.

9.8 NYPA letter, M. J. Colomb to the NRC, concerning additional information regarding Generic Letter 96-06, Jan. 25, 1999 (JAFP-99-0021).

10.0 HPCI MISSION TIME

10.1 NYPA Memo, P. Kokolakis to L. Roberts dated March 30, 1998 (GPL-98-018) concerning hot shutdown of IP-3.

10.2 10 CFR 50.48 and Appendix R to 10 CFR 50, dated Feb. 19, 1981 (45 FR 76602)

10.3 Original FSAR, Section 6.5.3.

10.4 "Loss-of-Coolant Accident and Emergency Core Cooling Models for General Electric Boiling Water Reactors," NEDO-10329, April 1971, Section 2.2.

10.5 GE Auxiliary Systems Data Book, Document 257HA791, Rev. 6, Oct. 5, 1977.

10.6 ANS 52.1-1983 "Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants."

10.7 ANS 58.9-1981 "Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems."

10.8 10 CFR 50.49, "Environmental qualification of electrical equipment important to safety for nuclear power plants, February 22, 1983.

10.9 James A. FitzPatrick Nuclear Power Plant Environmental Qualification Component List Validation Report, dated August 4, 1988 (EQ Reference #370).

10.10 EDP-20, Procedure for Establishing if Plant Electrical Equipment is Within the Scope of 10 CFR 50.49 (EQ).

10.11 JAF-SE-96-069, "Evaluation of Single Failure Consideration for Safe Shutdown Following a Control Rod Drop Accident," Rev. 0, Nov. 26, 1996.

10.12 JAFNPP Environmental Qualification Program Bases Documents, April 24, 1987 (EQ Reference #101) – EQ Reference #370 supersedes this document.

10.13 Impel Report No. 0900-040-1661, Material Analysis of the HPCI Turbine Essential Electrical Accessories at the JAFNPP, Dec. 29, 1986. (EQ Reference #335)

10.14 JAF-CALC-HPCI-00820, "Documentation of the Basis for the Removal of Certain HPCI Electrical Components From the JAF EQ Program," Revision 2, Dec. 4, 1996.

10.15 Investigation of Reactor Scram Due to a Postulated High Energy Line Break in the Reactor Building, November 3, 1984 (EQ Reference #181).

10.16 JAF-CALC-RAD-00050, "Small Break LOCA EQ Radiation Levels at Safety Relief Valves 02-RV-71 in Drywell, Revision 0, March 2, 1986.

10.17 JAF-SE-96-016, "Acceptability of Establishing a One Hour Post Accident Operating Time Requirement For the ADS System to Mitigate LOCA," Revision 0, March 3, 1986.

10.18 Technical Specification 3.6.A.3 and 3.6.A.4, Page 137, Amendment 179.

10.19 DBD-010 Rev. 0, "Residual Heat Removal System", Section 1.1.3.8.

11.0 OPERATOR ACTIONS

None

12.0 SAFETY ASSESSMENT OF THE ADS/HPCI CONFIGURATION

12.1 NYPA Memo, J. Circle to J. Gray, August 7, 1998 (RET-98-375).

12.2 EPRI TR-105396. "PSA Applications Guide", August 1995.

13.0 CONCLUSIONS AND RECOMMENDATIONS

13.1 General Electric Company Analytical and Experimental Programs for Resolution of ACRS Safety Concerns," APED-5608, April 1968.

13.2 10 CFR 50.71(e), concerning FSAR updates, July 22, 1980 (45 R 30614).

13.3 NYPA memo, P. Kokolakis to N. P. Mathur, February 2, 1998 (GPL-98-005).

13.4 NYPA letter, James Knubel to the N.R.C. concerning additional information related to Generic Letter 96-06, July 30, 1998. (JPN-98-034).

13.5 GE-NE-T23-00737-01, "James A. FitzPatrick Nuclear Power plant RHR Higher Service Water Temperature Analysis, August 1996.

13.6 AEC letter, J. O'Reilly to A. George (NYPA), May 31, 1973, concerning Inspection 73-05.

13.7 NYPA letter, A. George to J. Wainrib (SWEC), June 26, 1973, concerning cable separation.

13.8 AEC letter to G. Berry (NYPA), Oct. 4, 1973, concerning cable separation.

13.9 AEC letter to G. Berry (NYPA), January 10, 1974, concerning safeguard cable routing.

13.10 NYPA internal E-mail, T. Herrmann to J. Gray, June 7, 1999.

APPENDIX A

A.1.0 DEFICIENCY EVENT REPORTS (DERs), OPERABILITY ASSESSMENTS & INTERIM CORRECTIVE ACTIONS

A.1. DERs 97-701 & 1763

A.1.1. Description

DER 97-701 stated that the HPCI system might not be capable of depressurizing the reactor for very small breaks and that in order to stay within the bounds of the existing accident analysis, an active means of depressurizing the reactor was required. In addition, the DER identified that the ADS system was potentially subject to a single raceway failure. Further, the DER identified that it was not appropriate to rely on the ADS system or manual operation of the safety relief valves (SRVs) when HPCI is utilized for small break recovery in that HPCI and the ADS system are redundant for small break mitigation.

DER 97-1763 stated that a break in the range of 4,000 gpm and somewhat larger in the feedwater line through which HPCI injects would prevent effective HPCI injection, but at the same time, break flow would not allow RCS depressurization to the point low pressure systems become effective.

For a break near 4,000 gpm, but below 4,250 gpm, HPCI injection would feed the break with limited or no water reaching the core. Core boil-off due to decay heat would cause inventory depletion and reactor vessel level to drop. Since no reactor coolant would be lost from the break (HPCI is feeding the break), reactor depressurization would not occur. If ADS failed to operate as the assumed single failure, low-pressure systems would not be able to inject and core uncovery would occur. The validity of the hypothetical accident sequences in both DERs is dependent on ADS being subject to a single credible failure.

A.1.2 Assessments

A.1.2.1. Memorandum to P. Brozenich from B. Drain / A. Bartlik, "Operability Determination for the Suppression Pool for DER 97-701", JDED 97-0251, dated May 30, 1997.

This operability statement was based on Lake temperatures at that time (51°F) and the initial suppression pool temperature of 81.2°F which was substantially below the 95°F assumed in the accident analyses. The conclusion of this operability statement was that an extended operation of HPCI was possible,

providing the time to depressurize through the break or to restore the SRVs back to service.

A.1.2.2. Memorandum to P. Brozenich from N. Mathur / R. Penny, "Operability Assessment for DERs 97-701, 97-1763, HPCI / ADS Design Basis Issues", PEP-NM-97-317, dated December 23, 1997.

This operability statement recognized the fact that ADS was required to mitigate certain small breaks for which HPCI alone could not depressurize. A survey of literature pointed to the fact that ADS may have been single failure-proof or was not subject to a loss of function due to any credible single failure. To confirm the above, a detailed FMEA of the ADS common raceway was started and its initial results indicated that the ADS was not subject to failure from pipe whip, jet impingement or missiles.

A.1.2.3. Memorandum to P. Brozenich from T. Savory, "Operability Assessment in Support of DER 98-0456", JDED 98-0126, dated May 8, 1998.

The Failure Modes and Effects Analysis (FMEA) of the ADS system was undertaken with the assistance of EPM and is hereafter referred to as the EPM Study. The EPM Study was divided into three (3) phases.

Phase 1 assessed the hazard to the ADS cables presented by external mechanical sources. An evaluation was also performed at that time of the hazard presented by the power cables routed with the ADS cables. EPM has concluded that there is no single credible failure from these sources, which would preclude the ADS system from performing its safety related function during a LOCA.

Phase 2 of this process evaluated the hazard presented by the control and instrumentation cables routed with the ADS cables. A total of ninety-three (93) were identified which may have the potential to disable the ADS system.

Phase 3 would have evaluated the hazard to the ADS cables from Switchgear 71-MCC-133, 71-MCC-152 and Transformer 1PT-WRKB-2 and 2,000 other cables in close proximity to the ADS cables (but not in the same cable tray). Phase 3 is under consideration but has not yet been authorized.

Among the 93 vulnerabilities that EPM listed at the conclusion of Phase 2 of the study for the ADS cables was a Cat 1 circuit inside the drywell that services non-Cat 1 loads. This circuit is a 120 VAC power supply circuit to flow indicating switches. It is assumed that the non-Cat 1 load inside the drywell fails as a consequence of the accident. Further, the licensing basis requires that the ADS system remain functional in the presence of an additional single random failure. This circuit has only one level of protection. If failure of this protection is taken as

the presumed single random failure then the functionality of ADS is compromised, since the cable is located in the same wireway as the ADS cables. DER 98-00909 was issued, secondary protection was added and NSE-JAF-SE-98-017 was written to close out this issue. The NRC was notified in LER 98-003, dated May 29, 1998.

Among the 93 vulnerabilities were also seven safety cables having improperly sized protection in that the breaker sizes exceeded the cable ratings. If the postulated single failure was in the equipment served by any of these cables, then the improper sizing of their protective breakers has the potential of jeopardizing the functionality of ADS. An operability evaluation was completed of the seven cables and their existing protection and the conclusion was reached that despite the oversized breakers, these circuits do not present an operability problem.

The remaining 85 vulnerabilities pointed out by EPM were non-safety cables with a single protective device. Routing of non-safety cables is permitted by JAF criteria with one train of safety redundant systems.

A.1.3. Interim Corrective Action

The corrective actions suggested by the response to DER 97-701, dated June 20, 1997 (DERs 97-701, 1763), and response to DER 97-1763, dated January 7, 1998 (ACTS 29644) were documented in an Action Plan, PEP-APL-97-031 titled "DER 97-701 Resolution Action Plan, Revision 3", dated February 18, 1998. A Revision 4 of the Action Plan was approved on July 29, 1998 and was distributed on August 3, 1998 (Ref. A). The open items of the Action Plan are being addressed in this ADS / HPCI Licensing & Design Basis Issues Report) and will be closed out with the finalization and issuance of this report. In the interim, Revision 4 of the Action Plan is being kept open.

A.2. DERs 98-00999 & 98-01213

A.2.1 Description

DER 98-00999 states that General Electric (GE) Report, GE-NE-T23-0737-01, Section 5.9.2, implies that operation of the HPCI turbine is possible for lube oil temperatures of up to 200° to 210° F (this would occur for suppression pool temperatures between 190° and 200° F). This conflicts with the HPCI System DBD and General Electric SIL No. 615 which both state that the short term (2 hour) upper rated temperature limit for the HPCI pump is 170° F.

The DER further states that specific calculations designed to determine the suppression pool temperature at the time the reactor has depressurized to the point low pressure systems become effective have not been performed. These

are necessary to show HPCI can function throughout this period. The results of any such calculations are dependent on the reactor cooldown rate. DER 98-0010 identified that a minimum cooldown rate is required in order to avoid NPSH limitations. If it is determined that 170° F suppression pool temperature is a design limit for the HPCI pump, as this limit is below the NPSH limit of 188° F cited by DER 98-0010, an even more restrictive cooldown rate may be required.

DER 98-01213 states that SIL No. 615 recommends that for plants for which the ADS system is vulnerable to a single failure, it is necessary to either: 1. Demonstrate the RHR system is capable of maintaining the suppression pool below 170° F, such that long term operation of the HPCI pump is assured; or, 2. Verify that at least one SRV would be available to support an RCS depressurization, such that low pressure systems could be relied upon.

The DER states that the SIL is not technically complete, as it does not address the following:

The HPCI pump has a short term operating limit, for temperatures above 140° F, of 2 hours (based on telecon with GE). If this two-hour limit is valid for a scenario for which no RCS depressurization capabilities are assured, the effective maximum peak suppression pool temperature would be substantially below 170° F, as it takes well over two hours to heat the suppression pool to 170° F and cool it back down to 140° F. Consequently, the two-hour operating limit cannot be met.

A.2.2 Operability Assessment (DER 98-00999 AND DER 98-01213)

Memorandum to P. Brozenich from A. Bartlik, "JAF Revised Operability Determination Input for DER 98-0999", JDED 98-0227, dated May 15, 1998.

The above operability statement was applicable to both DERs 98-0099 and 98-01213.

The HPCI DBD identifies the maximum process fluid temperature permitted for short term and continuous operation as 170° F and 140° F, respectively. This operability statement concluded that the plant is physically capable of depressurizing the reactor below the pressure low pressure ECCS systems become effective, prior to the suppression pool temperature exceeding the maximum permissible process fluid temperature of 170° F for short term HPCI operation (assuming the availability of the SRVs). Operator training and procedural guidance ensures the operator will operate the equipment such that when required, an expeditious cooldown will be implemented. Based on the above, HPCI operation until the time low pressure systems become effective is ensured (assuming the availability of the SRVs).

A.2.3 Interim Corrective Actions

NYPA is seeking information from GE regarding the operating limits of the HPCI turbine. This will clarify the apparent discrepancies in HPCI DBD, SIL-615 and GE-NE-T23-0737-01. See ACTS 98-33857.

A.3. DERs 97-1226 & 97-1227

A.3.1. Description

DER 97-1226 indicates that a NYPA letter to the NRC contains an incorrect statement. JPN-97-003 states "A review of plant transient and accident analysis indicates that the transfer function (transfer of HPCI suction from CST to torus) is not required except for initiating events which would render the CST unavailable." The DER indicates that this statement appears to be incorrect since the transfer function is apparently required for mitigation of some small breaks.

DER 97-1227 states that "The operability assessment for GL 96-06 concluded that the transfer function coincident with thermal pressurization is not required. This conclusion was based on the premise that HPCI operation is a short duration event within which time significant torus heating does not occur. Accident sequences have been postulated which challenge this basis."

A.3.2. Operability Assessment (DER 97-1226 AND DER 97-1227)

DERs 97-1226 and 1227 dealt with concerns raised regarding a NRC Generic Letter 96-06 response JPN 97-003. Therefore, there are no operability issues.

A.3.3. Corrective Actions

Revise JPN-97-003, if required, based on the results of the technical review of the issues which are being conducted as part of DER 97-701 and DER 97-1227 (ACTS 97-28399).

APPENDIX B
HISTORICAL REVIEW OF FITZPATRICK LOCA ANALYSES

JAF is one of the early (1967 product line) design of GE's BWR 4s in which HPCI systems were introduced for high pressure injection for the first time. This is in addition to the CS and LPCI systems that were already applied in the earlier product line plants. At the time, besides the pace of evolution of the product designs and the models applied to analyze them, there were also dramatic changes in the regulatory environment. The allowable peak cladding temperature went from 3300° F to 2700° F to 2300° F and finally to 2200° F. This makes it difficult to put the history of the methods and acceptance criteria together.

The designer (GE), during JAF's early design stage, utilized the so-called interim evaluation model with level swell capabilities for the analysis of design basis LOCAs as described in the Preliminary Safety Analysis Report (PSAR). This was in accordance with the regulations and applicable acceptance criteria at the time. (On June 29, 1971 the AEC published an interim statement of policy [36FR12247] establishing an Interim Acceptance Criteria [IAC] for ECCS for LWRs).

There were no rules and regulations for ECCS performance, except the IAC, up until February 4, 1974 when Part 50.46 of 10 CFR was published. The Statements of Consideration published with the rule contained the following statement concerning the changes from the IAC:

> "The old criterion number one, specifying that the temperature of zircaloy cladding should not exceed 2300^0 F, is replaced by two criteria, lowering the allowed peak zircaloy temperature to 2200^0 F and providing a limit on the maximum allowed local oxidation. The other three criteria of the IAC are retained, with some modification of the wording. These three criteria limit the hydrogen generation from metal-water reactions, require maintenance of coolable core geometry, and provide for long-term cooling of the quenched core."

This new rule had significant impact in the development of newer methods and models with better features than the models used prior to 1971. This was the Appendix K era and models of this vintage were used until the mid-1980s. By that time, extensive experimental and analytical studies resulted in a new best-estimate ECCS evaluation methodology. The best-estimate methodology showed that the Appendix K safety margin (about 1000° F) is extremely conservative.

The following tables summarize the methods and acceptance criteria used for the FitzPatrick LOCA analysis over the life of the plant.

Large Break LOCA

TIME	REGULATORY BASIS/ACC. CRITERIA	SUCCESS CRITERIA	ASSUMPTIONS E.G, SINGLE FAILURE/SWELL/T CHF MODELS ETC.	MODELS, COMPUTER CODES
1967	IAC, before 1971 (Early Design Work Only) NO PLANT SPECIFIC ECCS ANALYSIS WAS NEEDED AT THE TIME.	PCT< 2700^0 F	Interim evaluation Model with level swell capability.	LAMB SCAT
1971	Interim Model ,1st Core Non-Appendix K	PCT< 2300^0 F	Upper plenum mixing model.	LAMB,CHASTE, SAFE
1974	10CFR50.46 (August 1st 1975)	PCT< 2200^0 F	1st APP K Model NEDO-21662	LAMB/SCAT/SAFE/ DBA-REFLOOD/CHASTE
1986	Best Estimate Models	PCT<< App. K value	NEDC-31317P	SAFER/GESTR-LOCA

The large break LOCA is one of the design basis accidents for the present light water cooled reactors. ECCS design since the beginning of the 1950s has always focused on the large break LOCAs. The early response of the ECCS and the peak cladding temperatures were the dominant concerns. Although some limited number of break spectra were considered in the early evaluation models, significant emphasis on small breaks and their appropriate treatment did not occur until after the TMI accident in 1979. Following TMI, in response to NRC Bulletin & Order Task Force initiatives, new and better models and methods were developed and employed for extensive evaluation of small break LOCAs.

Small Break LOCA (SBLOCA)

TIME	REGULATORY BASIS/ACC. CRITERIA	SUCCESS CRITERIA	ASSUMPTIONS E.G, SINGLE FAILURE/SWELL/TCHF MODELS ETC.	MODELS, COMPUTER CODES
1967	Almost identical with large break LOCA	No specifics for small break LOCAs	Level swell 1967 product line	Early evaluation models
1971	Interim Acceptance Criteria	GETAB	Several	Interim model No specifics for small break LOCAs
1974	10CFR50.46	NEDO-21662, 1977	PCT local oxidation, break size < 1.0 ft^2	LAMB/non-DBA REFLOOD