



NUCLEAR ENERGY INSTITUTE

Alexander Marion
EXECUTIVE DIRECTOR
NUCLEAR OPERATIONS & ENGINEERING
NUCLEAR GENERATION DIVISION

December 21, 2007

Mr. John A. Grobe
Associate Director for Engineering and Safety Systems
U.S. Nuclear Regulatory Commission
Mail Stop O-13 D13
Washington, DC 20555-001

Subject: Industry Methodology for Evaluating Multiple Spurious Operations

Project Number: 689

Dear Mr. Grobe:

In SRM-SECY-06-0196 ("Issuance Of Generic Letter 2006-XX, 'Post-Fire Safe-Shutdown Circuits Analysis Spurious Actuations'") the Commission directed the Staff to work with stakeholders to develop or endorse guidelines that provide a clearly defined method of compliance for licensees who do not choose to utilize the risk-informed approach contained in 10 CFR 50.48(c). To that end, we met with the NRC several times this year in an attempt to reach mutual agreement on an approach we are developing to address this issue. An initial version of our approach has been completed and included in a proposed revision to NEI 00-01, "Guidance for Post-Fire Safe-Shutdown Circuit Analysis". A draft of this document, which was endorsed in part by the NRC in an earlier revision, is enclosed for your review.

Industry Method

The industry method is outlined in the enclosed flowchart (Enclosure 1). Our approach can be summarized as follows:

- A draft generic list of multiple spurious circuit operations (MSOs) that challenge safe-shutdown will be developed by the NSSS Owners Groups (OGs). This list consists of a number of combinations of multiple component functional failures that could each challenge safe-shutdown. The list will be based on licensee input from safe shutdown analysis, fire protection program self assessments, NRC inspections and PRA results.
- The draft MSO list will be evaluated by the NSSS OGs to determine which entries can be generically excluded based on general design considerations. The NSSS OGs will forward the

resulting generic list of MSOs and the information developed during the NSSS OG review to each licensee.

- Each licensee will use an expert panel to review the generic MSO list and add or delete to it as appropriate to make the MSO list plant specific. All the reviews to this point will be done deterministically using design and as-built plant information.
- The plant specific MSO list will be dispositioned by one of the following methods:
 - Ensuring that deterministic fire protection requirements are met
 - Performing plant modifications to establish adequate separation
 - Completing fire modeling to show that fire will not affect the protected safe-shutdown train
 - Completing a focused scope PRA to show that the risk associated with a specific MSO is not significant
- The basis for acceptance will be documented.
- Appropriate licensing activities (license amendment or exemption if necessary) will be undertaken to ensure the licensing basis is properly managed and NRC approval is obtained if necessary.

NRC Feedback

We have interpreted the Staff's feedback on our methodology as generally positive except for concern with its use of risk methods (focused scope PRA). We believe that our methodology is an acceptable technical approach to resolution of the multiple spurious issue and respectfully disagree with the Staff on the acceptability of our risk methods under the current regulations. We offer the following bases for our position:

- Current regulations do not require that post-fire safe-shutdown analyses assume multiple spurious operations. GDC-3, 10CFR50.48 and Appendix R establish a number of requirements for fire protection programs and fire prevention and suppression methods, but they do not specifically address the circuit analysis methods that must be used to analyze for safe-shutdown. The need to evaluate single spurious operation or multiple spurious operations has always been a matter of interpretation. In fact, many plant licensing bases include documented evidence that single spurious methods were used to evaluate for safe-shutdown in the event of a fire, and in some cases NRC has specifically stated in SERs and other correspondence that this approach complies with the regulation. Because licensees are in compliance with their current licensing basis, the methods used by them to evaluate multiple spurious operations should not be a compliance issue.
- Even assuming that multiple spurious operations must be evaluated under the current regulations, the regulations (with the exception of 10CFR50.48(c) which is voluntary) are not specific on whether risk informed or deterministic methods can be used to evaluate safe-

shutdown. Therefore, the use of risk methods should be acceptable whether or not a plant commits to meet 10CFR50.48(c) and no exemption to the regulations should be necessary to use such methods. There is evidence that the Staff has agreed with this interpretation in the past. Specifically the Statements of Consideration that accompanied the publication of 10CFR50.48(c) contain the following question and answer in the Federal Register notice (69FR33544):

"Use of NFPA 805 Methods by Other Licensees"

"A commenter stated that licensees who do not adopt NFPA 805 should not be precluded from using risk tools from NFPA-805."

"The NRC agrees with the comment. However, licensees not adopting NFPA 805 in accordance with the final rule are not covered by the provisions for transitioning to NFPA-805. Such licensees who wish to use the risk tools in NFPA 805 will need to separately determine if their existing licensing basis would permit the use of such tools, and take appropriate action as necessary to change their licensing basis."

Licensing basis changes are associated with license amendment requests, not exemptions. Industry agrees that the appropriate licensing activities must be completed for MSO resolutions requiring this action.

- The use of focused scope PRA is consistent with the Commission's Policy Statement on use of PRA (60FR42622). This policy states in part:

"(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that compliments the NRC's deterministic approach and supports the NRC's traditional defense in depth philosophy."

In fact risk insights and methods are used frequently in licensing activities in other technical areas and in other fire protection licensing activities (exemptions). We do not believe that the use of risk methods in evaluating multiple spurious operations should be treated differently.

- Since the industry method will require some means of resolution (fire modeling or deterministic) for risk significant MSOs, the only MSOs that will be dispositioned through a risk argument are those that are not risk significant. A method that does not allow the use of risk to disposition non-risk-significant MSOs could result in the following unintended consequences:
 - If manual actions or some other means of compensatory action is undertaken to address the MSO, the effect may be to increase the overall risk for the plant.
 - If plant modifications are used to address the situation, the licensee may be forced to implement costly modifications to resolve an issue with negligible risk significance. This may divert resources from more safety-significant applications.

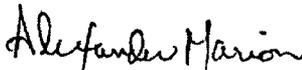
Conclusions

The Commission has directed the Staff to encourage licensees to adopt NFPA-805 and 10CFR50.48(c). For those that do, the Staff has not contested use of risk to address MSOs. However, for a number of reasons many licensees are not yet, and may never be, willing to adopt 10CFR50.48(c). For those that do not, the industry's methodology provides a technically sound way to address and resolve the MSO issue. We request that the Staff change its interpretation on the use of risk in this application and review our draft document on its technical merits. Resolution of this issue is long overdue.

One final point; we understand that the Staff is concerned that approval of a MSO methodology may affect a licensee's decision to transition to NFPA-805. We will study this question and address it in later correspondence.

We appreciate your review of our document and look forward to meeting with the Staff to address any comments. If you have any questions on this matter, please contact me (202-739-8080; am@nei.org) or Jim Riley (202-739-8137; jhr@nei.org).

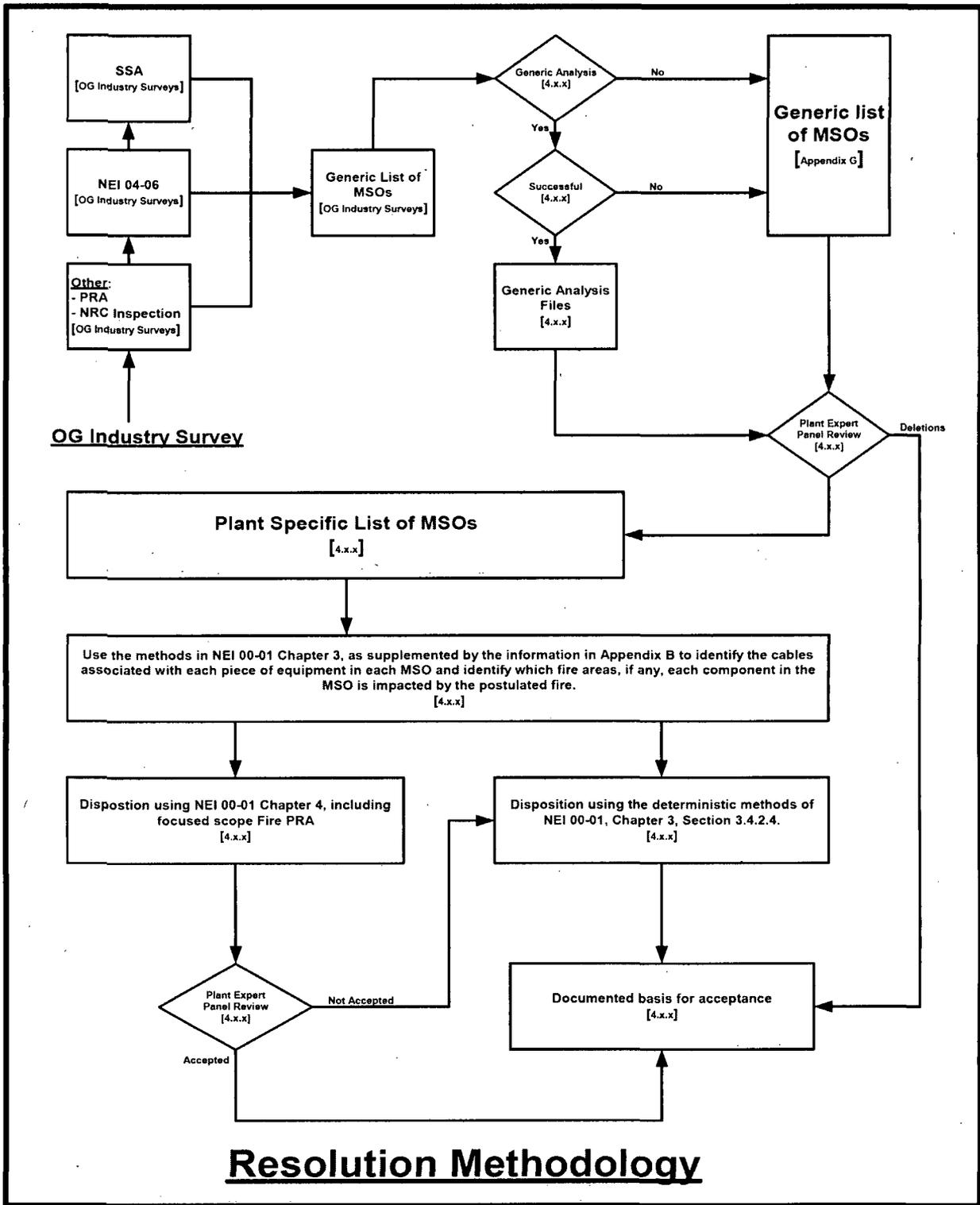
Sincerely,



Alexander Marion

Enclosures

c: Mr. James E. Dyer, U.S. Nuclear Regulatory Commission
Mr. Alexander R. Klein, U.S. Nuclear Regulatory Commission



NEI 00-01

Revision 2

**Guidance for Post-Fire
Safe Shutdown Circuit
Analysis**

DRAFT

December 2007

NEI 00-01

Revision 2

Nuclear Energy Institute

**Guidance for Post-Fire
Safe Shutdown Circuit
Analysis**

December 2007

Nuclear Energy Institute, 1776 I Street N. W., Suite 400, Washington D.C. (202.739.8000)

ACKNOWLEDGMENTS

NEI appreciates the extensive efforts of the utility members of the Circuit Failures Issue Task Force in developing and reviewing this document, as well as their utility management in supporting the members' participation.

Amir Afzali, Pacific Gas & Electric
Gordon Brastad, Energy Northwest
Maurice Dingler, Wolf Creek Nuclear Operating Corporation
Tom Gorman, PPL, Susquehanna
Dennis Henneke, GE Hitachi
Robert Kassawara, EPRI
Harvey Leake, Arizona Public Service
Bijan Najafi, SAIC

Chris Pragman, Exelon
Vicki Warren, Exelon
Woody Walker, Entergy

NEI also extends its thanks to the following organizations playing important roles in the completion of this guidance:

- EPRI: Funded a significant series of circuit failure tests and the Expert Panel who developed spurious actuation probabilities from the test results
- BWR Owners Group: Developed the deterministic portion of the NEI 00-01 guidance
- Westinghouse/CE and B&W Owners Groups: Along with the BWROG, funded the pilot applications of NEI 00-01 and a significant portion of the report preparation
- Duke Energy and NMC Corporation: Hosted pilot applications of NEI 00-01
- Omega Point Laboratories: Provided a cost-effective test facility for circuit failure testing
- The NRC and Sandia National Laboratories: Provided extensive participation in the EPRI/NEI circuit failure testing, and review and comment on NEI 00-01
- Edan Engineering: Wrote the EPRI report on the circuit failure testing and the analysis in Appendix B.1 on Multiple High Impedance Faults.

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

EXECUTIVE SUMMARY

NEI 00-01 was developed to provide a deterministic methodology for performing post-fire safe shutdown analysis. In addition, NEI 00-01 includes information on risk-informed methods that may be used in conjunction with the deterministic methods for resolving circuit failure issues related Multiple Spurious Operations (MSOs). The risk-informed method is intended for application by utilities to determine the risk significance of identified circuit failure issues related to MSOs. The deterministic safe shutdown analysis method described in Revision 0 of this document reflected practices in place for many years at a wide cross-section of U.S. nuclear plants and widely accepted by NRC. These practices were generally reflected in the plant's licensing basis. In Revision 1 these deterministic methods were revised to address insights gained from EPRI/NEI circuit failure testing and reflected in NRC's RIS-2004-03. While these insights do not change a plant's licensing basis, they reflect the NRC's new emphasis on considering potential safety implications of MSOs. This emphasis on MSOs became apparent as the NRC revised their inspection guidance to resume the inspection of circuits in January 2005. The methods presented in Revision 1 were intended to support licensees preparing for the resumed NRC circuit failure inspections.

In Revision 2 changes are being made to document the Resolution Methodology presented by the Industry to the NRC Staff for resolving the MSO Issue subsequent to the rejection of the Staff's generic letter on MSOs by the Commission. The methodology in Revision 2 reflects insights gained from, not only the EPRI/NEI Cable Fire Testing, but also the CAROLFIRE Cable Fire Testing. The methodology contained in Revision 2 is one method of addressing the MSO Issue.

This document neither changes nor supports any individual plant's licensing basis. The assumptions used in the licensing basis, and the nature of any approvals the NRC may have provided for these assumptions, are a plant-specific matter between each licensee and the NRC.

NEI 00-01 Revision 2 in Chapter 5 provides a methodology for a focused-scope Fire PRA for assessing the risk significance of specific MSOs. This method is intended for application to circuit failures involving MSOs. All MSO impacts deemed to be risk significant should be placed in the plant Corrective Action Program with an appropriate priority for action. Since a large number of low significance findings of uncertain compliance status could result from industry applications of this method to MSOs, separate discussions are being held with NRC to address the handling of such issues without unnecessary resource impacts for licensees and NRC alike

It is expected that plants adopting an alternate risk-informed licensing basis using NFPA 805 will be able to reference NEI 00-01 as an acceptable method for addressing circuit failure issues, including the MSO Issue.

[This page intentionally left blank.]

DRAFT

1	INTRODUCTION	1
1.1	PURPOSE	1
1.2	BACKGROUND	3
1.3	OVERVIEW OF POST-FIRE SAFE SHUTDOWN ANALYSIS	5
1.3.1	General Methodology Description	7
1.3.2	Deterministic Method	7
1.3.3	Risk Significance Methods	14
2	APPENDIX R REQUIREMENTS AND CONSIDERATIONS	15
2.1	REGULATORY REQUIREMENTS	15
2.2	REGULATORY GUIDANCE ON ASSOCIATED CIRCUITS	19
2.3	REGULATORY INTERPRETATION ON LOSS OF OFFSITE POWER	21
3	DETERMINISTIC METHODOLOGY	22
3.1	SAFE SHUTDOWN SYSTEMS AND PATH DEVELOPMENT	22
3.1.1	Criteria/Assumptions	25
3.1.2	Shutdown Functions	27
3.1.3	Methodology for Shutdown System Selection	31
3.2	SAFE SHUTDOWN EQUIPMENT SELECTION	34
3.2.1	Criteria/Assumptions	35
3.2.2	Methodology for Equipment Selection	36
3.3	SAFE SHUTDOWN CABLE SELECTION AND LOCATION	38
3.3	SAFE SHUTDOWN CABLE SELECTION AND LOCATION	39
3.3.1	Criteria/Assumptions	39
3.3.2	Associated Circuit Cables	41
3.3.3	Methodology for Cable Selection and Location	42
3.4	FIRE AREA ASSESSMENT AND COMPLIANCE STRATEGIES	45
3.4.1	Criteria/Assumptions	46
3.4.2	Methodology for Fire Area Assessment	47
3.5	CIRCUIT ANALYSIS AND EVALUATION	51
3.5.1	Criteria/Assumptions	51
3.5.2	Types of Circuit Failures	52
4	IDENTIFICATION AND TREATMENT OF MULTIPLE SPURIOUS OPERATIONS	64
5	RISK SIGNIFICANCE ANALYSIS	78
5.1	COMPONENT COMBINATION IDENTIFICATION	79
5.1.1	Consideration of Consequences	79
5.1.2	Selection of MSO Scenarios to be Analyzed	79

5.2	PRELIMINARY SCREENING	79
5.2.1	Screening Factors.....	79
5.2.2	Six-Factor Frequency of Core Damage (F*P*G*S*C*Z).....	83
5.2.3	Final Screening Table.....	84
5.2.4	Example Application	86
5.2.5	Summary	88
5.3	PLANT-SPECIFIC RISK SIGNIFICANCE SCREENING	95
5.3.1	EPRI/NEI Test Results.....	95
5.3.2	Large Early Release Frequency Evaluation (LERF)	99
5.3.3	Uncertainty and Sensitivity Analysis	99
5.4	INTEGRATED DECISION MAKING	100
5.4.1	Defense-In-Depth and Safety Margins Considerations.....	101
5.4.2	Corrective Action.....	103
5.4.3	Documentation	104
6	DEFINITIONS	107
7	REFERENCES	115
7.1	NRC GENERIC LETTERS	115
7.2	BULLETINS.....	115
7.3	NRC INFORMATION NOTICES.....	116
7.4	OTHER RELATED DOCUMENTS.....	119
7.5	ADMINISTRATIVE LETTERS	122
7.6	REGULATORY ISSUE SUMMARIES.....	122

FIGURES

	<u>Page #</u>	
Figure 1-1	NEI 00-01 Process Flow Chart	10
Figure 1-2	Deterministic Post-fire Safe Shutdown Overview	11
Figure 2-1	Appendix R Requirements Flowchart	17
Figure 3-1	Deterministic Guidance Methodology Overview	23
Figure 3-2	Safe Shutdown System Selection and Path Development	33
Figure 3-3	Safe Shutdown Equipment Selection	38
Figure 3-4	Safe Shutdown Cable Selection	44
Figure 3-5	Fire Area Assessment Flowchart	49
Figure 3.5.2-1	Open Circuit (Grounded Control Circuit)	54
Figure 3.5.2-2	Short to Ground (Grounded Control Circuit)	55
Figure 3.5.2-3	Short to Ground (Ungrounded Control Circuit)	56
Figure 3.5.2-4	Hot Short Grounded Control Circuit)	59

Figure 3.5.2-5	Hot Short (Ungrounded Control Circuit)	60
Figure 3.5.2-6	Common Power Source (Breaker Coordination)	61
Figure 4.1	Resolution Methodology	66
Figure 5-1	Simplified Process Diagram	82
Figure 5-2	Fragility Curves Thermoset	82

TABLES

		<u>Page #</u>
TABLE 5-1	Maxima for the Pairings F*P	89
TABLE 5-2	Maxima That Result from Maximum Credits for G (0.01), S (0.01), C (0.01) and Z (0.9)	89
TABLE 5-3	Point Requirements for Screening	90
TABLE 5-4	Establishing Relative Risk Ranking When All Zones Preliminarily Screen	91
TABLE 5-5	Generic Location Fire Frequencies	92
TABLE 5-6	Probabilities of Spurious Actuation Based on Cable Type and Failure Mode (Range)	93
TABLE 5-7	General Fire Scenario Characterization Type Bins Mapped to Fire Intensity Characteristics	93
TABLE 5-8	Statistical Unavailability Values for SSD Path-Based Screening CCDP	94
TABLE 5-9	Summary of the Probabilities (P_{SACD})	98

ATTACHMENTS

Attachment 1	Example of Typical BWR Safe Shutdown Path Development	123
Attachment 2	Annotated P&ID Illustrating SSD System Paths [BWR Example]	124
Attachment 3	Example of Safe Shutdown Equipment List	125
Attachment 4	Safe Shutdown Logic Diagram [BWR Example]	127
Attachment 5	Example of Affected Equipment Report	128
Attachment 6	Example of Fire Area Assessment Report	130

APPENDICES

Appendix A	Safe Shutdown Analysis as Part of an Overall Fire Protection Program	A-1
Appendix B	Deterministic Circuit Failure Characterization	B-1
Appendix B.1	Justification for the Elimination of Multiple High Impedance Faults	B.1-1
Appendix C	High/Low Pressure Interfaces	C-1
Appendix D	Alternative/Dedicated Shutdown Requirements	D-1
Appendix E	Manual Actions and Repairs	E-1
Appendix F	Supplemental Selection Guidance (Discretionary)	F-1
Appendix G	MSOs	G-1

GUIDANCE FOR POST-FIRE SAFE SHUTDOWN CIRCUIT ANALYSIS

1 INTRODUCTION

For some time there has been a need for a comprehensive industry guidance document for the performance of post-fire safe shutdown analysis to implement existing fire protection regulations. Such a document is needed to consistently apply the regulatory requirements for post-fire safe shutdown analysis contained in 10 CFR 50.48 (Reference 6.4.1) and 10 CFR 50 Appendix R (Reference 6.4.3).

From the standpoint of deterministic safe shutdown analysis, Generic Letter 86-10 (Reference 6.1.10) provided standardized answers to certain questions related to specific issues related to this topic. The answers provided, however, did not comprehensively address the entire subject matter. The lack of comprehensive guidance for post-fire safe shutdown analysis, in combination with the numerous variations in the approach used by the architect engineers responsible for each plant design, have resulted in wide variation in plant-specific approaches to deterministic post-fire safe shutdown analysis.

Some of these approaches are based on long-held industry interpretations of the NRC regulations and guidance. In many cases, these interpretations were not documented in a manner that indicated a clear NRC acceptance of the position. In an NRC letter to NEI in early March 1997 (Reference 6.4.30) NRC stated that the regulatory requirements and staff positions are well-documented, and that regulatory requirements recognize that fires can induce multiple hot shorts. The industry responded (Reference 6.4.31) that industry and NRC staff interpretations of existing regulations and regulatory guidance differ significantly on at least some aspects of the post-fire safe shutdown analysis requirements and provided reasons for these differing interpretations. The Boiling Water Reactor Owners Group (BWROG) developed a comprehensive document for BWRs to compile deterministic safe shutdown analysis practices based on existing regulatory requirements and guidance. That document was adopted into NEI 00-01 with minor changes to address PWR-specific safe shutdown analysis considerations.

1.1 PURPOSE

The purpose of this document is to provide a consistent process for performing a fire safe shutdown circuit analysis. While it describes differences between NRC and industry licensing positions, NEI 00-01 does not define what any plant's licensing basis is or should be. Plant licensing bases have been developed over many years of licensee interactions with NRC staff, and the interpretation of these licensing bases is a matter between each licensee and NRC staff. The guidance provided in this document accounts for differences and uncertainties in licensing basis assumptions about circuit failures. It also provides a method for the resolution of the differences between the NRC and the industry related to fire-induced circuit failures resulting in MSOs.

This document provides deterministic methods for addressing potential fire-induced circuit failure issues, either within or beyond the existing plant's licensing basis. The deterministic method, derived from NRC regulations, guidance, and plant licensing bases is provided for analyzing and resolving circuit failure issues. Risk-informed methods are provided to (1) select circuits and appropriate combinations thereof for the analysis of MSOs (note: the terms spurious actuation and spurious operation are considered synonymous. The term "spurious operation" is used in this document for consistency), and (2) determine the risk significance of identified circuit failure combinations (MSOs). While the selection of circuit failure combinations, MSOs, has not traditionally been included in plant circuit analysis methods to date, it is appropriate to consider such combinations in the light of the results of recent cable failure testing, both EPRI/NEI and CAROLFIRE. The Resolution Methodology for MSOs included in this document will assist the licensee in determining whether potentially risk-significant interactions could impact safe shutdown, but this Resolution Methodology does not change the plant licensing basis.

The methods in this document do not require the systematic reevaluation of a plant's post-fire safe shutdown circuit analysis. Such a systematic re-evaluation is entirely a licensee decision that may be based on NRC inspection findings, licensee self-assessment results, or industry experience. Neither do these methods take precedence over specific requirements accepted by the NRC in a plant's post-fire safe shutdown analysis. The deterministic methods in this document rely on approved licensing bases for individual plants. In addition, this document provides criteria for assessing the risk significance of those MSO issues that may not be included in current safe shutdown analyses, but that may be a concern because of potential risk significance.

This guidance in this document reflects the position that licensees should address potential risk-significant issues regardless of whether they involve compliance with the licensing basis. When issues are identified, the licensee should consider whether they involve violations of the licensing basis, are beyond the licensing basis, or are of uncertain compliance status and subject to possible disagreement with NRC. Licensees should also consider the risk significance of the findings consistent with the fire protection SDP. Consideration of these parameters is illustrated in the following table:

Type of Issue	Action to Address Issue	
	Issue Risk Significant	Issue Not Risk Significant
Finding (issue outside CLB)	Address in CAP	Green finding; action at licensee's discretion
Violation of CLB	Address in CAP	Address in CAP or provide licensing basis changes (using approved regulatory processes)

Type of Issue	Action to Address Issue	
	Issue Risk Significant	Issue Not Risk Significant
Compliance status/ CLB not clear	Address in CAP	Address in CAP or provide licensing basis changes (using approved regulatory processes)

As seen in the table above, NEI 00-01 concludes that the licensees should address risk-significant circuit failure issues regardless of whether they involve potential violations. Issues that are both risk-insignificant and outside the licensing basis should be treated in accordance with current ROP guidelines as illustrated in the table. Remaining low significance issues potentially involving compliance should be addressed consistently with current regulatory guidelines; licensing basis changes (using approved regulatory processes) may be in order, supported by the risk analysis performed using Section 5 risk analysis or the fire protection SDP methods.

An example will illustrate the use of NEI 00-01. In this example, assume that the licensee conducts a self-evaluation using this document and determines that he should postulate more than one simultaneous spurious operation in a certain fire area. Further assume that the licensing basis is inconclusive. The licensee could determine the risk significance of the issue using the methods of NEI 00-01, the revised fire protection Significance Determination Process, or other plant-specific risk analyses. The licensee should place the issue in the plant Corrective Action Program (CAP) if it is significant according to the risk criteria used, or could request licensing basis changes (using approved regulatory processes), or change the fire protection plan, if it is not. The compliance aspects would also be addressed in cases where it is not clear whether an issue is within the licensing basis (a "compliance issue") or not.

Potentially, a large number of exemption requests (on an industry-wide basis) for low significance issues could result in an unnecessary expenditure of industry and staff resources. NRC and industry are discussing ways for addressing low significance issues with uncertain compliance status to minimize this resource expenditure and still address regulatory requirements.

1.2 BACKGROUND

Reviewing past fire events can substantiate the uncertainty associated with the behavior of actual plant fires. On March 22, 1975, the Browns Ferry Nuclear Power Plant had the worst fire ever to occur in a commercial nuclear power plant operating in the United States. (Reference U.S. Nuclear Regulatory Commission (NRC) Inspection and Enforcement (IE) Bulletin Nos. 50-259/75 and 50-260/75-1, dated 2/25/75.) The Special Review Group that investigated the Browns Ferry fire made two recommendations pertaining to assuring that the effectiveness of the fire protection programs at operating nuclear power plants conform to General Design Criterion (GDC) 3.

- The NRC should develop specific guidance for implementing GDC 3.
- The NRC should review the fire protection program at each operating plant, comparing the program to the specific guidance developed for implementing GDC 3.

In response to the first recommendation, the NRC staff developed Branch Technical Position (BTP) Auxiliary Power Conversion Systems Branch (APCSB) 9.5-1, "Guidance for Fire Protection for Nuclear Power Plants," May 1, 1976; and Appendix A to BTP APCS 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants Docketed Prior to July 1, 1976," August 23, 1976. The guidance in these documents focused on the elements of fire protection defense-in-depth (DID): (1) prevention; (2) mitigation through the use of detection and suppression (automatic and manual); (3) passive protection of structures, systems and components (SSCs) important to safety and post-fire safe shutdown.

In response to the second recommendation, each operating plant compared its fire protection program with the guidelines of either BTP APCS 9.5-1 or Appendix A to BTP APCS 9.5-1. The staff reviewed the fire protection programs for compliance with the guidance.

The guidance in BTP APCS 9.5-1 and Appendix A to BTP APCS 9.5-1, however, did not provide sufficiently specific guidance for performing post-fire safe shutdown analysis. Also, independent testing sponsored by the NRC indicated that some of the separation concepts proposed by licensees under the BTP, such as coating intervening cable trays with fire retardant coatings, would not provide sufficient protection in the event of a severe fire. Thirdly, some licensees did not implement aspects of the BTP that the NRC Staff considered essential in order to achieve adequate protection. To address these issues and to provide the necessary guidance, the NRC issued 10 CFR 50.48, "Fire Protection," and Appendix R, "Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979," to 10 CFR Part 50 (45 FR 36082). The NRC published in the Federal Register (45 FR 76602) the final fire protection rule (10 CFR 50.48) and Appendix R to 10 CFR Part 50 on November 19, 1980. The Appendix R Regulation required compliance with sections III.G, III.J, and III.O for all plants licensed to operate before January 1, 1979, and also required individual licensees to comply with other lettered sections, based on the status of their outstanding items under the BTP review, as reflected by NRC correspondence to the individual licensees. Section III.G.2 of Appendix R reflected the results of the NRC's independent cable tray fire testing program, overriding any previous approvals the NRC may have granted regarding the protection of cables with fire retardant coatings.

This regulation applies to plants licensed to operate prior to January 1, 1979. For plants licensed to operate after January 1, 1979, the NRC staff, in most cases, required compliance with Appendix A to BTP APCS 9.5-1 and Sections III.G, J & O of Appendix R. For these licensees, the sections of Appendix R apply to the plant as a licensing commitment, rather than as a legal requirement imposed by the code of federal

regulations. Some other licensees provided comparisons to the guidelines of Section 9.5-1, "Fire Protection Program," of NUREG-0800, "Standard Review Plan," which incorporated the guidance of Appendix A to BTP APCS 9.5-1 and the criteria of Appendix R, or BTP CMEB 9.5-1. Additionally, some plants had aspects of their programs reviewed to the criteria contained in Draft Regulatory Guide 1.120 Revision 1 ("Fire Protection Guidelines for Nuclear Power Plants," November 1977), which primarily reflected the content of BTP APCS 9.5-1 Revision 1. Therefore, even though fire protection programs can be essentially equivalent from plant to plant, the licensing basis upon which these programs are founded can be very different.

The plant design changes required for passive and active fire protection features and administrative controls required by the regulations discussed were fairly specific. These changes have been implemented throughout the industry. These changes have been effective in preventing a recurrence of a fire event of the severity experienced at Browns Ferry.

To clarify the regulations, the NRC staff has issued numerous guidance documents in the form of memorandums, Generic Letters and Information Notices. These documents provide insights as to the NRC staff's interpretation of the regulations, their views on acceptable methods for complying with the regulations, and clarity of the requirements necessary in performing a post-fire safe shutdown analysis.

1.3 OVERVIEW OF POST-FIRE SAFE SHUTDOWN ANALYSIS

A fire in an operating nuclear power plant is a potentially serious event. In general, the likelihood of a large fire with the potential to damage plant equipment important to safe shutdown is considered to be small. The expected fire would be contained in a single electrical panel or a localized portion of one room or area. Typical plant design segregates important cables and equipment from threats such as missiles, flooding, and significant fire sources. The expected plant response to this type of event would be to maintain continued operation and to dispatch the plant fire brigade to extinguish the fire.

Despite this, the consequences of an event that damages plant equipment important to safe shutdown can be significant. The Browns Ferry fire resulted in damage to plant equipment important to safe shutdown. Although safe shutdown of the Browns Ferry unit was ultimately accomplished, the event was of sufficient significance to warrant major changes in fire protection design features of a nuclear power plant. Appendix A to this document provides a description of the improvements made in the fire protection design of nuclear power plants in response to the Browns Ferry fire event.

In addition to plants making changes to the fire protection design features, they have also placed increased attention on identifying those systems and equipment important to the post-fire safe shutdown of each unit. A safe plant design is achieved by identifying the systems and equipment important to post-fire safe shutdown, making conservative assumptions regarding the extent of fire damage and assuring adequate separation of the

redundant safe shutdown trains. These aspects of post-fire safe shutdown design, in combination with the changes made in the design of the plant fire protection features in response to the Browns Ferry fire, solidify this conclusion regarding plant safety.

The goal of post-fire safe shutdown is to assure that a single fire in any plant fire area will not result in any fuel cladding damage, rupture of the primary coolant boundary or rupture of the primary containment. This goal serves to prevent an unacceptable radiological release as a result of the fire. This goal is accomplished by assuring the following deterministic criteria are satisfied for a single fire in any plant fire area:

- One safe shutdown path required to achieve and maintain hot shutdown is free of fire damage
- Repairs to systems and equipment required to achieve and maintain cold shutdown can be accomplished within the required time frame
- Any operator manual actions required to support achieving either hot or cold shutdown are identified and meet the applicable regulatory acceptance requirements.

The deterministic method in Section 3 integrates the requirements and interpretations related to post-fire safe shutdown into a single location, and assures that these criteria are satisfied. It:

- Identifies the systems, equipment and cables required to support the operation of each safe shutdown path
- Identifies the equipment and cables whose spurious operation could adversely impact the ability of these safe shutdown paths to perform their required safe shutdown function
- Provides techniques to mitigate the effects of fire damage to the required safe shutdown path in each fire area.

Using this methodology to perform post-fire safe shutdown analysis will meet deterministic regulatory requirements and provide an acceptable level of safety resulting in a safe plant design. It is consistent with the fire protection defense-in-depth concept that addresses uncertainties associated with the actual behavior of fires in a nuclear power plant. Post-fire safe shutdown is one part of each plant's overall defense-in-depth fire protection program. The extent to which the requirements and guidance are applicable to a specific plant depends upon the age of the plant and the commitments established by the licensee in developing its fire protection program.

The information contained in Chapters 4 and 5 are provided for use in resolving the longstanding issues of MSOs. Using the Resolution Methodology described in these

chapters and in the appendices referenced within is one way for a licensee to address the MSO issue.

1.3.1 General Methodology Description

The deterministic methodology described in this document can be used to perform a post-fire safe shutdown analysis to address the current regulatory requirements. The Resolution Methodology for MSOs evaluates the risk significance of potential failures or combinations of failures. [Note: The term "MSOs" will be used throughout this document to denote one or more fire-induced component failures due to fire-induced circuit failures, including, but not limited to spurious operations resulting from hot shorts.] The Resolution Methodology for addressing MSOs is contained in Chapter 4.

1.3.2 Deterministic Method

When using the deterministic methodology to address the current regulatory requirements, a basic assumption of the methodology is that there will be fire damage to systems and equipment located within a common fire area. The size and intensity of the fire required to cause this system and equipment damage are not determined. Rather, fire damage is assumed to occur regardless of the level of combustibles in the area, the ignition temperatures of any combustible materials, the lack of an ignition source or the presence of automatic or manual fire suppression and detection capability. Fire damage is also postulated for all cables and equipment in the fire area that may be used for safe shutdown, even though most plant fire areas do not contain sufficient fire hazards for this to occur.

It is with these basic and conservative assumptions regarding fire damage that use of the Section 3 methodology begins. The methodology progresses by providing guidance on selecting systems and equipment needed for post-fire safe shutdown, on identifying the circuits of concern relative to these systems and equipment and on mitigating each fire-induced effect to the systems, equipment and circuits for the required safe shutdown path in each fire area. This methodology represents a comprehensive and safe approach for assuring that an operating plant can be safely shut down in the event of a single fire in any plant fire area.

To address the MSO issue, consideration is given to the MSO List in Appendix G and the circuit failure criteria contained in Appendix B. Using the Resolution Methodology described in Chapter 4, a licensee can determine the potential fire-induced MSO impacts applicable to its facility. These potential fire-induced impacts can then be dispositioned using the deterministic methods described in Chapter 3 or by using the risk-informed method described in Chapter 5. Additionally, fire modeling, as described in Chapter 4, may be used to assess whether or not a particular MSO in a particular location presents an impact to post-fire safe shutdown. In addressing MSOs the conservative assumptions discussed above for the Chapter 3 analysis are not necessarily applied, e.g. fire modeling or risk assessment may be an acceptable resolution approach.

In performing a deterministic post-fire safe shutdown analysis, the analyst must be cautious not to improperly apply the conservative assumptions described above. For example, one cannot rule out fire damage to unprotected circuits in a given fire area. This assumption is conservative only in terms of not being able to credit the systems and equipment associated with these circuits in support of post-fire safe shutdown. If the analyst, however, were to assume that these circuits were to be damaged by the fire when this provided an analytical advantage, this would be non-conservative. For example, assuming that fire damage results in a loss of offsite power may be non-conservative in terms of heat loads assumptions used in an analysis to determine the need for room cooling systems for the 72-hour fire coping period.

The methodology for performing deterministic post-fire safe shutdown analysis is depicted in Figure 1-1. The specific steps are summarized in Sections 1.3.2.1 through 1.3.2.6, and discussed in depth in Section 3.

1.3.2.1 Safe Shutdown Function Identification

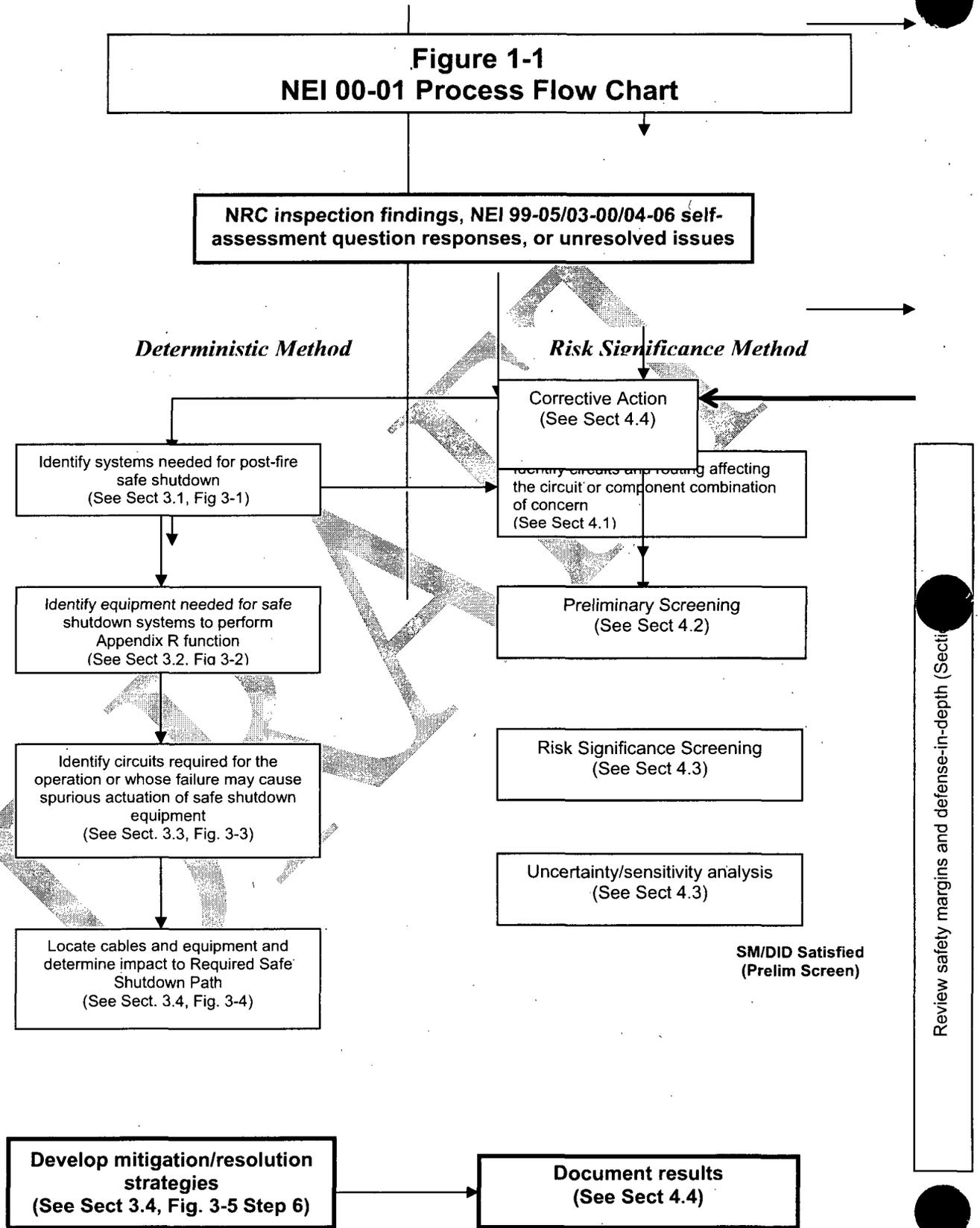
The goal of post-fire safe shutdown is to assure that a single fire in any single plant fire area will not result in any fuel cladding damage, rupture of the primary coolant boundary or rupture of the primary containment. This goal is accomplished by determining those functions important to safely shutting down the reactor and assuring that systems with the capability to perform these functions are not adversely impacted by a single fire in any plant fire area. The safe shutdown functions important to the plant are: (1) reactivity control; (2) pressure control; (3) inventory control; and (4) decay heat removal. To accomplish the required safe shutdown functions, certain support system functions (e.g., electrical power, ventilation) and process monitoring capability (e.g., reactor level, pressure indication) are also required.

In addition, the analyst must assure that fire-induced spurious operations do not occur that can prevent equipment in the required safe shutdown path from performing its intended safe shutdown function. Examples of spurious operations that present a potential concern for the safe shutdown functions described above are those that can cause a: (1) loss of inventory in excess of the make up capability; (2) flow diversion or a flow blockage in the safe shutdown systems being used to accomplish the inventory control function; (3) flow diversion or a flow blockage in the safe shutdown systems being used to accomplish the decay heat removal function¹. Additionally, Appendix G provides a Generic List of MSOs and Chapter 4 provides a methodology for converting this Generic List of MSOs to a Plant Specific List of MSOs through the use of an Expert Panel.

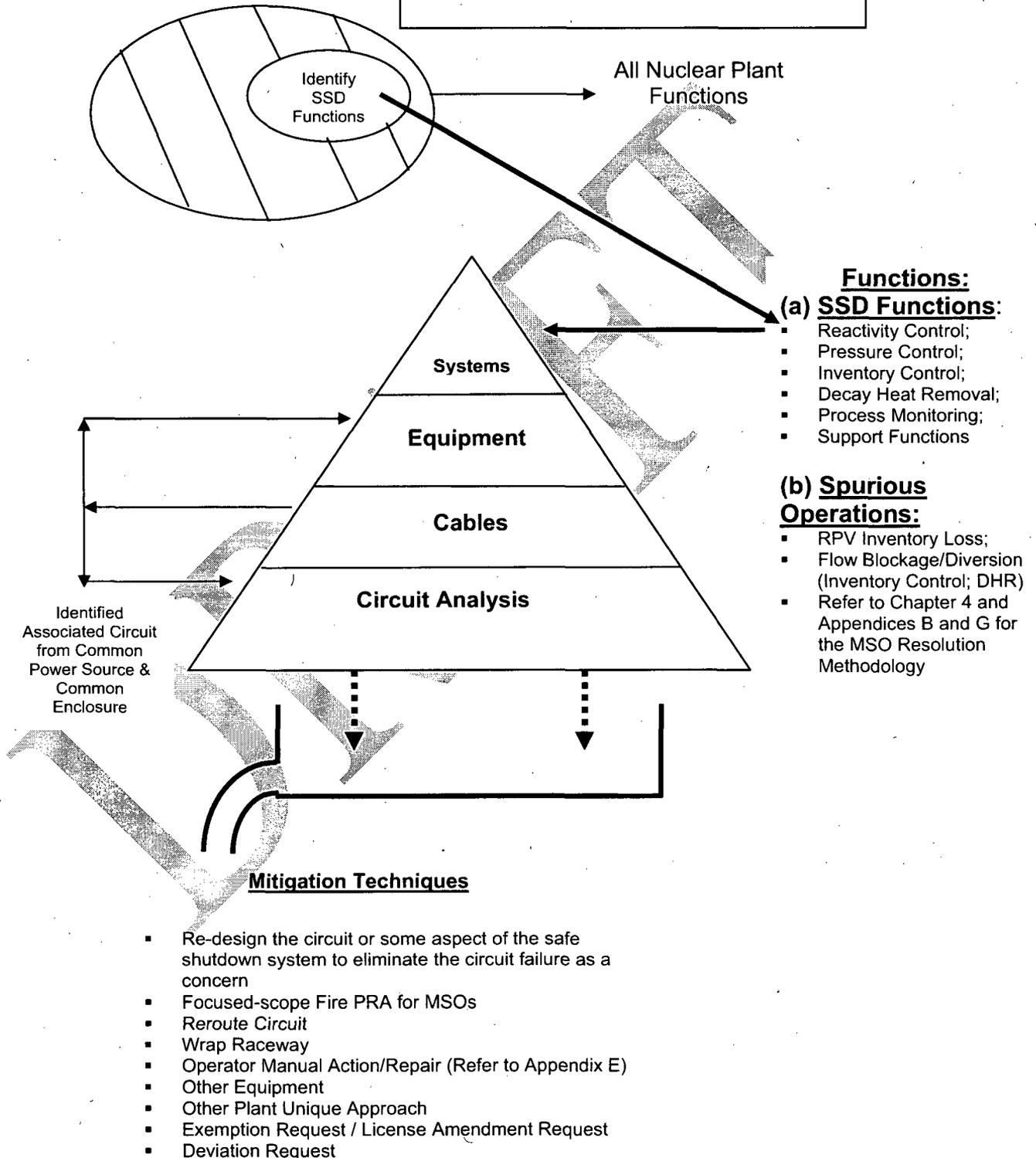
¹ Licensing Citation: Brown's Ferry SER dated November 2, 1995 Section 3.7.3 third paragraph. Monticello Inspection report dated December 3, 1986 paragraph (2) page 16.

[BWR] Although an inadvertent reactor vessel overfill condition is not a safe shutdown function listed above, the NRC has identified this as a concern. The acceptability of the current design features of the BWR to mitigate the effects of an inadvertent reactor vessel overfill condition as a result of either a fire or equipment failure has been addressed by the BWROG in GE Report No. EDE 07—390 dated April 2, 1990, in response to NRC Generic Letter 89-19. The NRC subsequently accepted the BWROG position in a Safety Evaluation dated June 9, 1994.

DRAFT



**Figure 1-1
Deterministic Post-fire
Safe Shutdown Overview**



1.3.2.2 Safe Shutdown System and Path Identification

Using the safe shutdown functions described above, the analyst identifies a system or combination of systems with the ability to perform each of these shutdown functions. The systems are combined to form safe shutdown paths.

1.3.2.3 Safe Shutdown Equipment Identification

Using the Piping and Instrument Diagrams (P&IDs) for the mechanical systems comprising each safe shutdown path, the analyst identifies the mechanical equipment required for the operation of the system and the equipment whose spurious operation could affect the performance of the safe shutdown systems. Equipment that is required for the operation of a safe shutdown system for a particular safe shutdown path is related to that path (i.e., designated as a safe shutdown component).

From a review of the associated P&IDs, the equipment that could spuriously operate and result in a flow blockage flow diversion (e.g., inventory makeup capability), loss of pressure control, etc. is identified. Similarly, this equipment is related to the particular safe shutdown path that it can affect.

The analyst reviews the P&IDs for the systems physically connected to the reactor vessel to determine the equipment that can result in a loss of reactor inventory in excess of make-up capability. This includes a special class of valves known as "high/low pressure interfaces." Refer to Appendix C for the special requirements associated with high/low pressure interface valves. Equipment in this category is typically related to all safe shutdown paths, since a loss of reactor vessel inventory would be a concern for any safe shutdown path.

1.3.2.4 Safe Shutdown Cable Identification

Using the electrical schematic drawings for the equipment identified above, the analyst identifies all the cables required for the proper operation of the safe shutdown equipment. This will include, in addition to the cables that are physically connected to the equipment, any cables interlocked to the primary electrical schematic through secondary schematics. The cables identified are related to the same safe shutdown path as the equipment they support.

While reviewing the electrical schematics for the equipment, the analyst identifies the safe shutdown equipment from the electrical distribution system (EDS). The EDS equipment (bus) for the safe shutdown path is associated with the equipment that it powers. All upstream busses are identified and similarly related to the safe shutdown path. In addition, all power cables associated with each bus in the EDS are identified and related to the same safe shutdown path as the EDS equipment. This information is required to support the Associated Circuits – Common Power Source Analysis.

1.3.2.5 Safe Shutdown Circuit Analysis

Using information on the physical routing of the required cables and the physical locations of all safe shutdown equipment, the analyst determines equipment and cable impact for each safe shutdown path in each plant fire area. Based on the number and types of impacts to these paths, each fire area is assigned a required safe shutdown path(s). Initially, it is assumed that any cables related to a required safe shutdown component in a given fire area will cause the component to fail in the worst-case position (i.e. if the safe shutdown position of a valve is closed, the valve is assumed to open if the required cable is routed in the fire area).

If necessary, a detailed analysis of the cable for the specific effect of the fire on that safe shutdown path is performed. This is accomplished by reviewing each conductor in each of these cables for the effects of a hot short, a short-to-ground or an open circuit² (test results indicate that open circuits are not the initial fire-induced failure mode) and determining the impact on the required safe shutdown component. The impact is assessed in terms of the effect on the safe shutdown system, the safe shutdown path, the safe shutdown functions and the goal for post-fire safe shutdown.

For the Plant Specific List of MSOs developed using the Resolution Methodology outlined in Chapter 4, apply the Circuit-Failure Criteria outlined in Appendix B.

1.3.2.6 Safe Shutdown Equipment Impacts

Using the process described above, the analyst identifies the potential impacts to safe shutdown equipment, systems, paths, and functions relied upon for each fire area, and then mitigates the effects on safe shutdown for each safe shutdown component impacted by the fire. The mitigating techniques must meet the regulations. For example, if an operator manual action is relied upon to mitigate the effects, then it must meet the regulatory acceptance criteria related to operator manual actions. Refer to Appendix E for additional information

The process of identifying and mitigating impacts to the required safe shutdown path(s) described above is explained in more detail throughout this document.

² Licensing Citation: Waterford III Submittal to NRR dated February 7, 1985, Item No. 5 on page 3. Susquehanna Steam Electric Station NRC Question 40.97 paragraph 3a. Wolf Creek/Callaway SSER 5 Section 9.5.1.5 second paragraph.

1.3.3 Risk Significance Methods

The Resolution Methodology for determining the Plant Specific List of MSOs is contained in Chapter 4. Refer to Chapter 4 for additional details. The method details both the determination of applicable plant-specific MSOs and the disposition/mitigation of the MSOs using either deterministic methods, Fire Modeling or risk (PRA) methods. The use of risk significance methods, such as a focused-scope Fire PRA is documented in Chapter 5.

DRAFT

2 APPENDIX R REQUIREMENTS AND CONSIDERATIONS

This section provides a general overview of the Appendix R regulatory requirements including the criteria for classifying the various shutdown methods. It describes the distinctions between redundant, alternative and dedicated shutdown capabilities and provides guidance for implementing these shutdown methods. In addition, the considerations dealing with a loss of offsite power and associated circuits concerns are also discussed. Refer to Figure 2-1.

2.1 REGULATORY REQUIREMENTS

10 CFR 50 Appendix A, General Design Criterion 3 establishes the overarching goals of NRC's fire protection requirements.

Criterion 3 -- Fire protection. Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials shall be used wherever practical throughout the unit, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Firefighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.

10 CFR 50 Appendix R Section III.G establishes the regulatory requirements for protecting structures, systems, equipment, cables and associated circuits required for achieving post-fire Appendix R Safe Shutdown, in order to satisfy the first sentence of GDC 3. Sections III.G.1 and III.G.2 discuss the requirements for "redundant" safe shutdown and Section III.G.3 discusses the requirements for "alternative or dedicated" shutdown. The requirements for each of these shutdown classifications will be considered separately.

The following sections discuss the regulations and distinctions regarding redundant shutdown methods. Requirements specifically for alternative/dedicated shutdown methods are discussed in Appendix D to this document:

Requirements for Redundant Safe Shutdown

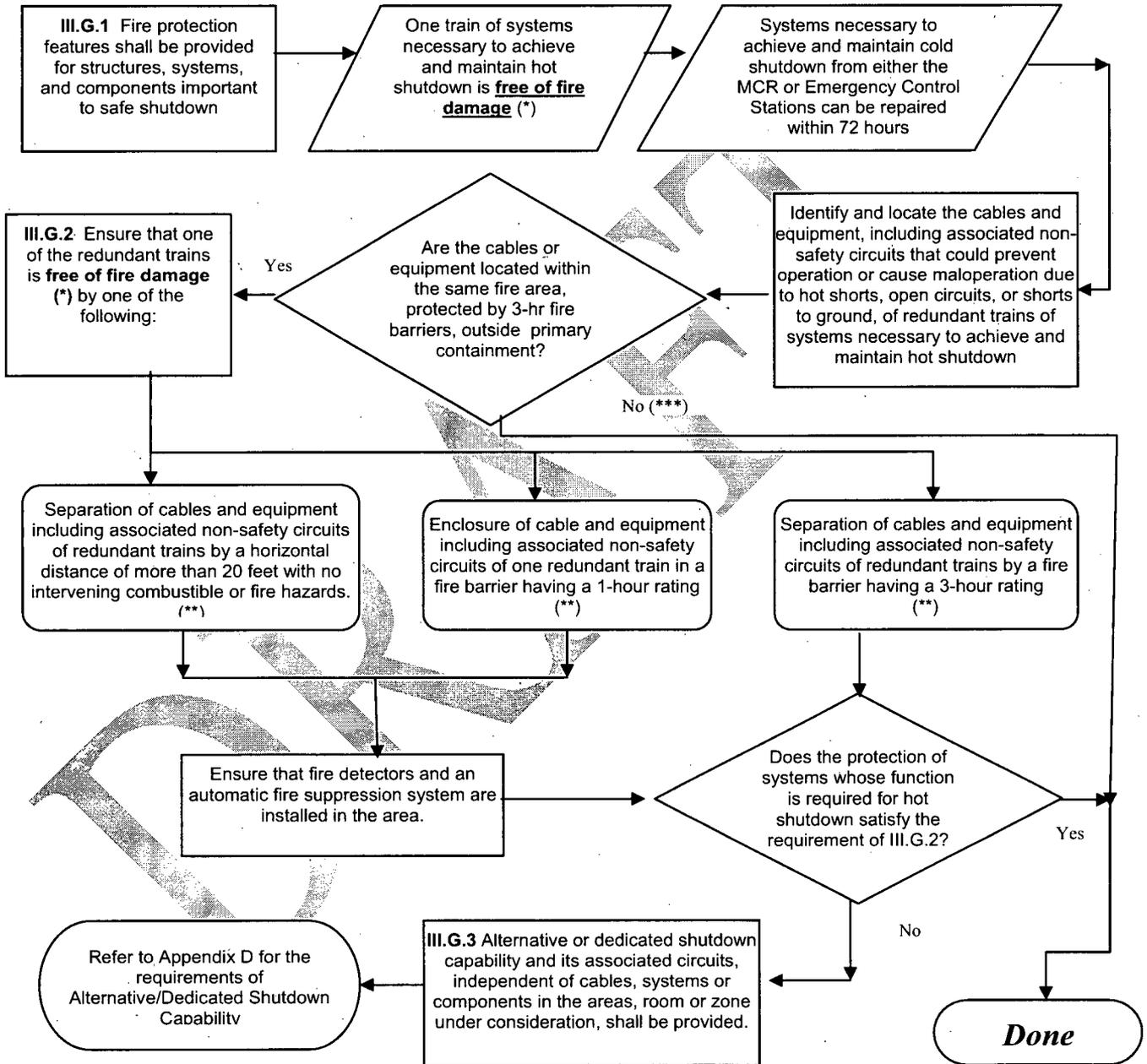
Section III.G.1 provides the requirements for fire protection of safe shutdown capability and states the following:

III. G. Fire protection of safe shutdown capability.

- I. *Fire protection features shall be provided for structures, systems, and components important to safe shutdown. These features shall be capable of limiting fire damage so that:*
 - a. *One train of systems necessary to achieve and maintain hot shutdown conditions from either the control room or emergency control station(s) is free of fire damage; and*
 - b. *Systems necessary to achieve and maintain cold shutdown from either the control room or emergency control station(s) can be repaired within 72 hours.*

DRAFT

Figure 2-1
Appendix R Requirements Flowchart



(*) "Free of Fire Damage" is achieved when the structure, system or component under consideration is capable of performing its intended function during and after the postulated fire, as needed

(**) Exemption Requests, Deviation Requests, GL 86-10 Fire Hazards Evaluations or Fire Protection Design Change Evaluations may be developed as necessary.

(***) For non-inerted containments, provide one of the protection methods identified in Appendix R Section III.G.2 (a), (b), or (c) or provide for 20 ft separation with no intervening combustibles or fire hazards, fire detection and automatic suppression, systems, or non-combustible radiant energy shields as specified in Appendix R Section III.G.2 (d), (e), or (f)

In Section III.G.1 there are no functional requirements specifically itemized for the structures, systems or components. The only requirements identified are those to initially achieve and maintain hot shutdown and to subsequently achieve cold shutdown once any required repairs have been completed.

Section III.G.1 establishes the requirement to ensure that adequate fire protection features exist to assure that one train of systems necessary to achieve and maintain hot shutdown is free of fire damage. Section III.G.1 presumes that some preexisting fire protection features have been provided, such as barriers (previously approved by the NRC under Appendix A to BTP APCS 9.5-1).

III.G.2 Except as provided for in paragraph G.3 of this section, where cables or equipment, including associated non-safety circuits that could prevent operation or cause maloperation due to hot shorts, open circuits, or shorts to ground, of redundant trains of systems necessary to achieve and maintain hot shutdown conditions are located within the same fire area outside of primary containment, one of the following means of ensuring that one of the redundant trains is free of fire damage shall be provided:

- a. Separation of cables and equipment and associated non-safety circuits of redundant trains by a fire barrier having a 3-hour rating. Structural steel forming a part of or supporting such fire barriers shall be protected to provide fire resistance equivalent to that required of the barrier;*
- b. Separation of cables and equipment and associated non-safety circuits of redundant trains by a horizontal distance of more than 20 feet with no intervening combustible or fire hazards. In addition, fire detectors and automatic fire suppression system shall be installed in the fire area; or*
- c. Enclosure of cable and equipment and associated non-safety circuits of one redundant train in a fire barrier having a 1-hour rating. In addition, fire detectors and an automatic fire suppression system shall be installed in the fire area;*

Inside non-inerted containments one of the fire protection means specified above or one of the following fire protection means shall be provided:

- d. Separation of cables and equipment and associated non-safety circuits of redundant trains by a horizontal distance of more than 20 feet with no intervening combustibles or fire hazards;*
- e. Installation of fire detectors and an automatic fire suppression system in the fire area; or*
- f. Separation of cables and equipment and associated non-safety circuits of redundant trains by a noncombustible radiant energy shield.*

Section III.G.2 provides separation requirements that must be utilized where redundant trains are located in the same fire area. To comply with the regulatory requirements in Section III.G.1 and 2, it is necessary to maintain those barriers previously reviewed and approved by the NRC under Appendix A to APCS 9.5-1 that provide separation essential for safe shutdown (this may include active fire suppression equipment originally credited for barrier functionality). Where redundant trains of systems necessary to achieve hot shutdown are located in the same fire area outside of primary containment, one must provide fire protection features consistent with the requirements of Section III.G.2.a, b, or c (III.G.2.d, e, and f are also acceptable options inside non-inerted containments) to protect structures, systems, components, cables and associated circuits for one train capable of achieving and maintaining hot shutdown conditions. One must also assure that any repairs required to equipment necessary to achieve and maintain cold shutdown, from either the MCR or emergency control station(s) can be made within 72 hours.

Depending on a plant's current licensing basis, exemptions, or deviations, or GL 86-10 fire hazards analyses and/or fire protection design change evaluations, NEI 02-03 (the replacement for the 10 CFR 50.59 process) may be used (when issued) to justify configurations that meet the underlying goals of Appendix R but not certain specific requirements.

2.2 REGULATORY GUIDANCE ON ASSOCIATED CIRCUITS

2.2.1 To ensure that safe shutdown systems remain available to perform their intended functions, the post-fire safe shutdown analysis also requires that other failures be evaluated to ensure that the safe shutdown system functions are not defeated. The analysis requires that consideration be given to cable failures that may cause spurious operations resulting in unwanted conditions. Also, circuit failures resulting in the loss of support systems such as the electrical power supply from improperly coordinated circuit protective devices must be considered. As defined in Generic Letter 81-12, these types of circuits are collectively referred to as associated circuits.³

2.2.2 Appendix R, Section III.G.2, states the following related to evaluating associated non-safety circuits when evaluating redundant shutdown capability

"Except as provided for in paragraph G.3 of this section, where cables or equipment, including associated non-safety circuits that can prevent operation or cause maloperation due to hot shorts, open circuits or shorts to ground, of redundant trains of systems necessary to achieve and maintain hot shutdown conditions are located within the same fire area outside of primary containment, one of the following means of assuring that one of the redundant trains is free of fire damage shall be provided..."

³ See the definition of "associated circuits of concern" in GL 81-12.

Associated circuits need to be evaluated to determine if cable faults can prevent the operation or cause the maloperation of redundant systems used to achieve and maintain hot shutdown.

From time to time, the NRC has issued Staff Positions (e.g., memorandum, Information Notices, Generic Letters, inspection findings) documenting their positions as to what systems they consider necessary to achieve and maintain hot shutdown conditions, as well as documenting what types of fire-induced faults should be considered credible for affecting these necessary systems.

2.2.3 NRC GL 81-12, Fire Protection Rule (45 FR 76602, November 19, 1980), dated February 20, 1981, provides additional clarification related to associated nonsafety circuits that can either prevent operation or cause maloperation of redundant safe shutdown trains. With respect to these associated circuits, GL 81-12 describes three types of associated circuits. The Clarification of Generic Letter 81-12 defines associated circuits of concern as those cables and equipment that:

- a). *Have a physical separation less than that required by Section III.G.2 of Appendix R, and:*
- b). *Have either:*
 - i) *A common power source with the shutdown equipment (redundant or alternative) and the power source is not electrically protected from the circuit of concern by coordinated breakers, fuses, or similar devices, or*
 - ii) *A connection to circuits of equipment whose spurious operation would adversely affect the shutdown capability (i.e., RHR/RCS isolation valves, ADS valves, PORVs, steam generator atmospheric dump valves, instrumentation, steam bypass, etc.), or*
 - iii) *A common enclosure (e.g., raceway, panel, junction) with the shutdown cables (redundant and alternative) and,*
 - (1) *are not electrically protected by circuit breakers, fuses or similar devices, or*
 - (2) *will not prevent propagation of the fire into the common enclosure.*

Although protecting the fire-induced failures of associated circuits is required, to reinforce that Generic Letter 81-12 simply provides guidance rather than requirements, the Clarification of Generic Letter 81-12 further states the following regarding alternatives for protecting the safe shutdown capability:

The guidelines for protecting the safe shutdown capability from fire-induced failures of associated circuits are not requirements. These guidelines should be

used only as guidance when needed. These guidelines do not limit the alternatives available to the licensee for protecting the safe shutdown capability. All proposed methods for protection of the shutdown capability from fire-induced failures will be evaluated by the [NRC] staff for acceptability.

2.3 REGULATORY INTERPRETATION ON LOSS OF OFFSITE POWER

2.3.1 The loss of offsite power has the potential to affect safe shutdown capability. In addition, the regulatory requirements for offsite power differ between the redundant and alternative/dedicated shutdown capability. Therefore, consideration must be given for the loss of offsite power when evaluating its effect on safe shutdown. The Appendix R requirement to consider a loss of offsite power is specified in Section III.L.3 as follows:

The shutdown capability for specific fire areas may be unique for each such area, or it may be one unique combination of systems for all such areas. In either case, the alternative shutdown capability shall be independent of the specific fire area(s) and shall accommodate post-fire conditions where offsite power is available and where offsite power is not available for 72 hours. Procedures shall be in effect to implement this capability.

2.3.2 Alternative/dedicated systems must demonstrate shutdown capability where offsite power is available and where offsite power is not available for 72 hours. If such equipment and systems used prior to 72 hours after the fire will not be capable of being powered by both onsite and offsite electric power systems because of fire damage, an independent onsite power system shall be provided. Equipment and systems used after 72 hours may be powered by offsite power only.

2.3.3 For redundant shutdown, offsite power may be credited if demonstrated to be free of fire damage, similar to other safe shutdown systems.

2.3.4 If offsite power is postulated to be lost for a particular fire area, and is not needed for the required safe shutdown path for 72 hours, actions necessary for its restoration are considered to be performed under the purview of the emergency response organization and do not require the development of specific recovery strategies or procedures in advance.

2.3.5 Since in an actual fire event offsite power may or may not be available, the potential availability of offsite power should also be considered to confirm that it does not pose a more challenging condition. For example, additional electric heat loads may affect HVAC strategies.

3 DETERMINISTIC METHODOLOGY

This section discusses a generic deterministic methodology and criteria that licensees can use to perform a post-fire safe shutdown analysis to address regulatory requirements. The plant-specific analysis approved by NRC is reflected in the plant's licensing basis. The methodology described in this section is also an acceptable method of performing a post-fire safe shutdown analysis. This methodology is indicated in Figure 3-1. Other methods acceptable to NRC may also be used. Regardless of the method selected by an individual licensee, the criteria and assumptions provided in this guidance document may apply. The methodology described in Section 3 is based on a computer database oriented approach, which is utilized by several licensees to model Appendix R data relationships. This guidance document, however, does not require the use of a computer database oriented approach.

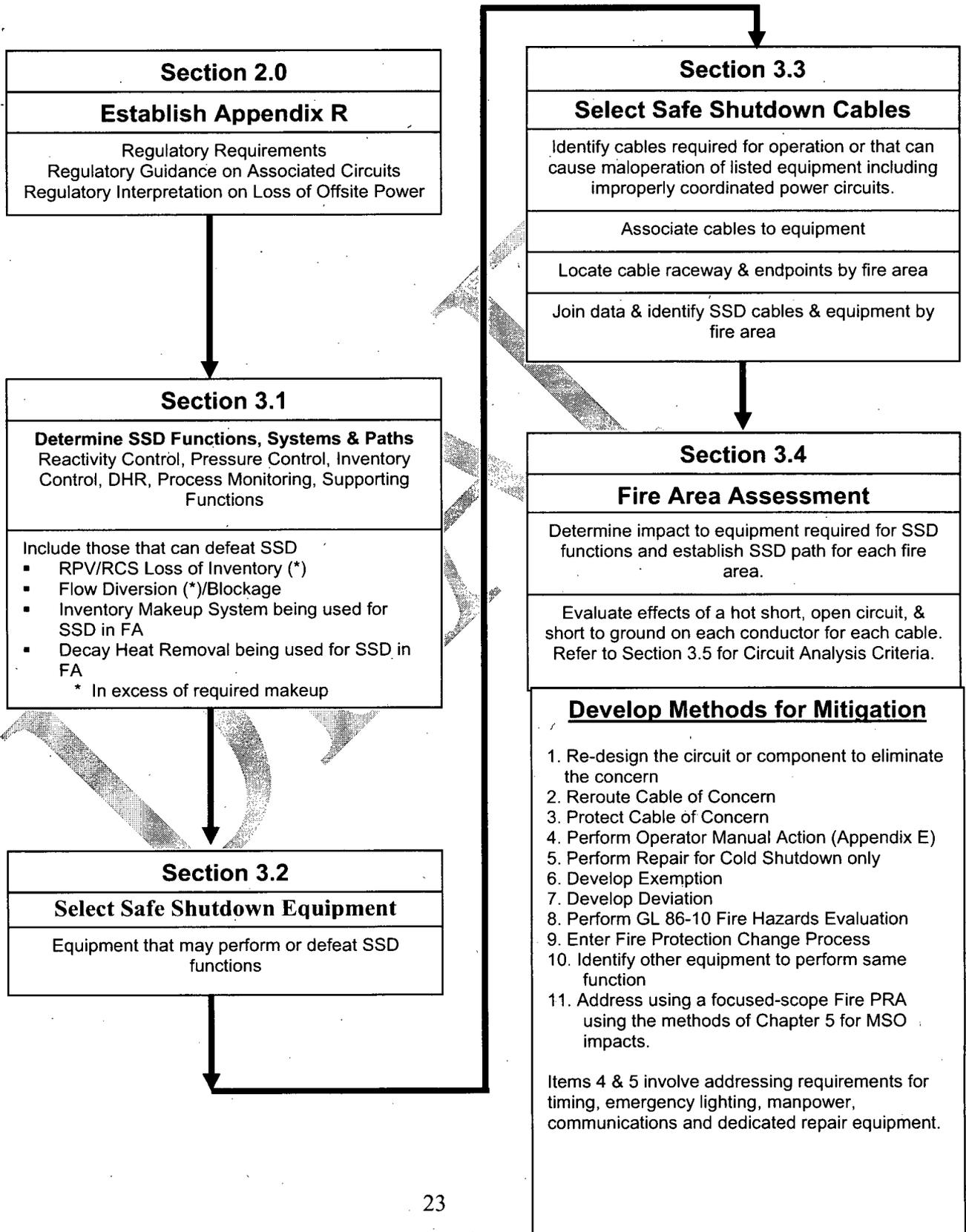
The requirements of Appendix R Sections III.G.1, III.G.2 and III.G.3 apply to equipment and cables required for achieving and maintaining safe shutdown in any fire area. Although equipment and cables for fire detection and suppression systems, communications systems and 8-hour emergency lighting systems are important features, this guidance document does not address them.

Additional information is provided in Appendix B to this document related to the circuit failure criteria to be applied in assessing the impact of MSOs on post-fire safe shutdown. Chapter 4 provides the Resolution methodology for determining the Plant Specific List of MSOs to be evaluated. Chapter 5 provides a focused-scope Fire PRA risk methodology for assessing the risk significance of any MSOs determined to be impacted within a common plant fire area.

3.1 SAFE SHUTDOWN SYSTEMS AND PATH DEVELOPMENT

This section discusses the identification of systems available and necessary to perform the required safe shutdown functions. It also provides information on the process for combining these systems into safe shutdown paths. Appendix R Section III.G.1.a requires that the capability to achieve and maintain hot shutdown be free of fire damage. Appendix R Section III.G.1.b requires that repairs to systems and equipment necessary to achieve and maintain cold shutdown be completed within 72 hours.

**Figure 3-1
Deterministic Guidance Methodology Overview**



The goal of post-fire safe shutdown is to assure that a one train of shutdown systems, structures, and components remains free of fire damage for a single fire in any single plant fire area. This goal is accomplished by determining those functions important to achieve and maintain hot shutdown. Safe shutdown systems are selected so that the capability to perform these required functions is a part of each safe shutdown path. The functions important to post-fire safe shutdown generally include, but are not limited to the following:

- Reactivity control
- Pressure control systems
- Inventory control systems
- Decay heat removal systems
- Process monitoring
- Support systems
 - Electrical systems
 - Cooling systems

These functions are of importance because they have a direct bearing on the safe shutdown goal of being able to achieve and maintain hot shutdown, which ensures the integrity of the fuel, the reactor pressure vessel and the primary containment. If these functions are preserved, then the plant will be safe because the fuel, the reactor and the primary containment will not be damaged. By assuring that this equipment is not damaged and remains functional, the protection of the health and safety of the public is assured.

In addition to the above listed functions, Generic Letter 81-12 specifies consideration of associated circuits with the potential for spurious equipment operation and/or loss of power source, and the common enclosure failures. Spurious operations/actuators can affect the accomplishment of the post-fire safe shutdown functions listed above. Typical examples of the effects of the spurious operations of concern are the following:

- A loss of reactor pressure vessel/reactor coolant inventory in excess of the safe shutdown makeup capability
- A flow loss or blockage in the inventory makeup or decay heat removal systems being used for the required safe shutdown path.

Spurious operations are of concern because they have the potential to directly affect the ability to achieve and maintain hot shutdown, which could affect the fuel and cause damage to the reactor pressure vessel or the primary containment. Additionally, Chapter 4 provides a Resolution Methodology for developing a Plant Specific List of MSOs for evaluation. Appendix B provides the circuit failure criteria applicable to the evaluation of the Plant Specific list of MSOs.

Common power source and common enclosure concerns could also affect these and must be addressed.

3.1.1 Criteria/Assumptions

The following criteria and assumptions may be considered when identifying systems available and necessary to perform the required safe shutdown functions and combining these systems into safe shutdown paths.

- 3.1.1.1 [BWR] GE Report GE-NE-T43-00002-00-01-R01 entitled "Original Safe Shutdown Paths For The BWR" addresses the systems and equipment originally designed into the GE boiling water reactors (BWRs) in the 1960s and 1970s, that can be used to achieve and maintain safe shutdown per Section III.G.1 of 10 CFR 50, Appendix R. Any of the shutdown paths (methods) described in this report are considered to be acceptable methods for achieving redundant safe shutdown.
- 3.1.1.2 [BWR] GE Report GE-NE-T43-00002-00-03-R01 provides a discussion on the BWR Owners' Group (BWROG) position regarding the use of Safety Relief Valves (SRVs) and low pressure systems (LPCI/CS) for safe shutdown. The BWROG position is that the use of SRVs and low pressure systems is an acceptable methodology for achieving redundant safe shutdown in accordance with the requirements of 10 CFR 50 Appendix R Sections III.G.1 and III.G.2. The NRC has accepted the BWROG position and issued an SER dated Dec. 12, 2000.
- 3.1.1.3 [PWR] Generic Letter 86-10, Enclosure 2, Section 5.3.5 specifies that hot shutdown can be maintained without the use of pressurizer heaters (i.e., pressure control is provided by controlling the makeup/charging pumps). Hot shutdown conditions can be maintained via natural circulation of the RCS through the steam generators. The cooldown rate must be controlled to prevent the formation of a bubble in the reactor head. Therefore, feedwater (either auxiliary or emergency) flow rates as well as steam release must be controlled.
- 3.1.1.4 The classification of shutdown capability as alternative shutdown is made independent of the selection of systems used for shutdown. Alternative shutdown capability is determined based on an inability to assure the availability of a redundant safe shutdown path. Compliance to the separation requirements of Sections III.G.1 and III.G.2 may be supplemented by the use of operator manual actions to the extent allowed by the regulations and the licensing basis of the plant (see Appendix E), repairs (cold shutdown only), exemptions, deviations, GL 86-10 fire hazards analyses or fire protection design change evaluations, as appropriate. These may also be used in conjunction with alternative shutdown capability.

- 3.1.1.5 At the onset of the postulated fire, all safe shutdown systems (including applicable redundant trains) are assumed operable and available for post-fire safe shutdown. Systems are assumed to be operational with no repairs, maintenance, testing, Limiting Conditions for Operation, etc. in progress. The units are assumed to be operating at full power under normal conditions and normal lineups.
- 3.1.1.6 No Final Safety Analysis Report accidents or other design basis events (e.g. loss of coolant accident, earthquake), single failures or non-fire-induced transients need be considered in conjunction with the fire.
- 3.1.1.7 For the case of redundant shutdown, offsite power may be credited if demonstrated to be free of fire damage. Offsite power should be assumed to remain available for those cases where its availability may adversely impact safety (i.e., reliance cannot be placed on fire causing a loss of offsite power if the consequences of offsite power availability are more severe than its presumed loss). No credit should be taken for a fire causing a loss of offsite power. For areas where train separation cannot be achieved and alternative shutdown capability is necessary, shutdown must be demonstrated both where offsite power is available and where offsite power is not available for 72 hours.
- 3.1.1.8 Post-fire safe shutdown systems and components are not required to be safety-related.
- 3.1.1.9 The post-fire safe shutdown analysis assumes a 72-hour coping period starting with a reactor scram/trip. Fire-induced impacts that provide no adverse consequences to hot shutdown within this 72-hour period need not be included in the post-fire safe shutdown analysis. At least one train can be repaired or made operable within 72 hours using onsite capability to achieve cold shutdown.
- 3.1.1.10 Manual initiation from the main control room or emergency control stations of systems required to achieve and maintain safe shutdown is acceptable where permitted by current regulations or approved by NRC (See Appendix E); automatic initiation of systems selected for safe shutdown is not required but may be included as an option, if the additional cables and equipment are also included in the analysis.
- 3.1.1.11 Where a single fire can impact more than one unit of a multi-unit plant, the ability to achieve and maintain safe shutdown for each affected unit must be demonstrated.

3.1.2 Shutdown Functions

The following discussion on each of these shutdown functions provides guidance for selecting the systems and equipment required for safe shutdown. For additional information on BWR system selection, refer to GE Report GE-NE-T43-00002-00-01-R01 entitled "Original Safe Shutdown Paths for the BWR."

3.1.2.1 Reactivity Control

[BWR] Control Rod Drive System

The safe shutdown performance and design requirements for the reactivity control function can be met without automatic scram/trip capability. Manual scram/reactor trip is credited. The post-fire safe shutdown analysis must only provide the capability to manually scram/trip the reactor. Each licensee should have an operator manual action to either vent the instrument air header or to remove RPS power in their post-fire safe shutdown procedures. The presence of this action precludes the need to perform circuit analysis for the reactivity control function and is an acceptable way to accomplish this function.

[PWR] Makeup/Charging

There must be a method for ensuring that adequate shutdown margin is maintained from initial reactor SCRAM to cold shutdown conditions, by ensuring boric acid water is utilized for RCS makeup/charging.

3.1.2.2 Pressure Control Systems

The systems discussed in this section are examples of systems that can be used for pressure control. This does not restrict the use of other systems for this purpose.

[BWR] Safety Relief Valves (SRVs)

Initial pressure control may be provided by the SRVs mechanically cycling at their setpoints (electrically cycling for EMRVs). Mechanically-actuated SRVs require no electrical analysis to perform their overpressure protection function. The SRVs may also be opened to maintain hot shutdown conditions or to depressurize the vessel to allow injection using low pressure systems. These are operated manually. Automatic initiation of the Automatic Depressurization System (ADS) is not a required function. Automatic initiation of the ADS may be credited, if available. If automatic ADS is not available and use of ADS is desired, an alternative means of initiation ADS separate from the automatic initiation logic for accomplishing the pressure control function should be provided.

[PWR] Makeup/Charging

RCS pressure is controlled by controlling the rate of charging/makeup to the RCS. Although utilization of the pressurizer heaters and/or auxiliary spray reduces operator burden, neither component is required to provide adequate pressure control. Pressure reductions are made by allowing the RCS to cool/shrink, thus reducing pressurizer level/pressure. Pressure increases are made by initiating charging/makeup to maintain pressurizer level/pressure. Manual control of the related pumps is acceptable.

3.1.2.3 Inventory Control

[BWR] Systems selected for the inventory control function should be capable of supplying sufficient reactor coolant to achieve and maintain hot shutdown. Manual initiation of these systems is acceptable. Automatic initiation functions are not required.

[PWR]: Systems selected for the inventory control function should be capable of maintaining level to achieve and maintain hot shutdown. Typically, the same components providing inventory control are capable of providing pressure control. Manual initiation of these systems is acceptable. Automatic initiation functions are not required.

3.1.2.4 Decay Heat Removal

[BWR] Systems selected for the decay heat removal function(s) should be capable of:

- Removing sufficient decay heat from primary containment, to prevent containment over-pressurization and failure.
- Satisfying the net positive suction head requirements of any safe shutdown systems taking suction from the containment (suppression pool).
- Removing sufficient decay heat from the reactor to achieve cold shutdown.

[PWR] Systems selected for the decay heat removal function(s) should be capable of:

- Removing sufficient decay heat from the reactor to reach hot shutdown conditions. Typically, this entails utilizing natural circulation in lieu of forced circulation via the reactor coolant pumps and controlling steam release via the Atmospheric Dump valves.
- Removing sufficient decay heat from the reactor to reach cold shutdown conditions.

This does not restrict the use of other systems.

3.1.2.5 Process Monitoring

The process monitoring function is provided for all safe shutdown paths. IN 84-09, Attachment 1, Section IX "Lessons Learned from NRC Inspections of Fire Protection Safe Shutdown Systems (10 CFR 50 Appendix R)" provides guidance on the instrumentation acceptable to and preferred by the NRC for meeting the process monitoring function. This instrumentation is that which monitors the process variables necessary to perform and control the functions specified in Appendix R Section III.L.1. Such instrumentation must be demonstrated to remain unaffected by the fire. The IN 84-09 list of process monitoring is applied to alternative shutdown (III.G.3). IN 84-09 did not identify specific instruments for process monitoring to be applied to redundant shutdown (III.G.1 and III.G.2). In general, process monitoring instruments similar to those listed below are needed to successfully use existing operating procedures (including Abnormal Operating Procedures).

BWR

- Reactor coolant level and pressure
- Suppression pool level and temperature
- Emergency or isolation condenser level
- Diagnostic instrumentation for safe shutdown systems
- Level indication for tanks needed for safe shutdown

PWR

- Reactor coolant temperature (hot leg / cold leg)
- Pressurizer pressure and level
- Neutron flux monitoring (source range)
- Level indication for tanks needed for safe shutdown
- Steam generator level and pressure
- Diagnostic instrumentation for safe shutdown systems

The specific instruments required may be based on operator preference, safe shutdown procedural guidance strategy (symptomatic vs. prescriptive), and systems and paths selected for safe shutdown.

3.1.2.6 Support Systems

3.1.2.6.1 Electrical Systems

AC Distribution System

Power for the Appendix R safe shutdown equipment is typically provided by a medium voltage system such as 4.16 KV Class 1E busses either directly from the busses or through step down transformers/load centers/distribution panels for 600, 480 or 120 VAC loads. For redundant safe shutdown performed in accordance with the requirements of Appendix R Section III.G.1 and 2, power may be supplied from either offsite power sources or the emergency diesel generator depending on which has been demonstrated to be free of fire damage. No credit should be taken for the beneficial effects of a fire causing a loss of offsite power. Refer to Section 3.1.1.7.

DC Distribution System

Typically, the 125VDC distribution system supplies DC control power to various 125VDC control panels including switchgear breaker controls. The 125VDC distribution panels may also supply power to the 120VAC distribution panels via static inverters. These distribution panels typically supply power for instrumentation necessary to complete the process monitoring functions.

For fire events that result in an interruption of power to the AC electrical bus, the station batteries are necessary to supply any required control power during the interim time period required for the diesel generators to become operational. Once the diesels are operational, the 125VDC distribution system can be powered from the diesels through the battery chargers.

[BWR] Certain plants are also designed with a 250VDC Distribution System that supplies power to Reactor Core Isolation Cooling and/or High Pressure Coolant Injection equipment.

The DC control centers may also supply power to various small horsepower Appendix R safe shutdown system valves and pumps. If the DC system is relied upon to support safe shutdown without battery chargers being available, it must be verified that sufficient battery capacity exists to support the necessary loads for sufficient time (either until power is restored, or the loads are no longer required to operate).

3.1.2.6.2 Cooling Systems

Various cooling water systems may be required to support safe shutdown system operation, based on plant-specific considerations. Typical uses include:

- RHR/SDC/DH Heat Exchanger cooling water
- Safe shutdown pump cooling (seal coolers, oil coolers)
- Diesel generator cooling
- HVAC system cooling water.

HVAC Systems

HVAC Systems may be required to assure that safe shutdown equipment remains within its operating temperature range, as specified in manufacturer's literature or demonstrated by suitable test methods, and to assure protection for plant operations staff from the effects of fire (smoke, heat, toxic gases, and gaseous fire suppression agents).

HVAC systems may be required to support safe shutdown system operation, based on plant-specific configurations. Typical uses include:

- Main control room, cable spreading room, relay room
- ECCS pump compartments
- Diesel generator rooms
- Switchgear rooms

Plant-specific evaluations are necessary to determine which HVAC systems are essential to safe shutdown equipment operation. Transient temperature response analyses are often utilized to demonstrate that specific HVAC systems would not be required. If HVAC systems are credited, the potential for adverse fire effects to the HVAC system must also be considered, including:

- Dampers closing due to fire exposure
- Recirculation or migration of toxic conditions (e.g., smoke from the fire, suppressants such as Carbon Dioxide).

3.1.3 Methodology for Shutdown System Selection

Refer to Figure 3-2 for a flowchart illustrating the various steps involved in selecting safe shutdown systems and developing the shutdown paths.

The following methodology may be used to define the safe shutdown systems and paths for an Appendix R analysis:

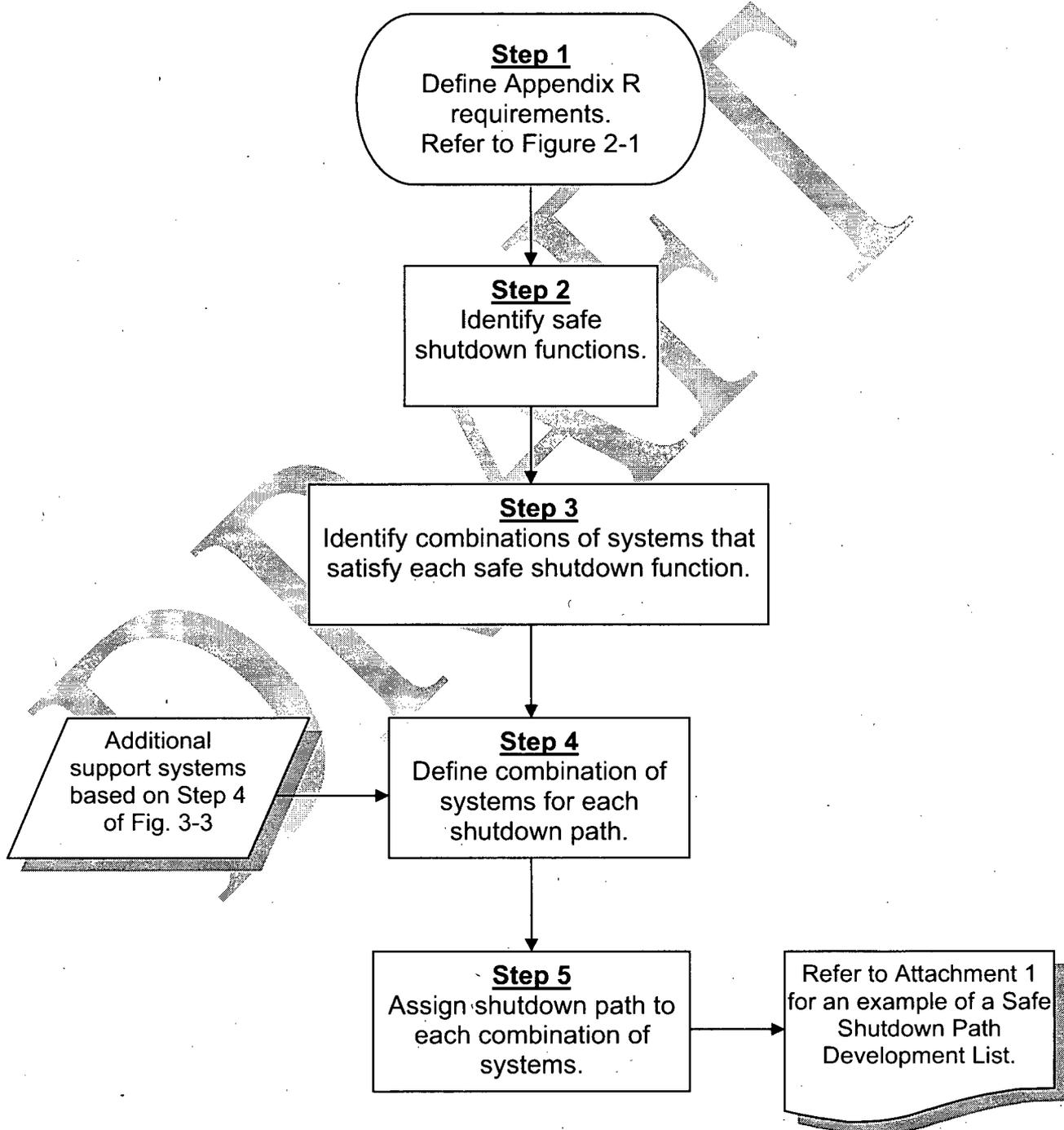
3.1.3.1 Identify safe shutdown functions

Review available documentation to obtain an understanding of the available plant systems and the functions required to achieve and maintain safe shutdown. Documents such as the following may be reviewed:

- Operating Procedures (Normal, Emergency, Abnormal)
- System descriptions
- Fire Hazard Analysis
- Single-line electrical diagrams
- Piping and Instrumentation Diagrams (P&IDs)
- [BWR] GE Report GE-NE-T43-00002-00-01-R02 entitled "Original Shutdown Paths for the BWR"

DRAFT

Figure 3-2
Safe Shutdown System Selection and Path Development



3.1.3.2 Identify Combinations of Systems That Satisfy Each Safe Shutdown Function

Given the criteria/assumptions defined in Section 3.1.1, identify the available combinations of systems capable of achieving the safe shutdown functions of reactivity control, pressure control, inventory control, decay heat removal, process monitoring and support systems such as electrical and cooling systems (refer to Section 3.1.2). This selection process does not restrict the use of other systems. In addition to achieving the required safe shutdown functions, consider spurious operations and power supply issues that could impact the required safe shutdown function.

3.1.3.3 Define Combination of Systems for Each Safe Shutdown Path

Select combinations of systems with the capability of performing all of the required safe shutdown functions and designate this set of systems as a safe shutdown path. In many cases, paths may be defined on a divisional basis since the availability of electrical power and other support systems must be demonstrated for each path. During the equipment selection phase, identify any additional support systems and list them for the appropriate path.

3.1.3.4 Assign Shutdown Paths to Each Combination of Systems

Assign a path designation to each combination of systems. The path will serve to document the combination of systems relied upon for safe shutdown in each fire area. Refer to Attachment 1 to this document for an example of a table illustrating how to document the various combinations of systems for selected shutdown paths.

3.2 SAFE SHUTDOWN EQUIPMENT SELECTION

The previous section described the methodology for selecting the systems and paths necessary to achieve and maintain safe shutdown for an exposure fire event (see Section 5.0 DEFINITIONS for "Exposure Fire"). This section describes the criteria/assumptions and selection methodology for identifying the specific safe shutdown equipment necessary for the systems to perform their Appendix R function. The selected equipment should be related back to the safe shutdown systems that they support and be assigned to the same safe shutdown path as that system. The list of safe shutdown equipment will then form the basis for identifying the cables necessary for the operation or that can cause the maloperation of the safe shutdown systems.

3.2.1 Criteria/Assumptions

Consider the following criteria and assumptions when identifying equipment necessary to perform the required safe shutdown functions:

3.2.1.1 Safe shutdown equipment can be divided into two categories. Equipment may be categorized as (1) primary components or (2) secondary components. Typically, the following types of equipment are considered to be primary components:

- Pumps, motor operated valves, solenoid valves, fans, gas bottles, dampers, unit coolers, etc.
- All necessary process indicators and recorders (i.e., flow indicator, temperature indicator, turbine speed indicator, pressure indicator, level recorder)
- Power supplies or other electrical components that support operation of primary components (i.e., diesel generators, switchgear, motor control centers, load centers, power supplies, distribution panels, etc.).

Secondary components are typically items found within the circuitry for a primary component. These provide a supporting role to the overall circuit function. Some secondary components may provide an isolation function or a signal to a primary component via either an interlock or input signal processor. Examples of secondary components include flow switches, pressure switches, temperature switches, level switches, temperature elements, speed elements, transmitters, converters, controllers, transducers, signal conditioners, hand switches, relays, fuses and various instrumentation devices.

Determine which equipment should be included on the Safe Shutdown Equipment List (SSEL). As an option, include secondary components with a primary component(s) that would be affected by fire damage to the secondary component. By doing this, the SSEL can be kept to a manageable size and the equipment included on the SSEL can be readily related to required post-fire safe shutdown systems and functions.

3.2.1.2 Assume that exposure fire damage to manual valves and piping does not adversely impact their ability to perform their pressure boundary or safe shutdown function (heat sensitive piping materials, including tubing with brazed or soldered joints, are not included in this assumption). Fire damage should be evaluated with respect to the ability to manually open or close the valve should this be necessary as a part of the post-fire safe shutdown scenario.

- 3.2.1.3 Assume that manual valves are in their normal position as shown on P&IDs or in the plant operating procedures.
- 3.2.1.4 Assume that a check valve closes in the direction of potential flow diversion and seats properly with sufficient leak tightness to prevent flow diversion. Therefore, check valves do not adversely affect the flow rate capability of the safe shutdown systems being used for inventory control, decay heat removal, equipment cooling or other related safe shutdown functions.
- 3.2.1.5 Instruments (e.g., resistance temperature detectors, thermocouples, pressure transmitters, and flow transmitters) are assumed to fail upscale, midscale, or downscale as a result of fire damage, whichever is worse. An instrument performing a control function is assumed to provide an undesired signal to the control circuit.
- 3.2.1.6 Identify equipment that could spuriously operate or mal-operate and impact the performance of equipment on a required safe shutdown path during the equipment selection phase. Additionally, refer to Chapter 4 for the Resolution Methodology for determining the Plant Specific List of MSOs requiring evaluation.
- 3.2.1.7 Identify instrument tubing that may cause subsequent effects on instrument readings or signals as a result of fire. Determine and consider the fire area location of the instrument tubing when evaluating the effects of fire damage to circuits and equipment in the fire area.

3.2.2 Methodology for Equipment Selection

Refer to Figure 3-3 for a flowchart illustrating the various steps involved in selecting safe shutdown equipment.

Use the following methodology to select the safe shutdown equipment for a post-fire safe shutdown analysis:

3.2.2.1 Identify the System Flow Path for Each Shutdown Path

Mark up and annotate a P&ID to highlight the specific flow paths for each system in support of each shutdown path. Refer to Attachment 2 for an example of an annotated P&ID illustrating this concept.

3.2.2.2 Identify the Equipment in Each Safe Shutdown System Flow Path Including Equipment That May Spuriously Operate and Affect System Operation

Review the applicable documentation (e.g. P&IDs, electrical drawings, instrument loop diagrams) to assure that all equipment in each system's flow path has been identified. Assure that any equipment that could spuriously

operate and adversely affect the desired system function(s) is also identified. If additional systems are identified which are necessary for the operation of the safe shutdown system under review, include these as systems required for safe shutdown. Designate these new systems with the same safe shutdown path as the primary safe shutdown system under review (Refer to Figure 3-1).

3.2.2.3 Develop a List of Safe Shutdown Equipment and Assign the Corresponding System and Safe Shutdown Path(s) Designation to Each.

Prepare a table listing the equipment identified for each system and the shutdown path that it supports. Identify any valves or other equipment that could spuriously operate and impact the operation of that safe shutdown system. Assign the safe shutdown path for the affected system to this equipment. During the cable selection phase, identify additional equipment required to support the safe shutdown function of the path (e.g., electrical distribution system equipment). Include this additional equipment in the safe shutdown equipment list. Attachment 3 to this document provides an example of a (SSEL). The SSEL identifies the list of equipment within the plant considered for safe shutdown and it documents various equipment-related attributes used in the analysis.

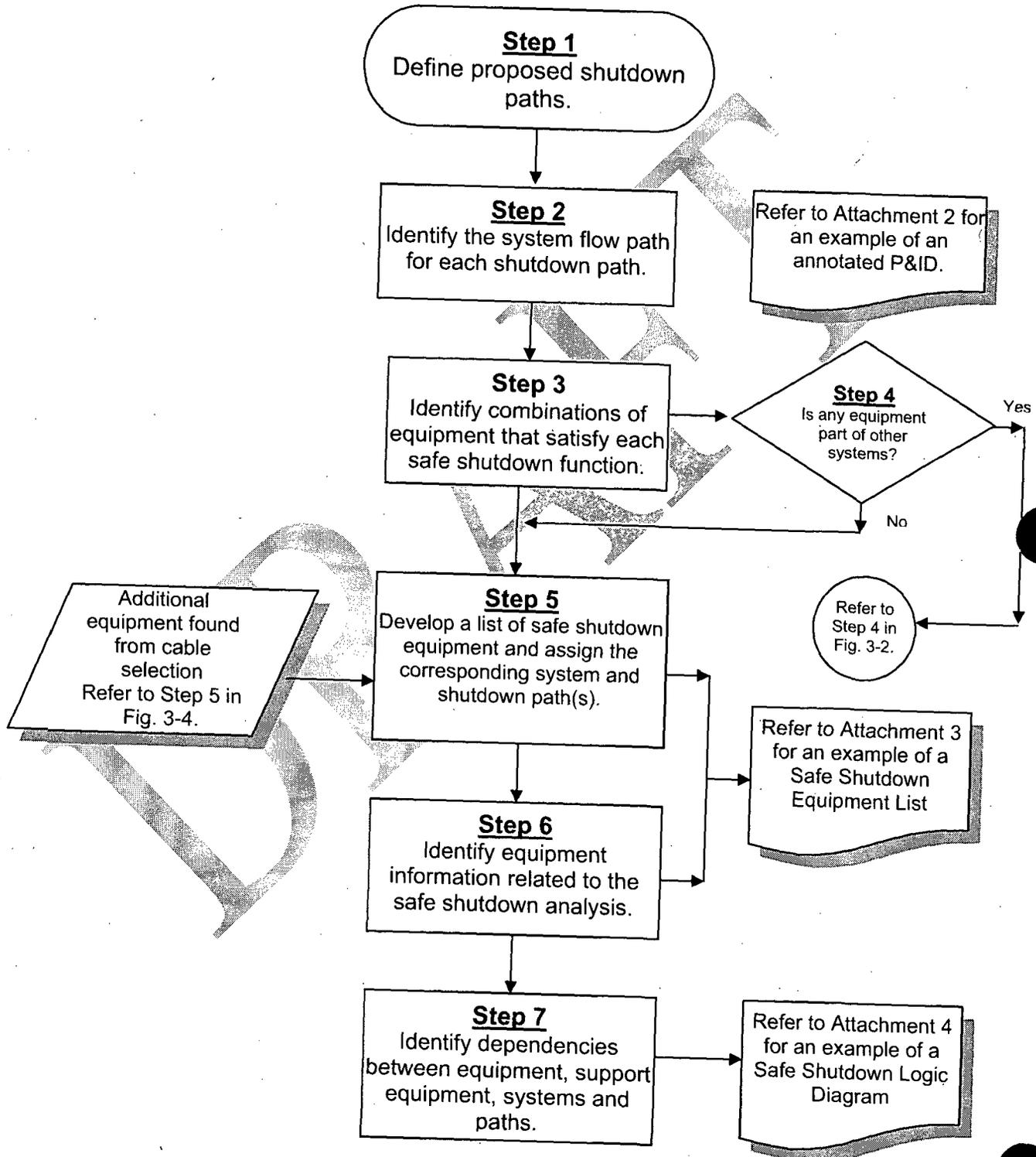
3.2.2.4 Identify Equipment Information Required for the Safe Shutdown Analysis

Collect additional equipment-related information necessary for performing the post-fire safe shutdown analysis for the equipment. In order to facilitate the analysis, tabulate this data for each piece of equipment on the SSEL. Refer to Attachment 3 to this document for an example of a SSEL. Examples of related equipment data should include the equipment type, equipment description, safe shutdown system, safe shutdown path, drawing reference, fire area, fire zone, and room location of equipment. Other information such as the following may be useful in performing the safe shutdown analysis: normal position, hot shutdown position, cold shutdown position, failed air position, failed electrical position, high/low pressure interface concern, and spurious operation concern.

3.2.2.5 Identify Dependencies Between Equipment, Supporting Equipment, Safe Shutdown Systems and Safe Shutdown Paths.

In the process of defining equipment and cables for safe shutdown, identify additional supporting equipment such as electrical power and interlocked equipment. As an aid in assessing identified impacts to safe shutdown, consider modeling the dependency between equipment within each safe shutdown path either in a relational database or in the form of a Safe Shutdown Logic Diagram (SSLD). Attachment 4 provides an example of a SSLD that may be developed to document these relationships.

Figure 3-3
Safe Shutdown Equipment Selection



3.3 SAFE SHUTDOWN CABLE SELECTION AND LOCATION

This section provides industry guidance on the recommended methodology and criteria for selecting safe shutdown cables and determining their potential impact on equipment required for achieving and maintaining safe shutdown of an operating nuclear power plant for the condition of an exposure fire. The Appendix R safe shutdown cable selection criteria are developed to ensure that all cables that could affect the proper operation or that could cause the maloperation of safe shutdown equipment are identified and that these cables are properly related to the safe shutdown equipment whose functionality they could affect. Through this cable-to-equipment relationship, cables become part of the safe shutdown path assigned to the equipment affected by the cable.

3.3.1 Criteria/Assumptions

To identify an impact to safe shutdown equipment based on cable routing, the equipment must have cables that affect it identified. Carefully consider how cables are related to safe shutdown equipment so that impacts from these cables can be properly assessed in terms of their ultimate impact on safe shutdown system equipment.

Consider the following criteria when selecting cables that impact safe shutdown equipment:

3.3.1.1 The list of cables whose failure could impact the operation of a piece of safe shutdown equipment includes more than those cables connected to the equipment. The relationship between cable and affected equipment is based on a review of the electrical or elementary wiring diagrams. To assure that all cables that could affect the operation of the safe shutdown equipment are identified, investigate the power, control, instrumentation, interlock, and equipment status indication cables related to the equipment. Review additional schematic diagrams to identify additional cables for interlocked circuits that also need to be considered for their impact on the ability of the equipment to operate as required in support of post-fire safe shutdown. As an option, consider applying the screening criteria from Section 3.5 as a part of this section. For an example of this see Section 3.3.1.4.

3.3.1.2 In cases where the failure (including spurious operations) of a single cable could impact more than one piece of safe shutdown equipment, include the cable with each piece of safe shutdown equipment.

3.3.1.3 Electrical devices such as relays, switches and signal resistor units are considered to be acceptable isolation devices. In the case of instrument loops and electrical metering circuits, review the isolation capabilities of the devices in the loop to determine that an acceptable isolation device has been installed at each point where the loop must

be isolated so that a fault would not impact the performance of the safe shutdown instrument function. Refer to Section 3.5 for the types of faults that should be considered when evaluating the acceptability of the isolation device being credited.

- 3.3.1.4 Screen out cables for circuits that do not impact the safe shutdown function of a component (i.e., annunciator circuits, space heater circuits and computer input circuits) unless some reliance on these circuits is necessary. However, they must be isolated from the component's control scheme in such a way that a cable fault would not impact the performance of the circuit. Refer to Section 3.5 for the types of faults that should be considered when evaluating the acceptability of the isolation device being credited.
- 3.3.1.5 For each circuit requiring power to perform its safe shutdown function, identify the cable supplying power to each safe shutdown and/or required interlock component. Initially, identify only the power cables from the immediate upstream power source for these interlocked circuits and components (i.e., the closest power supply, load center or motor control center). Review further the electrical distribution system to capture the remaining equipment from the electrical power distribution system necessary to support delivery of power from either the offsite power source or the emergency diesel generators (i.e., onsite power source) to the safe shutdown equipment. Add this equipment to the safe shutdown equipment list. Evaluate the power cables for this additional equipment for associated circuits concerns.
- 3.3.1.6 The automatic initiation logics for the credited post-fire safe shutdown systems are generally not required to support safe shutdown. Typically, each system can be controlled manually by operator actuation in the main control room or emergency control station. If operator actions outside the MCR are necessary, those actions must conform to the regulatory requirements on operator manual actions (See Appendix E). However, if not protected from the effects of fire, the fire-induced failure of automatic initiation logic circuits should be considered for its potential to adversely affect any post-fire safe shutdown system function.
- 3.3.1.7 Cabling for the electrical distribution system is a concern for those breakers that feed associated circuits and are not fully coordinated with upstream breakers. With respect to electrical distribution cabling, two types of cable associations exist. For safe shutdown considerations, the direct power feed to a primary safe shutdown component is associated with the primary component. For example, the power feed to a pump is necessary to support the pump. Similarly, the power feed from the load center to an MCC supports the MCC. However, for cases where sufficient branch-circuit coordination is not provided, the

same cables discussed above would also support the power supply. For example, the power feed to the pump discussed above would support the bus from which it is fed because, for the case of a common power source analysis, the concern is the loss of the upstream power source and not the connected load. Similarly, the cable feeding the MCC from the load center would also be necessary to support the load center.

3.3.2 Associated Circuit Cables

Appendix R, Section III.G.2, requires that separation features be provided for equipment and cables, including associated nonsafety circuits that could prevent operation or cause maloperation due to hot shorts, open circuits, or shorts to ground, of redundant trains of systems necessary to achieve hot shutdown. The three types of associated circuits were identified in Reference 6.1.5 and further clarified in a NRC memorandum dated March 22, 1982 from R. Mattson to D. Eisenhut. Reference 6.1.6. They are as follows:

- Spurious actuations
- Common power source
- Common enclosure.

Cables Whose Failure May Cause Spurious Operations

Safe shutdown system spurious operation concerns can result from fire damage to a cable whose failure could cause the spurious operation/mal-operation of equipment whose operation could affect safe shutdown. These cables are identified in Section 3.3.3 together with the remaining safe shutdown cables required to support control and operation of the equipment. The circuit failure criteria contained in Appendix B is to be used with the Plant Unique List of MSOs developed through the Resolution Methodology contained in Chapter 4.

Common Power Source Cables

The concern for the common power source associated circuits is the loss of a safe shutdown power source due to inadequate breaker/fuse coordination. In the case of a fire-induced cable failure on a non-safe shutdown load circuit supplied from the safe shutdown power source, a lack of coordination between the upstream supply breaker/fuse feeding the safe shutdown power source and the load breaker/fuse supplying the non-safe shutdown faulted circuit can result in loss of the safe shutdown bus. This would result in the loss of power to the safe shutdown equipment supplied from that power source preventing the safe shutdown equipment from performing its required safe shutdown function. Identify these cables together with the remaining safe shutdown cables required to support control and operation of the equipment. Refer to Section 3.5.2.4 for an acceptable methodology for analyzing the impact of these cables on post-fire safe shutdown.

Common Enclosure Cables

The concern with common enclosure associated circuits is fire damage to a cable whose failure could propagate to other safe shutdown cables in the same enclosure either because the circuit is not properly protected by an isolation device (breaker/fuse) such that a fire-induced fault could result in ignition along its length, or by the fire propagating along the cable and into an adjacent fire area. This fire spread to an adjacent fire area could impact safe shutdown equipment in that fire area, thereby resulting in a condition that exceeds the criteria and assumptions of this methodology (i.e., multiple fires). Refer to Section 3.5.2.5 for an acceptable methodology for analyzing the impact of these cables on post-fire safe shutdown.

3.3.3 Methodology for Cable Selection and Location

Refer to Figure 3-4 for a flowchart illustrating the various steps involved in selecting the cables necessary for performing a post-fire safe shutdown analysis.

Use the following methodology to define the cables required for safe shutdown including cables that may cause associated circuits concerns for a post-fire safe shutdown analysis:

3.3.3.1 Identify Circuits Required for the Operation of the Safe Shutdown Equipment

For each piece of safe shutdown equipment defined in section 3.2, review the appropriate electrical diagrams including the following documentation to identify the circuits (power, control, instrumentation) required for operation or whose failure may impact the operation of each piece of equipment:

- Single-line electrical diagrams
- Elementary wiring diagrams
- Electrical connection diagrams
- Instrument loop diagrams.

For electrical power distribution equipment such as power supplies, identify any circuits whose failure may cause a coordination concern for the bus under evaluation.

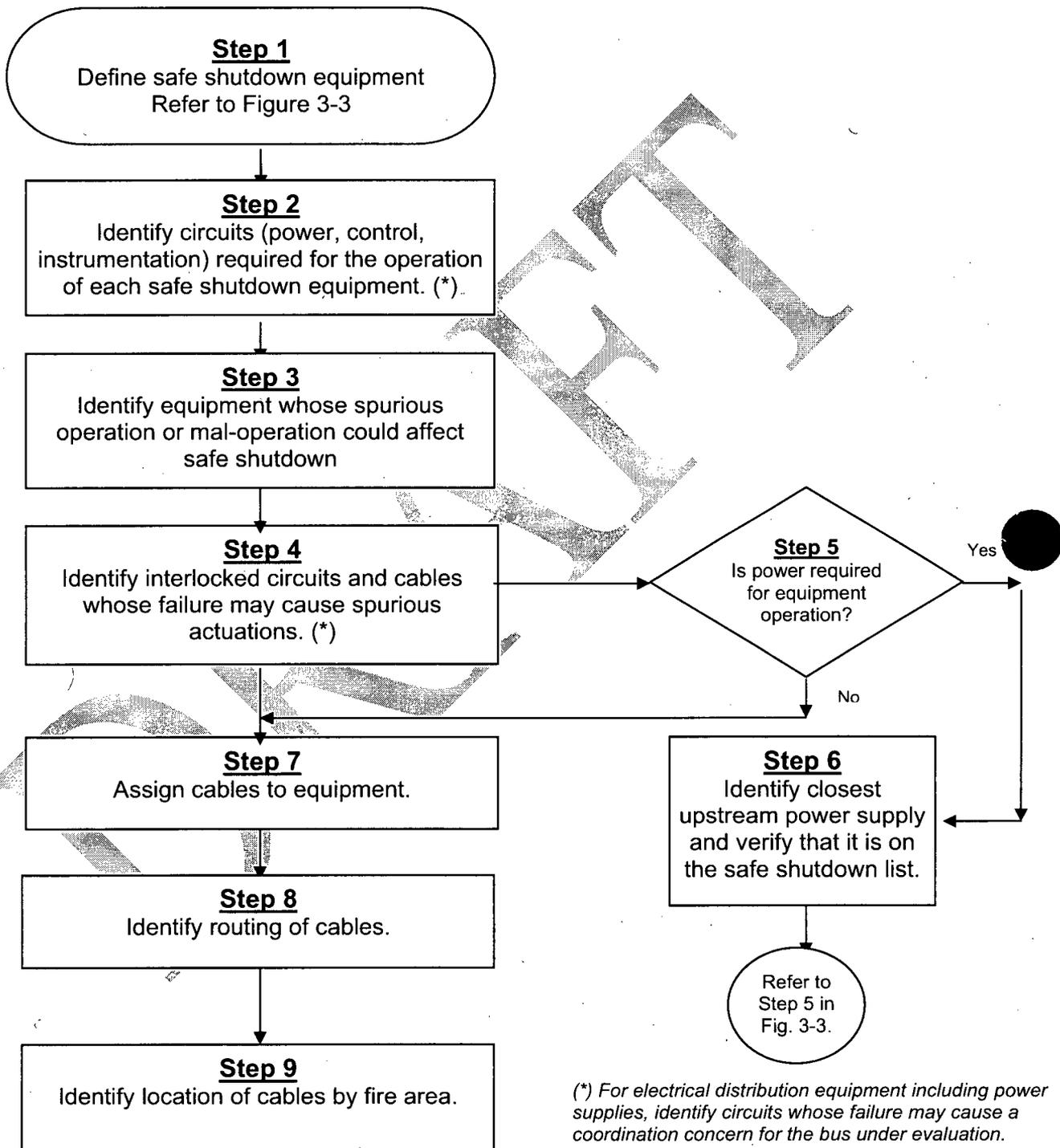
If power is required for the equipment, include the closest upstream power distribution source on the safe shutdown equipment list. Through the iterative process described in Figures 3-2 and 3-3, include the additional upstream power sources up to either the offsite or the emergency power source.

3.3.3.2 Identify Interlocked Circuits and Cables Whose Spurious Operation or Mal-operation Could Affect Shutdown

In reviewing each control circuit, investigate interlocks that may lead to additional circuit schemes, cables and equipment. Assign to the equipment any cables for interlocked circuits that can affect the equipment.

DRAFT

Figure 3-4 Safe Shutdown Cable Selection



While investigating the interlocked circuits, additional equipment or power sources may be discovered. Include these interlocked equipment or power sources in the safe shutdown equipment list (refer to Figure 3-3) if they can impact the operation of the equipment under consideration.

3.3.3.3 Assign Cables to the Safe Shutdown Equipment

Given the criteria/assumptions defined in Section 3.3.1, identify the cables required to operate or that may result in maloperation of each piece of safe shutdown equipment.

Tabulate the list of cables potentially affecting each piece of equipment in a relational database including the respective drawing numbers, their revision and any interlocks that are investigated to determine their impact on the operation of the equipment. In certain cases, the same cable may support multiple pieces of equipment. Relate the cables to each piece of equipment, but not necessarily to each supporting secondary component.

If adequate coordination does not exist for a particular circuit, relate the power cable to the power source. This will ensure that the power source is identified as affected equipment in the fire areas where the cable may be damaged.

3.3.3.4 Identify Routing of Cables

Identify the routing for each cable including all raceway and cable endpoints. Typically, this information is obtained from joining the list of safe shutdown cables with an existing cable and raceway database.

3.3.3.5 Identify Location of Raceway and Cables by Fire Area

Identify the fire area location of each raceway and cable endpoint identified in the previous step and join this information with the cable routing data. In addition, identify the location of field-routed cable by fire area. This produces a database containing all of the cables requiring fire area analysis, their locations by fire area, and their raceway.

3.4 FIRE AREA ASSESSMENT AND COMPLIANCE STRATEGIES

By determining the location of each component and cable by fire area and using the cable to equipment relationships described above, the affected safe shutdown equipment in each fire area can be determined. Using the list of affected equipment in each fire area, the impacts to safe shutdown systems, paths and functions can be determined. Based on an assessment of the number and types of these impacts, the required safe shutdown path for each fire area can be determined. The specific impacts to the selected safe shutdown path can be evaluated using the circuit analysis and evaluation criteria contained in Section 3.5 of this document. For MSOs the Resolution Methodology outlined in Section 4, Section 5, Appendix B and Appendix G should be applied.

Having identified all impacts to the required safe shutdown path in a particular fire area, this section provides guidance on the techniques available for individually mitigating the effects of each of the potential impacts.

3.4.1 Criteria/Assumptions

The following criteria and assumptions apply when performing fire area compliance assessment to mitigate the consequences of the circuit failures identified in the previous sections for the required safe shutdown path in each fire area.

- 3.4.1.1 Assume only one fire in any single fire area at a time.
- 3.4.1.2 Assume that the fire may affect all unprotected cables and equipment within the fire area. This assumes that neither the fire size nor the fire intensity is known. This is conservative and bounds the exposure fire that is required by the regulation.
- 3.4.1.3 Address all cable and equipment impacts affecting the required safe shutdown path in the fire area. All potential impacts within the fire area must be addressed. The focus of this section is to determine and assess the potential impacts to the required safe shutdown path selected for achieving post-fire safe shutdown and to assure that the required safe shutdown path for a given fire area is properly protected.
- 3.4.1.4 Use operator manual actions where appropriate to achieve and maintain post-fire safe shutdown conditions in accordance with NRC requirements.
- 3.4.1.5 Where appropriate to achieve and maintain cold shutdown within 72 hours, use repairs to equipment required in support of post-fire shutdown.
- 3.4.1.6 Appendix R compliance requires that one train of systems necessary to achieve and maintain hot shutdown conditions from either the control room or emergency control station(s) is free of fire damage (III.G.1.a). When cables or equipment, including associated circuits, are within the same fire area outside primary containment and separation does not already exist, provide one of the following means of separation for the required safe shutdown path(s):
 - Separation of cables and equipment and associated nonsafety circuits of redundant trains within the same fire area by a fire barrier having a 3-hour rating (III.G.2.a)
 - Separation of cables and equipment and associated nonsafety circuits of redundant trains within the same fire area by a horizontal distance of more than 20 feet with no intervening

combustibles or fire hazards. In addition, fire detectors and an automatic fire suppression system shall be installed in the fire area (III.G.2.b).

- Enclosure of cable and equipment and associated non-safety circuits of one redundant train within a fire area in a fire barrier having a one-hour rating. In addition, fire detectors and an automatic fire suppression system shall be installed in the fire area (III.G.2.c).

For fire areas inside non-inerted containments, the following additional options are also available:

- Separation of cables and equipment and associated nonsafety circuits of redundant trains by a horizontal distance of more than 20 feet with no intervening combustibles or fire hazards (III.G.2.d);
- Installation of fire detectors and an automatic fire suppression system in the fire area (III.G.2.e); or
- Separation of cables and equipment and associated non-safety circuits of redundant trains by a noncombustible radiant energy shield (III.G.2.f).

Use exemptions, deviations and licensing change processes to satisfy the requirements mentioned above and to demonstrate equivalency depending upon the plant's license requirements.

3.4.1.7 Consider selecting other equipment that can perform the same safe shutdown function as the impacted equipment. In addressing this situation, each equipment impact, including spurious operation, is to be addressed in accordance with regulatory requirements and the NPP's current licensing basis.

3.4.1.8 Consider the effects of the fire on the density of the fluid in instrument tubing and any subsequent effects on instrument readings or signals associated with the protected safe shutdown path in evaluating post-fire safe shutdown capability. This can be done systematically or via procedures such as Emergency Operating Procedures.

3.4.2 Methodology for Fire Area Assessment

Refer to Figure 3-5 for a flowchart illustrating the various steps involved in performing a fire area assessment.

Use the following methodology to assess the impact to safe shutdown and demonstrate Appendix R compliance:

3.4.2.1 Identify the Affected Equipment by Fire Area

Identify the safe shutdown cables, equipment and systems located in each fire area that may be potentially damaged by the fire. Provide this information in a report format. The report may be sorted by fire area and by system in order to understand the impact to each safe shutdown path within each fire area (see Attachment 5 for an example of an Affected Equipment Report).

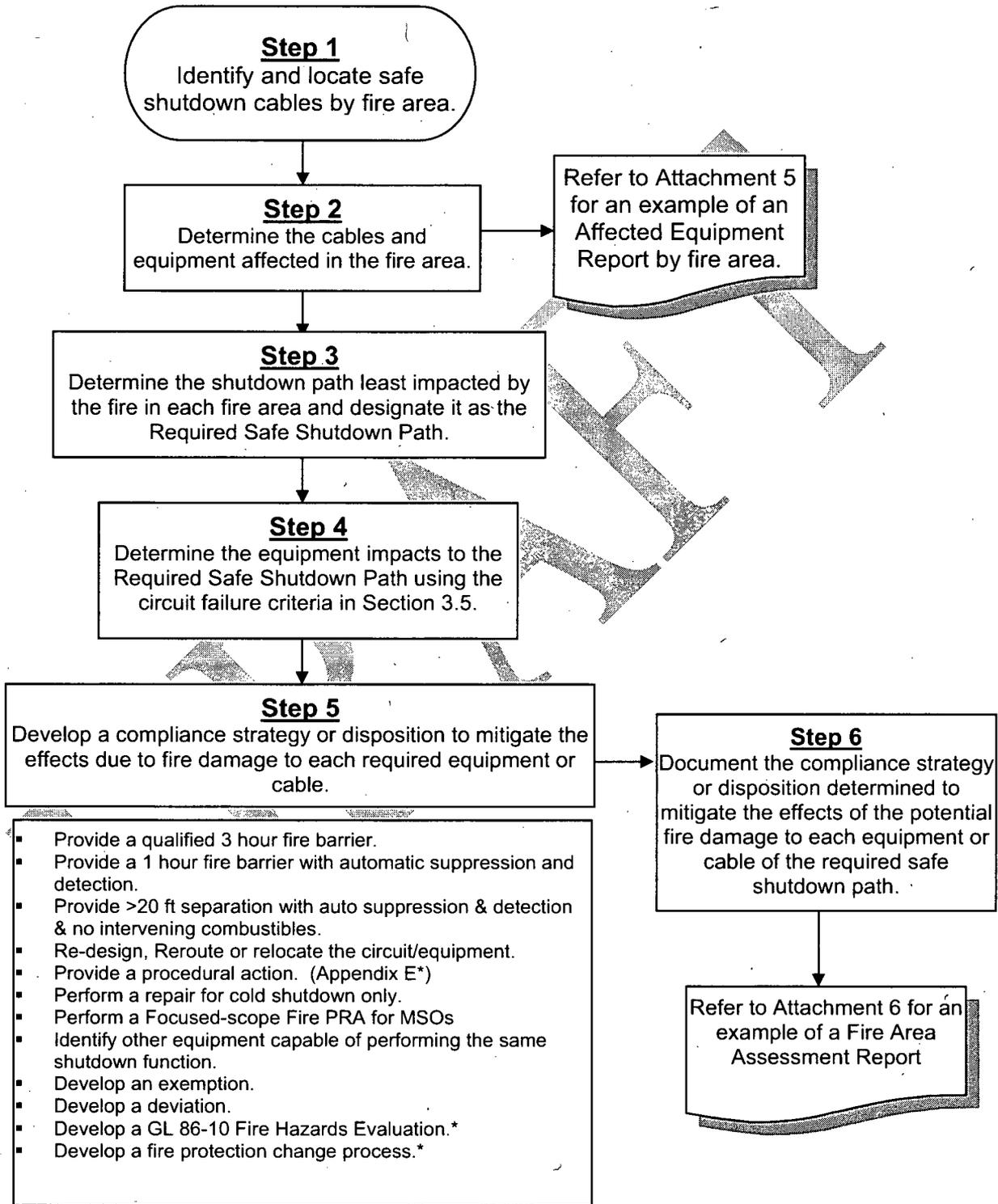
3.4.2.2 Determine the Shutdown Paths Least Impacted By a Fire in Each Fire Area

Based on a review of the systems, equipment and cables within each fire area, determine which shutdown paths are either unaffected or least impacted by a postulated fire within the fire area. Typically, the safe shutdown path with the least number of cables and equipment in the fire area would be selected as the required safe shutdown path. Consider the circuit failure criteria and the possible mitigating strategies, however, in selecting the required safe shutdown path in a particular fire area. Review support systems as a part of this assessment since their availability will be important to the ability to achieve and maintain safe shutdown. For example, impacts to the electric power distribution system for a particular safe shutdown path could present a major impediment to using a particular path for safe shutdown. By identifying this early in the assessment process, an unnecessary amount of time is not spent assessing impacts to the frontline systems that will require this power to support their operation.

Based on an assessment as described above, designate the required safe shutdown path(s) for the fire area. Identify all equipment not in the safe shutdown path whose spurious operation or mal-operation could affect the shutdown function. Include these cables in the shutdown function list. For each of the safe shutdown cables (located in the fire area) that are part of the required safe shutdown path in the fire area, perform an evaluation to determine the impact of a fire-induced cable failure on the corresponding safe shutdown equipment and, ultimately, on the required safe shutdown path.

When evaluating the safe shutdown mode for a particular piece of equipment, it is important to consider the equipment's position for the specific safe shutdown scenario for the full duration of the shutdown scenario. It is possible for a piece of equipment to be in two different states depending on the shutdown scenario or the stage of shutdown within a particular shutdown scenario. Document information related to the normal and shutdown positions of equipment on the safe shutdown equipment list.

**Figure 3-5
 Fire Area Assessment Flowchart**



* Seek regulatory approval where necessary

3.4.2.3 Determine Safe Shutdown Equipment Impacts

Using the circuit analysis and evaluation criteria contained in Section 3.5 of this document, determine the equipment that can impact safe shutdown and that can potentially be impacted by a fire in the fire area, and what those possible impacts are.

3.4.2.4 Develop a Compliance Strategy or Disposition to Mitigate the Effects Due to Fire Damage to Each Required Component or Cable

The available deterministic methods for mitigating the effects of circuit failures are summarized as follows (see Figure 1-2):

- Provide a qualified 3-fire rated barrier.
- Provide a 1-hour fire rated barrier with automatic suppression and detection.
- Provide separation of 20 feet or greater with automatic suppression and detection and demonstrate that there are no intervening combustibles within the 20 foot separation distance.
- Redesign, Reroute or relocate the circuit/equipment, or perform other modifications to resolve vulnerability.
- Provide a procedural action in accordance with Appendix E.
- Perform a cold shutdown repair in accordance with regulatory requirements.
- Perform a Focused-scope Fire PRA using the methods of Chapter 5 for MSOs.
- Identify other equipment not affected by the fire capable of performing the same safe shutdown function.
- Develop exemptions, deviations, Generic Letter 86-10 evaluation or fire protection design change evaluations with a licensing change process.

Additional options are available for non-inerted containments as described in 10 CFR 50 Appendix R section III.G.2.d, e and f.

3.4.2.5 Document the Compliance Strategy or Disposition Determined to Mitigate the Effects Due to Fire Damage to Each Required Component or Cable

Assign compliance strategy statements or codes to components or cables to identify the justification or mitigating actions proposed for achieving safe shutdown. The justification should address the cumulative effect of the actions relied upon by the licensee to mitigate a fire in the area. Provide each piece of safe shutdown equipment, equipment not in the path whose spurious operation or mal-operation could affect safe shutdown, and/or cable for the required safe shutdown path with a specific compliance strategy or disposition. Refer to Attachment 6 for an example of a Fire Area Assessment Report documenting each cable disposition.

3.5 CIRCUIT ANALYSIS AND EVALUATION

This section on circuit analysis provides information on the potential impact of fire on circuits used to monitor, control and power safe shutdown equipment. Applying the circuit analysis criteria will lead to an understanding of how fire damage to the cables may affect the ability to achieve and maintain post-fire safe shutdown in a particular fire area. This section should be used in conjunction with Section 3.4, to evaluate the potential fire-induced impacts that require mitigation.

Appendix R Section III.G.2 identifies the fire-induced circuit failure types that are to be evaluated for impact from exposure fires on safe shutdown equipment. Section III.G.2 of Appendix R requires consideration of hot shorts, shorts-to-ground and open circuits.

3.5.1 Criteria/Assumptions

Apply the following criteria/assumptions when performing fire-induced circuit failure evaluations.

3.5.1.1 Consider the following circuit failure types on each conductor of each unprotected safe shutdown cable to determine the potential impact of a fire on the safe shutdown equipment associated with that conductor.

- A hot short may result from a fire-induced insulation breakdown between conductors of the same cable, a different cable or from some other external source resulting in a compatible but undesired impressed voltage or signal on a specific conductor. A hot short may cause a spurious operation of safe shutdown equipment.
- An open circuit may result from a fire-induced break in a conductor resulting in the loss of circuit continuity. An open circuit may prevent the ability to control or power the affected equipment. An open circuit may also result in a change of state for normally energized equipment. (e.g. [for BWRs] loss of power to the Main Steam Isolation Valve (MSIV) solenoid valves due to an open circuit will result in the closure of the MSIVs).
- A short-to-ground may result from a fire-induced breakdown of a cable insulation system, resulting in the potential on the conductor being applied to ground potential. A short-to-ground may have all of the same effects as an open circuit and, in addition, a short-to-ground may also cause an impact to the control circuit or power train of which it is a part.

Consider the three types of circuit failures identified above to occur individually on each conductor of each safe shutdown cable on the required safe shutdown path in the fire area.

For the plant Specific List of MSOs use the circuit failure criteria outlined in Appendix B.

3.5.1.2 Assume that circuit contacts are positioned (i.e., open or closed) consistent with the normal mode/position of the safe shutdown equipment as shown on the schematic drawings. The analyst must consider the position of the safe shutdown equipment for each specific shutdown scenario when determining the impact that fire damage to a particular circuit may have on the operation of the safe shutdown equipment.

3.5.1.3 Assume that circuit failure types resulting in spurious operations exist until action has been taken to isolate the given circuit from the fire area, or other actions have been taken to negate the effects of circuit failure that is causing the spurious operation. The fire is not assumed to eventually clear the circuit fault. For MSOs the criteria in Appendix B of hot shorts clearing and going to ground within 20 minutes may be used.

3.5.1.4 When both trains are in the same fire area outside of primary containment, all cables that do not meet the separation requirements of Section III.G.2 are assumed to fail in their worst case configuration.

3.5.2 Types of Circuit Failures

Appendix R requires that nuclear power plants must be designed to prevent exposure fires from defeating the ability to achieve and maintain post-fire safe shutdown. Fire damage to circuits that provide control and power to equipment on the required safe shutdown path and any other equipment whose spurious operation/mal-operation could affect shutdown in each fire area must be evaluated for the effects of a fire in that fire area. Only one fire at a time is assumed to occur. The extent of fire damage is assumed to be limited by the boundaries of the fire area. Given this set of conditions, it must be assured that one redundant train of equipment capable of achieving hot shutdown is free of fire damage for fires in every plant location. To provide this assurance, Appendix R requires that equipment and circuits required for safe shutdown be free of fire damage and that these circuits be designed for the fire-induced effects of a hot short, short-to-ground, or an open circuit. With respect to the electrical distribution system, the issue of breaker coordination must also be addressed.

This section will discuss specific examples of each of the following types of circuit failures:

- Open circuit
- Short-to-ground
- Hot short.

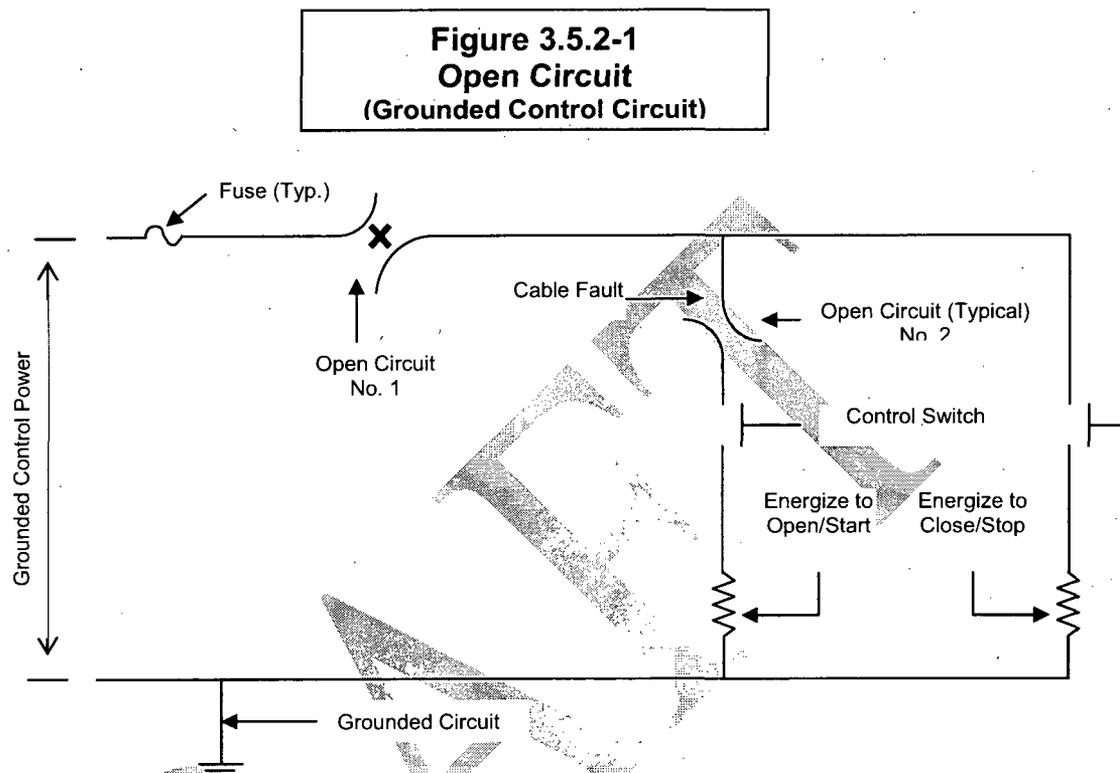
Also, refer to Appendix B for the circuit failure criteria to be applied in assessing the impact of the Plant Specific List of MSOs on post-fire safe shutdown.

3.5.2.1 Circuit Failures Due to an Open Circuit

This section provides guidance for addressing the effects of an open circuit for safe shutdown equipment. An open circuit is a fire-induced break in a conductor resulting in the loss of circuit continuity. An open circuit will typically prevent the ability to control or power the affected equipment. An open circuit can also result in a change of state for normally energized equipment. For example, a loss of power to the main steam isolation valve (MSIV) solenoid valves [for BWRs] due to an open circuit will result in the closure of the MSIV.

- Loss of electrical continuity may occur within a conductor resulting in de-energizing the circuit and causing a loss of power to, or control of, the required safe shutdown equipment.
- In selected cases, a loss of electrical continuity may result in loss of power to an interlocked relay or other device. This loss of power may change the state of the equipment. Evaluate this to determine if equipment fails safe.
- Open circuit on a high voltage (e.g., 4.16 kV) ammeter current transformer (CT) circuit may result in secondary damage.

Figure 3.5.2-1 shows an open circuit on a grounded control circuit.



Open circuit No. 1:

An open circuit at location No. 1 will prevent operation of the subject equipment.

Open circuit No. 2:

An open circuit at location No. 2 will prevent opening/starting of the subject equipment, but will not impact the ability to close/stop the equipment.

3.5.2.2 Circuit Failures Due to a Short-to-Ground

This section provides guidance for addressing the effects of a short-to-ground on circuits for safe shutdown equipment. A short-to-ground is a fire-induced breakdown of a cable insulation system resulting in the potential on the conductor being applied to ground potential. A short-to-ground can cause a loss of power to or control of required safe shutdown equipment. In addition, a short-to-ground may affect other equipment in the electrical power distribution system in the cases where proper coordination does not exist.

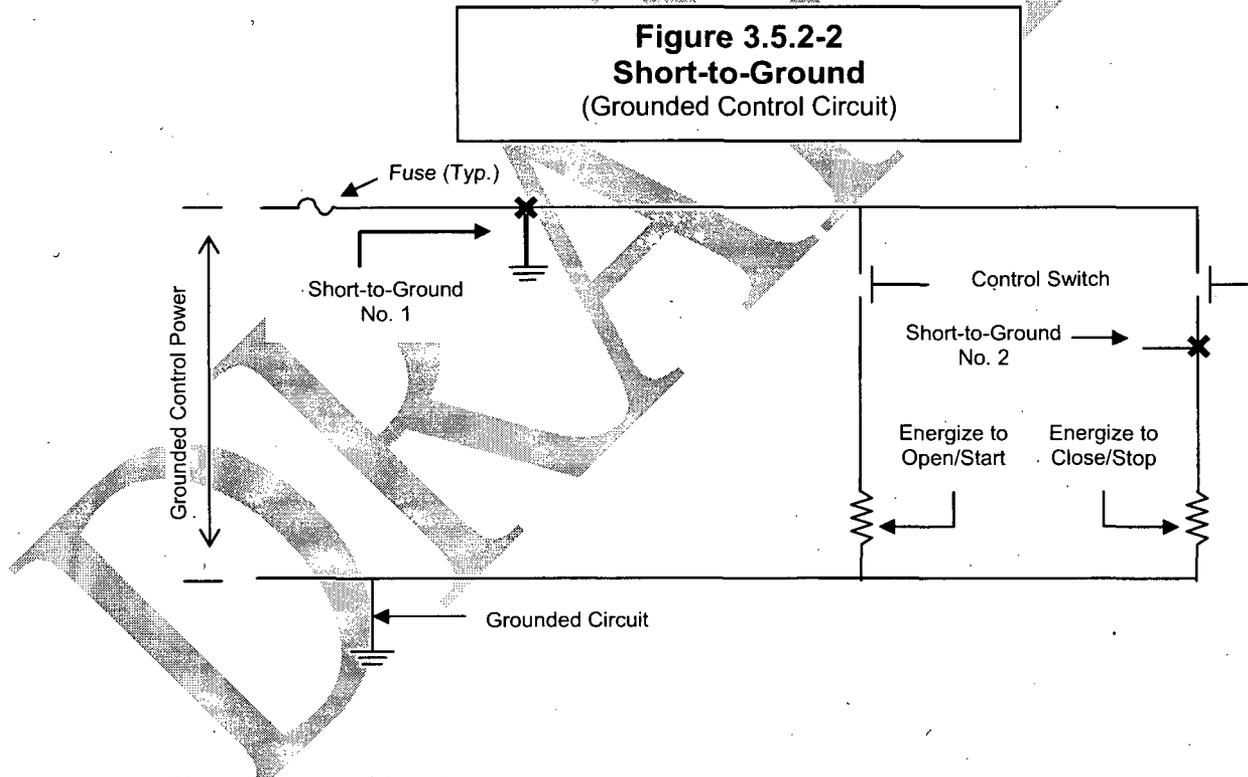
Consider the following consequences in the post-fire safe shutdown analysis when determining the effects of circuit failures related to shorts-to-ground:

- A short to ground in a power or a control circuit may result in tripping one or more isolation devices (i.e. breaker/fuse) and causing a loss of power to or control of required safe shutdown equipment.
- In the case of certain energized equipment such as HVAC dampers, a loss of control power may result in loss of power to an interlocked relay or other device that may cause one or more spurious operations.

Short-to-Ground on Grounded Circuits

Typically, in the case of a grounded circuit, a short-to-ground on any part of the circuit would present a concern for tripping the circuit isolation device thereby causing a loss of control power.

Figure 3.5.2-2 illustrates how a short-to-ground fault may impact a grounded circuit.



Short-to-ground No. 1:

A short-to-ground at location No. 1 will result in the control power fuse blowing and a loss of power to the control circuit. This will result in an inability to operate the equipment using the control switch. Depending on the coordination characteristics between the protective device on this circuit and upstream circuits, the power supply to other circuits could be affected.

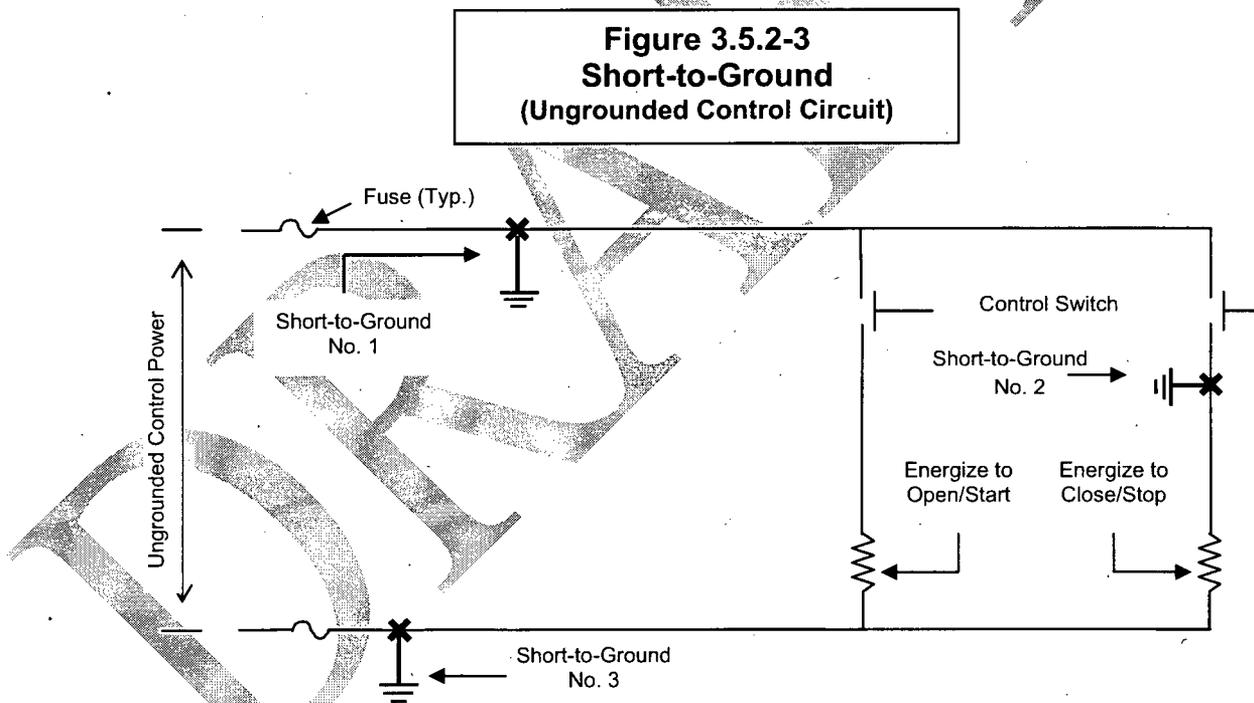
Short-to-ground No. 2:

A short-to-ground at location No. 2 will have no effect on the circuit until the close/stop control switch is closed. Should this occur, the effect would be identical to that for the short-to-ground at location No. 1 described above. Should the open/start control switch be closed prior to closing the close/stop control switch, the equipment will still be able to be opened/started.

Short-to-Ground on Ungrounded Circuits

In the case of an ungrounded circuit, postulating only a single short-to-ground on any part of the circuit may not result in tripping the circuit isolation device. Another short-to-ground on the circuit or another circuit from the same source would need to exist to cause a loss of control power to the circuit.

Figure 3.5.2-3 illustrates how a short to ground fault may impact an ungrounded circuit.



Short-to-ground No. 1:

A short-to-ground at location No. 1 will result in the control power fuse blowing and a loss of power to the control circuit if short-to-ground No. 3 also exists either within the same circuit or on any other circuit fed from the same power source. This will result in an inability to operate the equipment using the control switch. Depending on the coordination characteristics between the protective device on this circuit and upstream circuits, the power supply to other circuits could be affected.

Short-to-ground No. 2:

A short-to-ground at location No. 2 will have no effect on the circuit until the close/stop control switch is closed. Should this occur, the effect would be identical to that for the short-to-ground at location No. 1 described above. Should the open/start control switch be closed prior to closing the close/stop control switch, the equipment will still be able to be opened/started.

3.5.2.3 Circuit Failures Due to a Hot Short

This section provides guidance for analyzing the effects of a hot short on circuits for required safe shutdown equipment. A hot short is defined as a fire-induced insulation breakdown between conductors of the same cable, a different cable or some other external source resulting in an undesired impressed voltage on a specific conductor. The potential effect of the undesired impressed voltage would be to cause equipment to operate or fail to operate in an undesired manner.

Consider the following specific circuit failures related to hot shorts as part of the post-fire safe shutdown analysis:

- A hot short between an energized conductor and a de-energized conductor within the same cable may cause a spurious operation of equipment. The spuriously operated device (e.g., relay) may be interlocked with another circuit that causes the spurious operation of other equipment. This type of hot short is called an intracable hot short (also known as conductor-to-conductor hot short or an internal hot short).
- A hot short between any external energized source such as an energized conductor from another cable and a de-energized conductor may also cause a spurious operation of equipment. This is called an intercable hot short (also known as cable-to-cable hot short/external hot short).

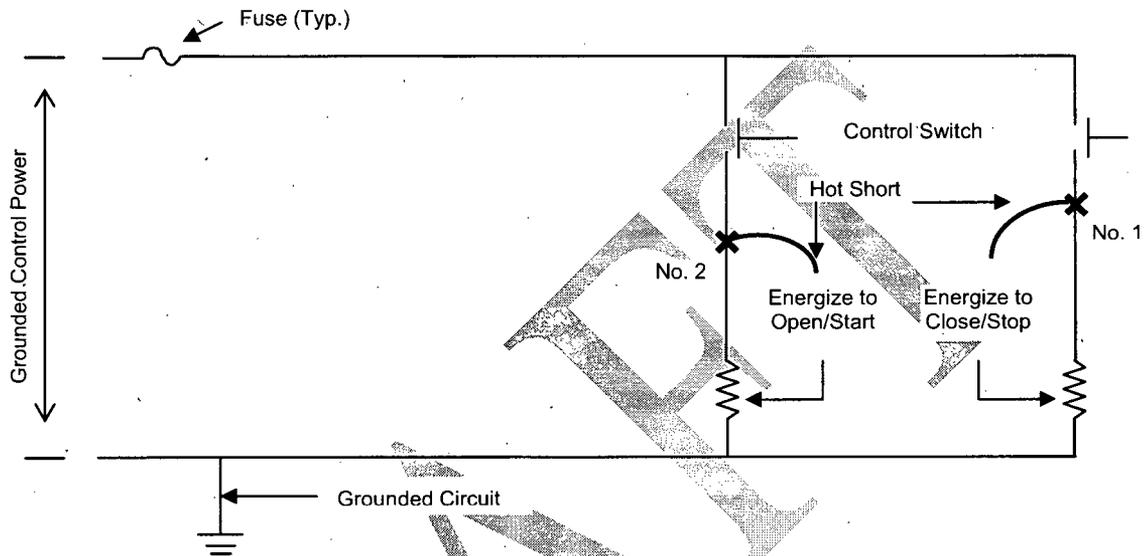
A Hot Short on Grounded Circuits

A short-to-ground is another failure mode for a grounded control circuit. A short-to-ground as described above would result in de-energizing the circuit. This would further reduce the likelihood for the circuit to change the state of the equipment either from a control switch or due to a hot short. Nevertheless, a hot short still needs to be considered. Figure 3.5.2-4 shows a typical grounded control circuit that might be used for a motor-operated valve. However, the protective devices and position indication lights that would normally be included in the control circuit for a motor-operated valve have been omitted, since these devices are not required to understand the concepts being explained in this section. In the discussion provided below, it is assumed that a single fire in a given fire area could cause any one of the hot shorts depicted.

The following discussion describes how to address the impact of these individual cable faults on the operation of the equipment controlled by this circuit.

DRAFT

**Figure 3.5.2-4
Hot Short
(Grounded Control Circuit)**



Hot short No. 1:

A hot short at this location would energize the close relay and result in the undesired closure of a motor-operated valve.

Hot short No. 2:

A hot short at this location would energize the open relay and result in the undesired opening of a motor-operated valve.

A Hot Short on Ungrounded Circuits

In the case of an ungrounded circuit, a single hot short may be sufficient to cause a spurious operation. A single hot short can cause a spurious operation if the hot short comes from a circuit from the positive leg of the same ungrounded source as the affected circuit.

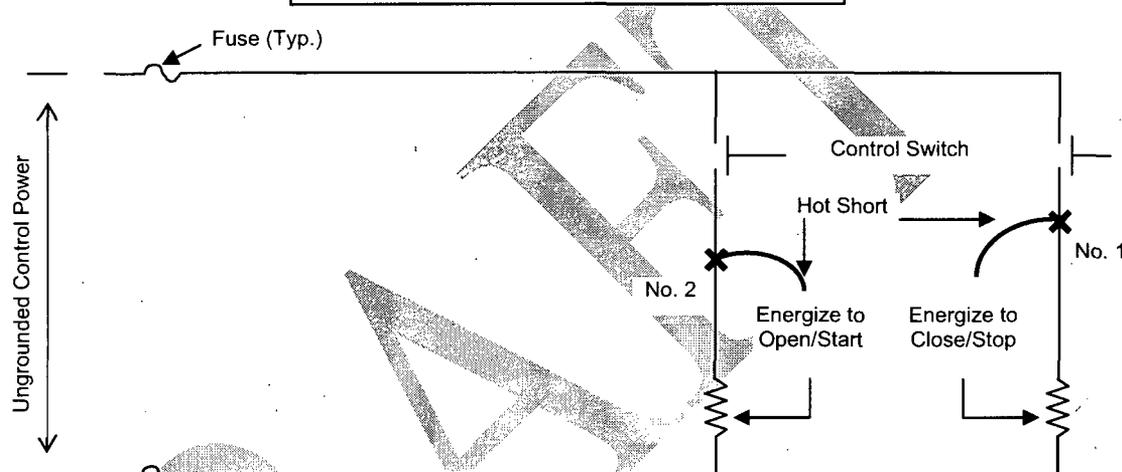
In reviewing each of these cases, the common denominator is that in every case, the conductor in the circuit between the control switch and the start/stop coil must be involved.

Figure 3.5.2-5 depicted below shows a typical ungrounded control circuit that might be used for a motor-operated valve. However, the protective devices and position indication lights that would normally be included in the control circuit

for a motor-operated valve have been omitted, since these devices are not required to understand the concepts being explained in this section.

In the discussion provided below, it is assumed that a single fire in a given fire area could cause any one of the hot shorts depicted. The discussion provided below describes how to address the impact of these cable faults on the operation of the equipment controlled by this circuit.

Figure 3.5.2-5
Hot Short
(Ungrounded Control Circuit)



Hot short No. 1:

A hot short at this location from the same control power source would energize the close relay and result in the undesired closure of a motor operated valve.

Hot short No. 2:

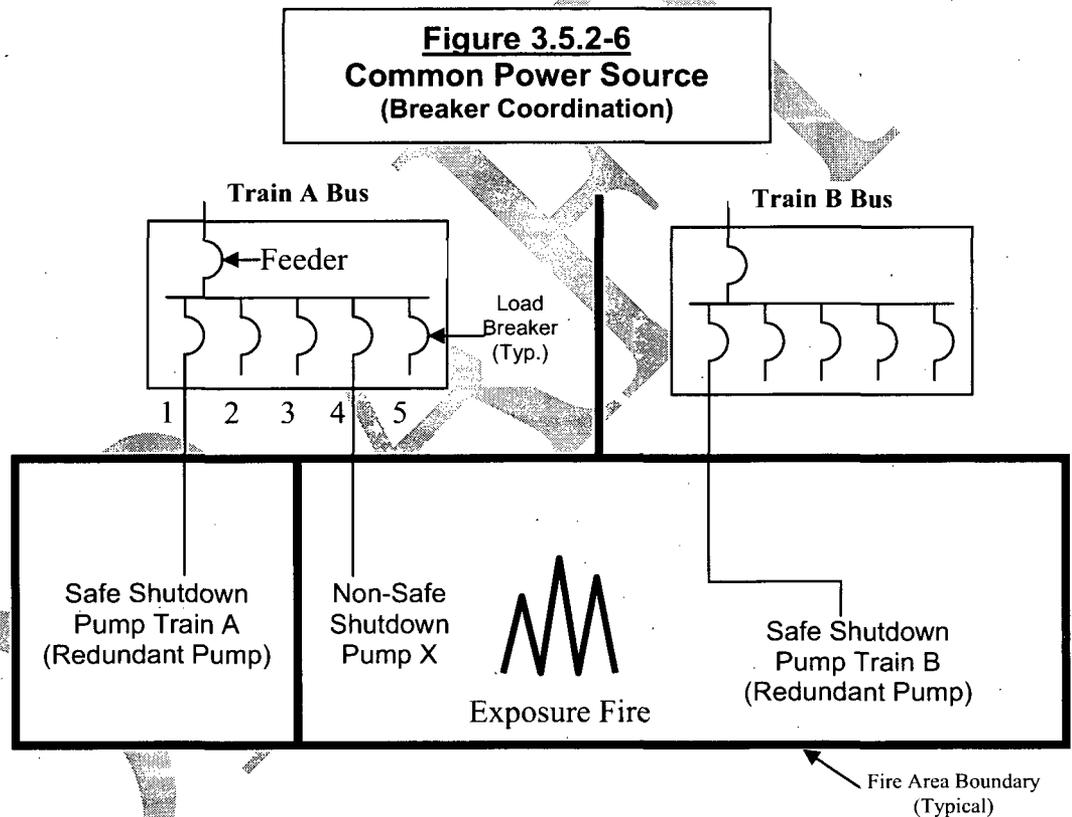
A hot short at this location from the same control power source would energize the open relay and result in the undesired opening of a motor operated valve.

3.5.2.4 Circuit Failures Due to Inadequate Circuit Coordination

The evaluation of associated circuits of a common power source consists of verifying proper coordination between the supply breaker/fuse and the load breakers/fuses for power sources that are required for safe shutdown. The concern is that, for fire damage to a single power cable, lack of coordination between the supply breaker/fuse and the load breakers/fuses can result in the loss of power to a safe shutdown power source that is required to provide power to safe shutdown equipment.

For the example shown in Figure 3.5.2-6, the circuit powered from load breaker 4 supplies power to a non-safe shutdown pump. This circuit is damaged by fire in the same fire area as the circuit providing power to from the Train B bus, which is redundant to the Train A pump.

To assure safe shutdown for a fire in this fire area, the damage to the non-safe shutdown pump powered from load breaker 4 of the Train A bus cannot impact the availability of the Train A pump, which is redundant to the Train B pump. To assure that there is no impact to this Train A pump due to the associated circuits' common power source breaker coordination issue, load breaker 4 must be fully coordinated with the feeder breaker to the Train A bus.



A coordination study should demonstrate the coordination status for each required common power source. For coordination to exist, the time-current curves for the breakers, fuses and/or protective relaying must demonstrate that a fault on the load circuits is isolated before tripping the upstream breaker that supplies the bus. Furthermore, the available short circuit current on the load circuit must be considered to ensure that coordination is demonstrated at the maximum fault level.

The methodology for identifying potential associated circuits of a common power source and evaluating circuit coordination cases of associated circuits on a single circuit fault basis is as follows:

- Identify the power sources required to supply power to safe shutdown equipment.
- For each power source, identify the breaker/fuse ratings, types, trip settings and coordination characteristics for the incoming source breaker supplying the bus and the breakers/fuses feeding the loads supplied by the bus.
- For each power source, demonstrate proper circuit coordination using acceptable industry methods.
- For power sources not properly coordinated, tabulate by fire area the routing of cables whose breaker/fuse is not properly coordinated with the supply breaker/fuse. Evaluate the potential for disabling power to the bus in each of the fire areas in which the associated circuit cables of concern are routed and the power source is required for safe shutdown. Prepare a list of the following information for each fire area:
 - Cables of concern.
 - Affected common power source and its path.
 - Raceway in which the cable is enclosed.
 - Sequence of the raceway in the cable route.
 - Fire zone/area in which the raceway is located.

For fire zones/areas in which the power source is disabled, the effects are mitigated by appropriate methods.

- Develop analyzed safe shutdown circuit dispositions for the associated circuit of concern cables routed in an area of the same path as required by the power source. Evaluate adequate separation based upon the criteria in Appendix R, NRC staff guidance, and plant licensing bases.

3.5.2.5 Circuit Failures Due to Common Enclosure Concerns

The common enclosure associated circuit concern deals with the possibility of causing secondary failures due to fire damage to a circuit either whose isolation device fails to isolate the cable fault or protect the faulted cable from reaching its ignition temperature, or the fire somehow propagates along the cable into adjoining fire areas.

The electrical circuit design for most plants provides proper circuit protection in the form of circuit breakers, fuses and other devices that are designed to isolate cable faults before ignition temperature is reached. Adequate electrical circuit protection and cable sizing are included as part of the original plant electrical design maintained as part of the design change process. Proper protection can be verified by review of as-built drawings and change documentation. Review the fire rated barrier and penetration designs that preclude the propagation of fire from one fire area to the next to demonstrate that adequate measures are in place to alleviate fire propagation concerns.

DRAFT

4 IDENTIFICATION AND TREATMENT OF MULTIPLE SPURIOUS OPERATIONS

4.1 Introduction

The purpose of this section is to provide a methodology for addressing multiple fire-induced circuit failures and multiple spurious operations by individual licensees. This methodology uses identification and analysis techniques similar to methods applied under NEI 04-02 for Risk-Informed Fire Protection, but does not include steps for self-issued change analysis as allowed under NEI 04-02 and NFPA-805.

With NRC acceptance, the methodology presented in this document addresses multiple spurious operations resulting from fire-induced circuit failures for safe shutdown in accordance with the requirements of 10 CFR 50 Appendix R, Sections III.G. 1 and 2.

The basic philosophy behind this method is that the Fire Safe Shutdown Procedures and associated Operator Actions should focus on potentially risk important scenarios. This agrees with the philosophy as described in RIS 2004-03. To satisfy the regulatory requirements for spurious operation, all potential fire-induced spurious operations must be identified and a mitigating action must be developed for each. This mitigating action may be an action taken prior to the start of the fire event that precludes the condition from occurring or as a post fire action that mitigates the effects of the condition prior to it reaching an unrecoverable condition relative to safe shutdown. The corresponding mitigating action for each potential spurious operation must be known and this action must be capable of limiting the potential adverse effects of the spurious operation without reliance on any other equipment that is also potentially susceptible to a spurious operation resulting from a fire in the same fire area.

If the procedures and actions are expanded to include very low risk scenarios, the operator actions would become too complex, resulting in higher expected operator failures for the important scenarios. By placing bounds in the number of scenarios that the procedures address, this results in lower plant risk by ensuring optimal operator response for the potential risk important scenarios.

This philosophy is similar to the development of plant emergency operating procedures, where low risk scenarios are not included in the procedures while potentially high-risk scenarios are addressed.

If a mitigating action is not taken for multiple spurious operations identified using the methods described below, a regulatory submittal (Exemption/Deviation) must be developed. In order to minimize the number of regulatory submittals, the method provided must limit the multiple spurious operations to be consistent with RIS 2004-03 by concentrating identification on circuit failures that have a relatively high likelihood of occurrence.

Additionally, the methodology must provide a process for incorporating new information on spurious operations that are determined to be likely to occur. This may include new information gained from additional fire testing, or as a result of feedback from plants implementing this method (or NFPA 805).

The list of Generic Multiple Spurious Operations developed by the Owner's Groups and required to be considered in conjunction with the information in this appendix are contained in Appendix G. The types of circuit failures and the number of these types of circuit failures that are to be considered in each circuit type are described in Appendix B.

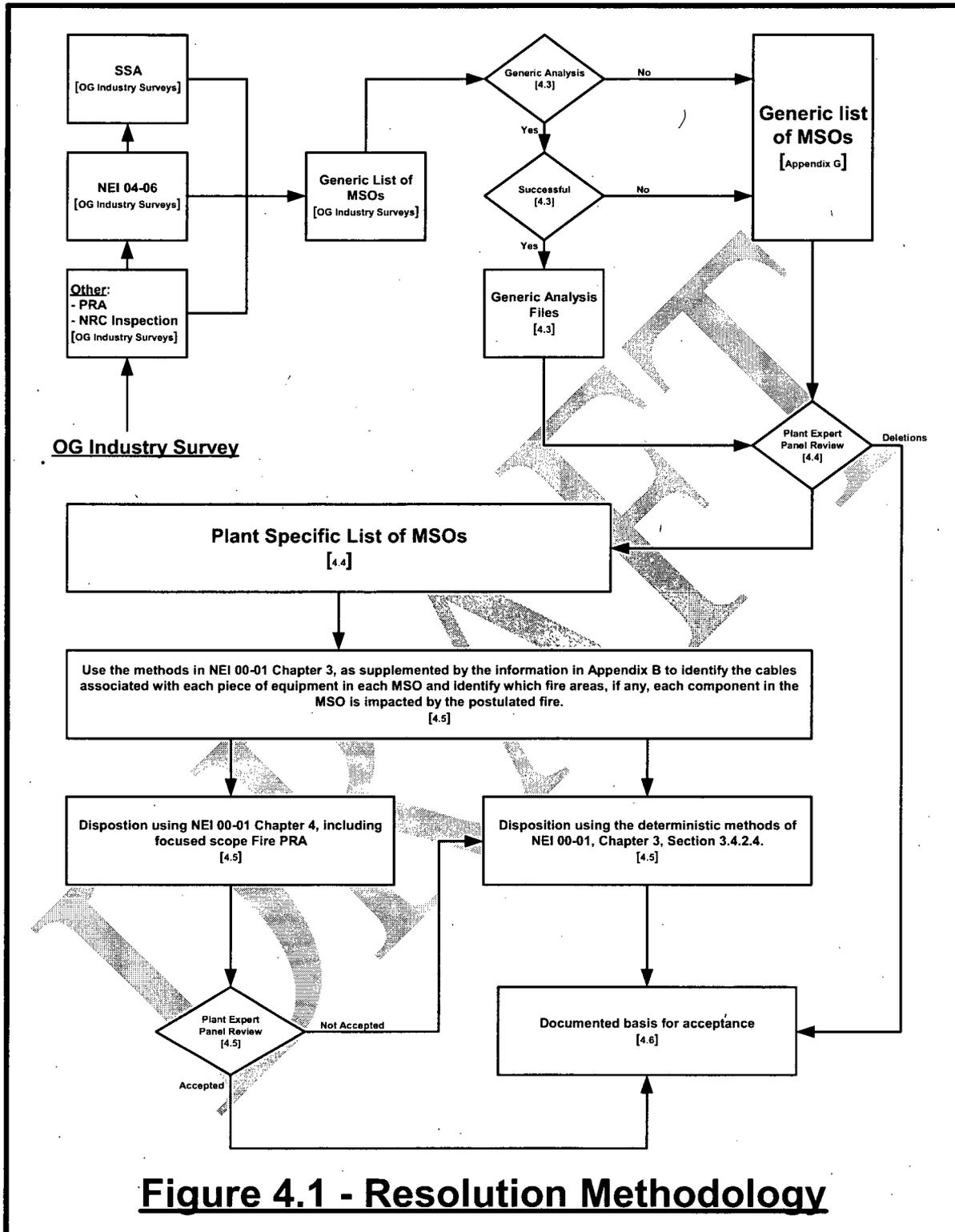
This Appendix is intended to be used to address multiple spurious operations. The affects of single spurious operations due to single fire induced circuit failure is to be addressed using the methods in Chapter 3 of this document. The methods described in this chapter are not to be used for addressing single spurious operations resulting from single fire induced circuit failures.

The process described below, including the generic MSO lists, do not artificially limit the number of spurious operations or hot shorts included in each scenario considered. In some cases, spurious operation of a specific component may require multiple hot shorts. Depending on the type of circuit involved, guidance on the appropriate assumptions to be made relative to this condition are contained in Appendix B. It is also intended that multiple hot shorts being required should not result in any screening of MSOs from consideration prior to the inclusion of the MSO combination in the Safe Shutdown analysis. The multiple hot shorts would be considered when reviewing the hot shorts against the cable criteria in Appendix B or in the PRA calculations.

Spurious operations that are as a result of shorts to ground are considered for this guidance to be the same as spurious operations due to hot shorts. Thus an MSO involving a single spurious operation resulting from hot short and another spurious operation resulting from a short to ground is to be evaluated under the criteria in this section.

4.2 Overview of the MSO Identification and Treatment Process

Figure 4-1 provides an overview of the MSO Identification and Treatment Process. Sections 4.3 to 4.5 below provide a description of each of the steps in the figure.



4.3 Generic List of MSOs

Appendix G provides a list of generic scenarios to consider in a plant specific evaluation for multiple spurious. The generic list of MSOs was developed from an industry survey of all US plants. The survey asked the plants to "Describe the extent to which multiple hot shorts and multiple spurious operations (MSOs) have been addressed for your facility in each of the following areas:"

- 1) Licensing Basis Safe Shutdown Analysis
- 2) Assessments performed for NRC RIS 2004-03 using NEI 04-06
- 3) Evaluations performed as a result of NRC Inspections
- 4) MSO Expert Panel Reviews conducted for Fire PRA or NFPA 805
- 5) Other Instances where MSOs [Combined Equipment Impacts] with potential risk significance been identified (e.g. PRA Analysis Internal Events Model, Fire PRA or other source)

The results of the survey responses were then compiled into a table, and the final list is a composite list of applicable scenarios for each reactor type.

Although not all scenarios for a reactor type are considered applicable to every reactor, the list is provided here as an input to the MSO identification and treatment process.

As can be seen from Figure 4-1, generic Owner's Group analysis can be performed for a given reactor type to disposition generic MSO scenarios. The generically dispositioned scenarios do not need to be included in the plant specific MSO list, provided an individual licensee performs a review of the generic analysis, verifies plant specific parameters bound those critical parameters used in the generic analysis and obtain the concurrence of its plant specific Expert Panel. The method and the critical parameters used for each generic analysis will vary, depending on the MSO. These aspects of the generic analysis are not described further in this document. Refer to each generic analysis for the required information.

4.4 Plant Specific List of MSOs

The method described below provides steps to provide a more accurate and complete list of MSO to be addressed in the plants SSA. This includes steps that both a) screen the generic list of MSO scenarios that are not applicable to a plant and b) add new scenarios that are not listed in the generic scenarios.

4.4.1 Screening (deletion) of Generic MSO Scenarios

The screening of generic MSO scenarios can be performed to remove from consideration scenarios not applicable for a given plant. The screening process involves the review of each scenario in the generic list for applicability and disposition. Scenarios can be screened from the plant specific MSO list, given the following:

- 1) Components identified in the scenario do not exist in the plant, and the scenario is not applicable to similar components or systems, or
- 2) Specific plant design features (see additional comments below) make the scenario either not possible, or does not fail the safe shutdown function.

Additionally, scenarios screened from the plant specific MSO list should be reviewed with the following considerations:

- A) If the design feature that makes the scenario not possible for the plant involves cable routing, circuit design, electrical protection, or other similar design feature, the scenario should not be screened from consideration at this step. Similarly, if an operator action is in place that would prevent the scenario, the scenario should not be screened at this step. The process for these scenarios would be to include the scenario in the MSO list, and to use the design feature as a disposition for the MSO.
- B) Documentation that the scenario does not fail the safe shutdown function should be based on the original Safe Shutdown Analysis assumptions. If specific analysis is performed to show the MSO doesn't fail the function, then the MSO should be included in the plant specific MSO list, and the analysis used in the disposition of the MSO.

For item A) above, the general concept is that if the design feature can possibly change as a result of a design change, the MSO needs to be included in the site specific MSO list. This would ensure that changes to the design would be reviewed against the MSO to ensure the MSO remains not possible as changes are made to the plant over the course of time. For item B) it is intended that whatever is credited in the original SSA, this is carried forward to the MSO list. For example, if there are two injection trains credited for all "A" train fire areas, and an MSO fails only one of the two trains, then the MSO can be screened at this point. In this example, however, the post-fire safe shutdown analysis must be revised to make it clear that only a single injection train is credited in all "A" train fire areas. Another example would be a scenario that drains a water supply tank into the containment sump, and analysis is performed to show the water can be provided from the sump to an injection pump. In this example, if the sump flow path was not in the original SSA, the MSO should not be screened.

Deletions from the Generic List of MSOs is subject to review and concurrence by the Expert Panel. One alternative to the initial screening of generic MSOs is to perform the screening during the expert panel process. This can be done simultaneous to the expert panel exploration of new MSO scenarios, either plant specific or similar to the screened MSO. Documentation of screened MSOs would be required, with performed with the initial screening or by the expert panel.

4.4.2 Plant Specific Additions to MSO list

An Expert Panel Review of the MSO list determines plant Specific Additions. The additions can come from a number of sources, including:

- 1) MSOs resulting from review of the existing Safe Shutdown Analysis
- 2) MSOs resulting from review of the PRA sensitivity runs or results
- 3) MSOs identified by the Expert Panel

The first two inputs are as a result of preparatory work for the Expert Panel review. These preparatory steps and the performance of the Expert Panel process are described in the following sections.

4.4.2.1 Review of Existing Safe Shutdown Analysis

As an input to the Expert Panel process, a list of the existing SSA spurious operations components and scenarios should be developed. Much of the information for this list is already available in SSA supporting documents, but may not be in a form to support external review or an expert panel. This list should provide both a description of the scenario of concern and the disposition of the scenario in the SSA. Manual Operator Actions associated with any disposition should also be documented, including documentation of feasibility criteria (timing, etc.). Key to the documentation are any assumptions made for the SSA, since these assumptions may not be valid for multiple spurious operations scenarios. Both generic and scenario specific assumptions should be documented as an input to the expert panel review.

Scenarios that are dispositioned as not needing operator manual action (or other compliance strategies), due to the presence of additional components down stream of the initial component, should be reviewed by the expert panel in detail. Pre-identification of these scenarios as additions to the MSO list should be performed. For example, if a diversion includes two MOVs, and the first MOV is dispositioned as not a concern due to the presence of the second MOV, then the expert panel should consider spurious operation of both MOVs as a potential multiple spurious operation scenario. Similarly, if a non-post-fire safe shutdown credited pump start is not a concern due to a closed discharge MOV/AOV, then the expert panel should consider the scenario (Pump spuriously starts and valve spuriously opens).

Similarly, for a post-fire safe shutdown credited pump start with a normally open minimum flow valve, then the expert panel should consider the scenario (Pump spuriously starts and the minimum flow valve spuriously closes).

Scenarios where positive operator action is taken where both single and multiple spurious operations are addressed may need to be considered further. The scenario would need to be reviewed for the effect on timing and operator action feasibility to ensure no further review is required. For example, if operator action on a flow path is determined to have 20 minutes prior to reaching an unrecoverable state, but a second spurious can change the timing to 10 minutes, then a review by the expert panel is needed. This timing issue is especially critical for spurious pump operation. For example, for PWR SG overfeed or for the pressurizer going solid, the timing for single pump spurious start/run can be much different that when 2 or 3 pumps start/run, and the credited operator action may not be completed in time for the MSO.

An Example SSA Results Table is provided in Table 1 below. Notice that in the table, there are several examples where Expert Panel Consideration will be required. For example, for MOV-1, the expert panel will need to consider the timing in Table 2 to see if additional spurious operations will result in failure of the feasibility criteria. For MOV-2, the credited disposition is the use of another valve, MOV-3. If the same fire can damage this MOV-3, then a multiple spurious scenario may result. MOV-4 is likely to not be a concern for multiple spurious scenarios, unless it can be involved in scenarios where a hot standby results. In this case, it could affect the timing of an existing scenario or result in a new scenario being introduced.

Component	Scenario	Disposition	Reference for Disposition
MOV-1	Spurious Opening Results in Excess Letdown	Local Operator Manual Action per procedure OP-3	Table 2, Manual Actions Feasibility table
MOV-2	Spurious Closure results in a loss of injection	Use of second injection valve, MOV-3	Procedure OP-3, step 17
MOV-4	Spurious Closure will result in failure of letdown. This will result in the inability to achieve cold shutdown in 72 hours	Manual Action per procedure OP-3	Table 2, Manual Actions Feasibility table

4.4.2.2 PRA Input to the Plant Specific MSO List

A review of PRA results should be performed in preparation for the expert panel review. If this PRA review was provided as a part of the development of the generic MSO list, this step may not be necessary, depending on the completeness of the information provided for the generic MSO list, and whether item 3 below (new accident sequence review) was performed as input to the generic MSO list.

PRA input to the Expert Panel Review (below) can include a number of inputs, depending on the status and completeness of the PRA and Fire PRA effort. Appendix F includes a broad discussion of PRA reviews that can be performed, including the following:

- 1) Cutset or Sequence Review – a review of cutsets sorted by probability or order to indicate where fire-induced damage can result in a potentially high-risk sequence. Cutsets can also be manipulated by setting basic events representing fire-induced spurious operation (e.g., fail to remain open or closed) to 1.0 and resort the cutsets. This review should result in an identification of spurious operation failure modes (fail to remain opened or closed) with a high Risk Achievement Worth or F-V importance.
- 2) Resolve the model, by assuming a fire-induced initiating event has occurred (Reactor Trip, Loss of Offsite Power) and spurious operation events are set to 1.0, including (but not limited to):
 - MOV spuriously open or close
 - AOV spuriously open or close
 - PORV spuriously open or close
 - Spurious actuation of automatic actuation signals
- 3) Review of possible new Fire-Induced Accident Sequences. This would include a review similar to that performed in preparation for a Fire PRA model development, where fire damage or the performance of operator actions following a fire are assumed, and any accident sequences not already included in the PRA are identified. Details of this review are provided in Attachment H.

The above PRA reviews do not include a complete list of sensitivity studies or analysis that can be performed using an existing PRA. In addition, a simple review of risk importance measures, especially Risk Achievement Worth (RAW) of spurious operations, would be useful.

For Event tree linking models Fussel-Vesely and Risk Achievement Worth of individual basic events representing spurious actuations can be calculated in a similar manner to that performed for fault tree linking models. However the process of identifying potentially risk significant multiple spurious actuations is slightly more involved with a linked event tree model due to the lack of sequence cutsets. In this case the spurious actuation basic events are set to 1.0 and the

sequences (combinations of split fractions leading to core damage) are resolved. The new set of dominant sequences should then be compared with those derived from the base case quantification to identify those sequences that have risen significantly in value. This is followed by an investigation of the cutsets associated with those split fractions which contribute to the inflated sequence values to identify spurious and multiple spurious actuation combinations.

If a full Fire PRA is available, then the results of the Fire PRA can be used as a direct input to the Expert Panel Review (or directly to the Safe Shutdown Analysis, if expert panel review is determined to be not needed for important scenarios). In this case, the following should be included in the safe shutdown analysis:

- 1) Components whose spurious operation in combination with other components results in a risk for the combination (including all cutsets for all fire areas/scenarios) is above $1E-06$ /year CDF or $1E-07$ /year LERF, prior to the performance of post-fire operator actions.
- 2) Single spurious operations, where direct core damage would occur when fire-induced damage of other components in the scenario occurs, and post-fire operator action is assumed failed.

The output from any PRA review should be assessed and summarized. The results of this assessment will be provided to the expert panel for additional considerations.

4.4.2.3 Expert Panel Identification of MSO New Scenarios

The Expert Panel Review is performed to systematically and completely review all spurious and MSO scenarios and determine whether or not each individual scenario is to be included or excluded from the plant specific list of multiple spurious operations to be considered in the plant specific post-fire safe shutdown analysis. Input to the Expert Panel is provided from a number of sources discussed above, resulting in a comprehensive review of spurious operation scenarios.

NEI 04-06, Appendix A provides the scope of circuits to be reviewed, including specific examples of circuit combinations to be included in a review. For example, A-2.1.2.2.1 includes specific PWR examples to be reviewed. These examples should be reviewed in detail by the expert panel to determine scenarios to be reviewed further.

Prior to performing the expert panel review, the following is performed in preparation:

- 1) Provide to the expert panel, the results of the SSA and PRA performed above.
- 2) Provide to the expert panel the generic MSO list and any plant specific review of this list.

3) Provide training to the expert panel.

If the expert panel is held over a several day period, and substitute expert panel members are used, substitute members should also be provided the above information and training prior to participating.

The expert panel as used for the review of MSOs, results in a list of potential MSO that supplements the previously screened generic MSO list. Scenarios identified by the expert panel that should be considered in the SSA are documented and added to the generic MSO list for disposition using the process described in 4.5 below.

As discussed in Appendix F, complete documentation of the expert panel review for new MSOs is important. This documentation should include details of the new MSOs to be considered, as well as possible MSO scenarios that were not considered for treatment under the SSA and the reasoning for not recommending them for consideration. See appendix F for further discussion on documentation of the process, training and results.

4.4.3 Expert Panel Review of MSO List Deletions

The MSO Expert Panel will review all recommended deletions of the generic MSO list. In this review, the expert panel will perform the following functions:

- 1) Review the justification for deletion. Ensure the justification follows the guidance above in 4.4.1, and the justification is adequate.
- 2) Discuss the possible addition of alternate and similar MSO scenarios applicable for the plant.

The expert panel review of the deletions should be documented in a report and retained in support of the MSO review process. Refer to Appendix F for additional guidance on the Expert Panel review.

4.5 Addressing the Plant Specific List of MSOs

4.5.1 Cable Selection & Association for Each Component in an MSO

Components that are not already included in the base SSA are added to the Safe Shutdown Equipment list and analyzed in the same manner as other components in that list. The approach outlined in Section 3.3 can be used to determine the cables associated with each component in an MSO combination. Cables are associated with MSO components in the same manner as they are associated with any other safe shutdown component.

4.5.2 Fire Area Assessment and Compliance Strategies for MSOs

Impacts to specific MSOs are assessed on a fire area basis in the same manner as other impacts to post-fire safe shutdown components. Each component in an MSO combination is assigned to a safe shutdown path. If the individual safe shutdown component's safe shutdown path association is different than the safe shutdown path associated with the component when assessed as part of an MSO, then the additional safe shutdown path(s) associated with the MSO must also be assigned to each component in that MSO. If all components associated with a particular safe shutdown path are located in a common fire area where they have the potential, if damaged by a fire, to impact the required safe shutdown path for that fire area, then a mitigating strategy must be provided for the MSO.

Mitigation strategies applicable to MSOs include the following in addition to the traditional mitigation strategies described in Section 3.4.2.4:

- 1) Disposition based on consideration of Circuit Failure Criteria.
- 2) Disposition based on Fire Modeling
- 3) Disposition based on a Focused-Scope Fire PRA

Several considerations may affect the disposition method chosen for an MSO. First, the least expensive method for dispositioning an MSO may be the traditional compliance strategy, such as a design change or use of an approved operator manual action. If the PRA or Fire Modeling analysis takes more resources to perform than fixing the design or adding a simple operator manual action, then cost may dictate the approach used. If an approved operator manual action is used, however, consideration of the effect of this operator manual action on other fire response operator manual actions should be considered. For example, if the addition of a new operator manual action means the fire response procedure is more difficult, then the existing actions may become less reliable. In this case, the addition of the operator manual action may increase overall risk rather than reducing risk as intended.

This balance is to be considered prior to selecting a mitigating strategy that relies upon operator manual action.

4.5.2.1 Mitigation through Consideration of Circuit Failure Criteria

Circuit failure criteria applicable to MSOs is contained in Appendix B. When evaluating the impact of an MSO on a particular fire area, the circuit failure types for the circuit types contained in Appendix B should be considered. Using the circuit failure criteria, MSOs should be considered as potential "combined equipment impacts". Stated differently, if any of the fire induced circuit failure as described in Appendix B can cause an impact to the group of components in the MSO, this must be evaluated. For example, if the listed MSO were the failure of the block valve to close in conjunction with a spurious opening of a PORV, the block valve would need to be evaluated for circuit failure types that could prevent closure of the block valve, (i.e. a short-to-ground causing a loss of control power or an open circuit causing a

los of circuit continuity). Similarly, if an immediate action to close the block valve at the start of the fire we credited and, if a hot short could subsequently spuriously open the block valve in the same fire area where another hot short could cause the spurious opening of the PORV, then this condition also needs to be addressed.

If all potential fire-induced circuit failures outlined in Appendix B are addressed and, if none leads to all components in the MSO being damaged in a manner that impacts the required post-fire safe shutdown path, then the MSO is dispositioned on the basis of circuit analysis.

If mitigation by the use of circuit analysis is not possible, then another means of mitigation, either one of the traditional means described in Section 3.4.2.4 or one of the means listed below, must be developed. If either of the means listed below is used as the mitigating strategy for the MSO, then review and acceptance of the disposition by the Expert Panel is required.

4.5.2.2 Fire Modeling Disposition

Licensees currently perform qualitative fire ignition, fire spread and fire damage analysis as a part of fire hazard analyses, engineering equivalency evaluations, deviation requests and/or exemption requests, as appropriate. Use of industry accepted Fire Modeling Programs will serve as an upgrade to this current practice. As an alternative to obtaining NRC review and concurrence for these types of equivalency evaluations, the Resolution Methodology proposes an additional enhancement to the equivalency evaluation process by the introduction of an Expert Panel review and concurrence for those instances where fire modeling is used to disposition an identified MSO Impact.

Fire Modeling used during for the disposition of MSOs must be performed consistent with the methods described in NUREG/CR-6850, using verified fire models as described in NUREG-1824. Additionally, process improvements developed for NFPA-805 applications will be incorporated, as applicable.

When selecting a fire size for the analysis, the 98% upper bound of the fire size should be used. Additionally, the location of the fire would include consideration of the pinch points for the cables, possible ignition of secondary combustibles, etc. For transient combustibles, any location within the plant should be considered unless it is physically impossible

4.5.2.3 Fire PRA Disposition

Disposition using a Focused-Scope Fire PRA is performed using Chapter 5, Risk Significant Screening.

4.5.3 Expert Panel Review of MSO Disposition

As can be seen from Figure 4-1 above, MSOs dispositioned using the methods described in 3.4.2 or using the circuit failure criteria from Appendix B as explained above do not need to be reviewed by the Expert Panel. All other methods of disposition, however, need to be reviewed by the Expert Panel.

In this review, the Expert Panel will review the disposition for adequacy, as well as take into account additional deterministic factors. This review includes:

- 1) Review the justification for deletion. Ensure the justification follows the guidance above (or in Chapter 5), and the justification is adequate.
- 2) Discuss the possible alternative dispositions for the MSO scenario, including traditional compliance methods discussed in 3.4.2.

The review in item 2 should include the uncertainty/sensitivity of the evaluation being performed, the effect the traditional compliance strategy would have on other MSOs or spurious operations, the cumulative effect of spurious operations and fire risk in the area, and other factors the Expert Panel determines are important.

The review of the disposition of an MSO using Fire PRA will vary slightly between the MSO using a focused-scope Fire PRA and a Full Fire PRA. With a full Fire PRA, the analysis of a compartment or area will include analysis of all potentially important fire scenarios. The expert panel should become familiar with the general compartment/area results, and the characteristics of the area that affect both overall risk and the risk for the MSO. These characteristics should be consistent, and given they are consistent, the expert panel review of the MSO analysis is somewhat simpler. With a Focused-scope Fire PRA, the expert panel will need to ensure that the characteristics affecting the MSO analysis are consistently and accurately applied. The sensitivity and uncertainty analysis should include the affects of assumptions made for the fire characteristics, including basic factors such as fire size assumptions, non-suppression probabilities, etc.

Refer to Appendix F for additional guidance on the Expert Panel review.

4.5.4 Feedback to the Generic MSO List

As this and other MSO methods are implemented (e.g., implementation of NFPA 805), the MSO list is expected to grow. For the method above, the following criteria should be used to determine if any new MSO should be added to the generic MSO list:

- a. Any new MSO not on the generic list,
- b. The MSO does not screen using the conservative screening in Chapter 5 (i.e., requires detailed Fire PRA to determine the risk), or is not analyzed using Fire PRA resulting in a compliance strategy being applied.

Any new MSO meeting the above criteria should be provided to NEI and the respective Owner's Group. NEI will then screen the MSO, resulting in an updated generic MSO list.

4.6 Documentation

Documentation should be included in the Fire Area Assessment, as discussed in 3.4.2.5 above. The Fire Area Assessment may refer to additional analysis supporting the disposition such as the PRA or Fire Modeling Analysis.

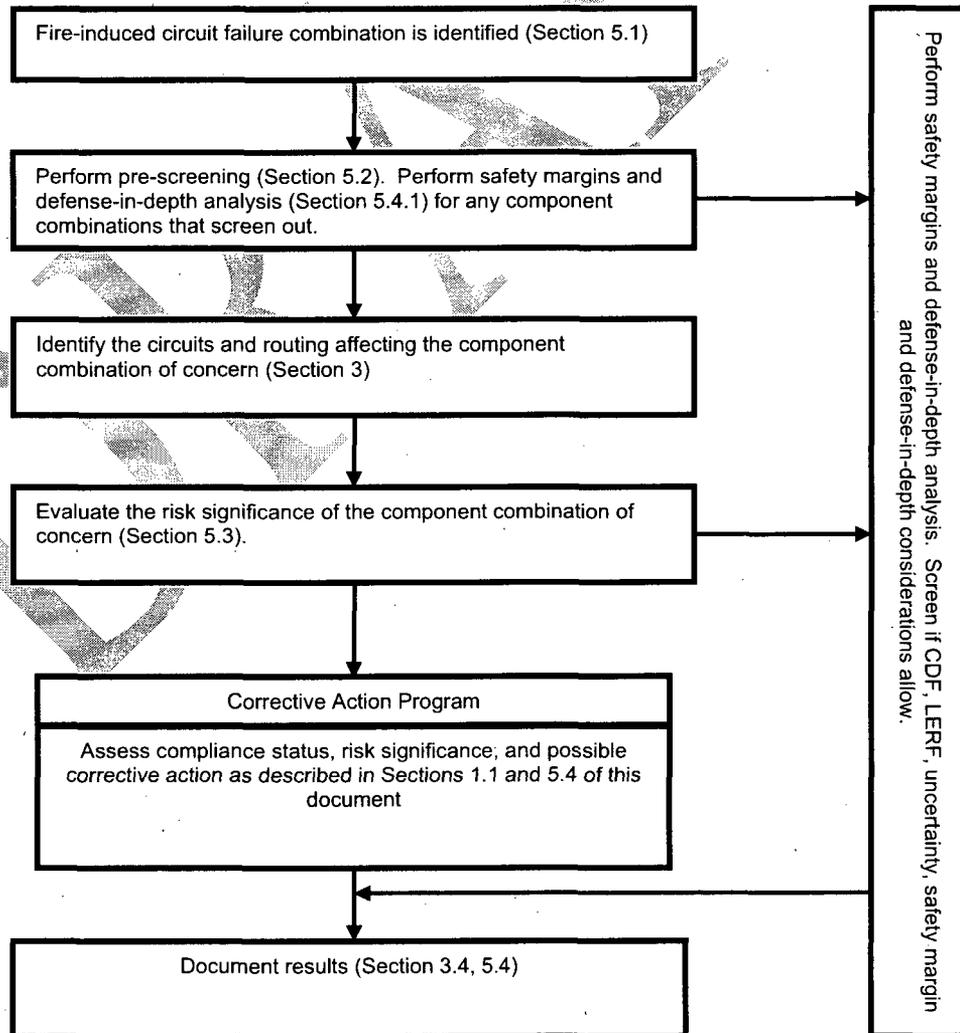
DRAFT

5 RISK SIGNIFICANCE ANALYSIS

This section provides a method for determining the risk significance of identified fire induced circuit failure component combinations (MSOs) to address the risk significance of the current circuit failure issues.

Section 5.2 focuses on the preliminary screening of these circuit failures to determine if more detailed analysis methods are warranted. Section 5.3 provides a quantitative method for evaluating the risk significance of identified component combinations. Section 5.4 covers integrated decision making for the risk analysis, including consideration of safety margins and defense-in-depth considerations.

**Figure 5-1
Simplified Process Diagram**



5.1 COMPONENT COMBINATION IDENTIFICATION

5.1.1 Consideration of Consequences

This first step limits consideration to component combinations whose maloperation could result in loss of a key safety function, or in immediate, direct, and unrecoverable consequences comparable to high/low pressure interface failures. The component combinations identified in Chapter 4 above, would initially be reviewed to ensure that the MSO scenario results in a consequence of concern. If the MSO scenario does not result in one of the above consequences, the MSO may be qualitatively screened as low risk. This review must take into account all possible fire-induced failures, and the overall affect of the MSO on the plant risk.

5.1.2 Selection of MSO Scenarios to be Analyzed

The purpose of this review is to ensure the proper risk is assessed for the possible component combinations prior to screening a combination for consideration. Given an MSO combination is provided, this combination will result in one or more PRA scenario of interest. The MSO scenario may need further definition at this point, including identification of additional fire-damaged components, timing issues, etc. Timing issues may include details such as component A would need to spuriously operate before component B for the scenario to affect safe shutdown.

5.2 PRELIMINARY SCREENING

The "risk screening tool" presented here is taken directly from Reference 7.4.43. It is the result of the NRC's effort to develop this method. Adapted from NEI 00-01 Rev 0 [Ref. 7.4.46], it is relatively simple, based on measures readily available from the FP SDP [Ref. 7.4.45], but conservative in that credits are limited to ensure the likelihood of "screening out" a circuit issue that could be of greater-than-very-low-risk-significance is minimized. Examples of this conservatism include use of generic fire frequencies based on fire zone or major components; treatment of potentially independent spurious actuations as dependent (i.e., no multiplication of more than two probabilities); crediting of manual suppression in a fire zone only if detection is present there; and choice of the most stringent screening criterion from Ref. 7.4.46. Note that none of the "additional considerations" among the screening factors below is permitted to introduce a factor <0.01 as a multiplier.

5.2.1 Screening Factors

The following screening factors are used.

5.2.1.1 Fire Frequency (F)

Table 1.4.2 of the FP SDP [Ref. 7.4.45] (modified here as Table 4-5 for use in the subsequent example application) and Table 4-3 of EPRI-1003111 [Ref. 7.4.44] list the mean fire frequencies at power by plant location and ignition source. The frequencies are characteristic of a fire occurring anywhere within the location. The mean fire frequencies by location range from a minimum of $\sim 0.001/\text{yr}$ (Cable Spreading Room in Ref. 7.4.45; Battery Room in Ref. 7.4.44) to maximum of $\sim 0.1/\text{yr}$ (Boiling Water Reactor Building in Ref. 674.45; Turbine Building in both Ref. 7.4.44 and Ref. 7.4.45). These values used in Ref. 7.4.44 and Ref. 7.4.45 eliminate fire events judged to be "non-challenging." Considering uncertainties in their probability distributions (somewhat reflected in the two-sided 90% upper and lower confidence bounds in Ref. 7.4.44), the following ranges for fire frequencies are used:

- HIGH, $\geq 0.03/\text{yr}$ but $\leq 1/\text{yr}$
- MEDIUM, $\geq 0.003/\text{yr}$ but $< 0.03/\text{yr}$
- LOW, $< 0.003/\text{yr}$

5.2.1.2 Probability of Spurious Actuation (P)

Table 2.8.3 of the Ref. 7.4.45 (modified here as Table 5-6 for use in the subsequent example application) and Tables 7.1 and 7.2 of Ref. 7.4.40 provide point estimates for the probability of spurious actuation ranging from a minimum of "virtually impossible" (armored inter-cable interactions in Ref. 7.4.45; armored thermoset inter-cable interactions in Ref. 7.4.40) to a maximum approaching 1.0 ("no available information about cable type or current limiting devices" in Ref. 7.4.45; any intra-cable short in Ref. 7.4.40). Ref. 7.4.40 also provides ranges for these estimates. The lowest non-zero values are 0.01 for "in-conduit, inter-cable only" in Ref. 7.4.45 and 0.002 for the "high confidence range" on intra-cable, armored thermoset with fuses in Ref. 7.4.40.

NRC Regulatory Issue Summary 2004-03 [Ref. 6.6.1] states that "for cases involving the potential damage of more than one multiconductor cable, a maximum of two cables should be assumed to be damaged concurrently". Therefore, no more than two multiple spurious actuations within separate cables are assumed to be independent when calculating the probability P, i.e., no more than two of the spurious actuation probabilities in Ref. 7.4.40 or Ref. 7.4.45 should be multiplied together. Consideration of this conservative assumption and the ranges cited in these reports suggests the following ranges for probability of spurious actuation:

- HIGH, > 0.3 but ≤ 1
- MEDIUM, ≥ 0.03 but < 0.3

- LOW, ≥ 0.003 but < 0.03
- VERY LOW, < 0.003

Multiplying F and P over their respective ranges yields the maxima shown in Table 5-1 for the pairings F*P.

5.2.1.3 Additional Considerations

The F*P pairings represent the frequency of a fire-induced spurious actuation of a component combination. Core damage will occur only if (1) the fire is localized and severe enough to induce spurious actuation; (2) the fire is not suppressed prior to inducing the spurious actuation, and (3) other non-fire related contingencies, including human actions and equipment operation, are unsuccessful. Thus, for core damage to occur, there must also be a "challenging" fire; failure to suppress the fire prior to the spurious actuation; and failure to avoid core damage via non-fire means, represented by the conditional core damage probability (CCDP). The number of potentially vulnerable locations (zones) addresses possible variation in the screening threshold frequency depending upon the number of zones that the equipment traverses where there is a potential for fire damage.

5.2.1.4 Challenging Fire (G)

Fires can vary in magnitude, ranging from small, essentially self-extinguishing, electrical relay fires to complete combustion of an entire compartment. To estimate how challenging a fire could be for screening purposes, we consider the largest fire source in the zone and combustible type. Ref. 7.4.45 specifies categories (bins) for both fire type and size.⁴ The factor (G), independent from the fire frequency, for a challenging fire is based on combustible type.

Table 2.3.1 of the Ref. 7.4.45 (modified here as 5-7 for use in the subsequent example application) assigns both 50th and 95th percentile fires for various combustibles to fire size bins ranging from heat release rates of 70 kW to 10 MW. Fires in the 70 kW-200 kW range are considered small; 200 kW-650 kW moderate; and ≥ 650 kW large. Typically, some train separation is built into plant designs in accordance with NRC Regulatory Guide 1.75 [Ref. 7.4.50]. Therefore, small fires are not likely to damage separated trains. Although moderate fires are more damaging, some credit for train separation can still be expected.

Based on the above, for small or moderate size fires that are not expected to be challenging, such as small electrical fires, a factor of 0.01 is applied. For moderate severity fires, including larger electrical fires, a factor of 0.1 is

⁴ Room size and other spatial factors also influence how challenging a fire can be. However, we do not consider these for screening purposes.

applied. For large fires, including those from oil-filled transformers or very large fire sources, the factor is 1.

5.2.1.5 Fire Suppression (S)

Both automatic and manual fire suppression (including detection by automatic or manual means) are creditable. It is assumed that automatic is preferred and a more reliable suppressor than manual, suggesting a non-suppression probability of 0.01 for automatic and 0.1 for manual.⁵ If automatic can be credited, then manual will not. Manual will only be credited if automatic cannot. Thus, the product $F \cdot P$ will be reduced by a factor of either 0.01 (if automatic suppression is creditable) or 0.1 (if automatic suppression is not creditable, but manual is).⁶ Both, implying a reduction by 0.001, will never be credited. Thus, the maximum reduction in the product $F \cdot P$ that can be achieved through consideration of fire suppression is 0.01.

Note the following exception. Energetic electrical fires and oil fires, which are likely to be the most severe fires at a nuclear power plant, may grow too quickly or too large to be controlled reliably by even a fully creditable automatic suppression system. This is not due to degradation of the system but to the characteristics of the fire. Therefore, for fire zones where energetic electrical⁷ or oil fires may occur, no credit will be given to manual suppression, while that for automatic will be reduced to 0.1.

5.2.1.6 CCDP (C)

There should be at least one fire-independent combination of human actions and equipment operation to prevent core damage, provided these are not precluded by the fire itself or its effects. To incorporate this, a CCDP, given the preceding ignition and failures, must be appended to the $F \cdot P \cdot G \cdot S$ value. Table 2.1.1 of the FPSDP (modified here as Table 5-8 for use in the subsequent example application) specifies three types of "remaining mitigation capability" for screening CCDP unavailabilities based on safe shutdown path. These are (1) 0.1 if only an automatic steam-driven train can be credited; (2) 0.01 if a train that

⁵ To credit manual suppression, this method assumes that detection must be present in the fire zone.

⁶ If neither is creditable (e.g., no automatic suppression system and timing/location/nature/intensity of fire precludes manual suppression), there will be no reduction in the product $F \cdot P$. This would apply to scenarios where the source and target are the same or very close to one another. Fire suppression may not be creditable due to insufficient time for suppression prior to cable damage. This is expected to be a rare event and should not be considered unless the configuration clearly shows that immediate component damage is likely to occur.

⁷ Ref. 7.4.48 documents energetic faults only in nuclear power plant switchgear >4 kV. The FP SDP considers both switchgear and load centers as low as ~400 V subject to energetic faults. Consistent with the nature of this screening tool, the FP SDP approach is suggested (i.e., considering switchgear and load centers down to ~400 V as subject to energetic faults).

can provide 100% of a specified safety function can be credited; and (3) 0.1 or 0.01 depending upon the credit that can be assigned to operator actions.⁸

For this last group, a value of 0.1 is assumed if the human error probability (HEP) lies between 0.05 and 0.5, and 0.01 if the HEP lies between 0.005 and 0.05. Credit is based on additional criteria being satisfied, as listed in Table 2.1.1 of the FPSDP.⁹

5.2.1.7 Factor for Number of Vulnerable Zones (Z)

While there is no way to know a priori the exact number of fire zones through which the vulnerable equipment will pass, or the number of these where there is potential for fire damage, something on the order of 10 zones will be assumed for screening purposes. Theoretically, the total frequency of core damage from spurious actuation would be the sum of the frequencies from the individual zones. In general, a higher value would be expected for a higher number of zones. Thus, some type of credit is given for a scenario where the number of vulnerable zones is less than the assumed generic number of 10, say, e.g., five zones or less.

This type of credit would translate into an increase in the screening threshold frequency per zone (call it X), or equivalently a decrease in the zonal core damage frequency (call it D). If we assume limiting the number of vulnerable zones to five or less produces at least a 10% increase in the allowable frequency for zonal screening, i.e., 1.1X, this translates into a decrease in the zonal core damage frequency (D) by a factor Z. To estimate Z, consider the following.

For zonal core damage frequency (D) to meet the threshold (X), D must be $< X$. For five or less vulnerable zones, we allow an increase to at least 1.1X, such that the zonal core damage frequency meets this new threshold, $D < 1.1X$. Relative to the original threshold, X, we require $X > D/1.1$, or $X > 0.9D$. The factor 0.9 corresponds to a maximum value for Z for five or less vulnerable zones.

5.2.2 Six-Factor Frequency of Core Damage (F*P*G*S*C*Z)

The maximum frequencies that result from assuming the maximum credits for G (0.01), S (0.01), C (0.01) and Z (0.9), i.e., a joint credit of 9E-7, for the F*P pairings are shown in Table 4-2. Revision 0 of this document stated that “[t]he criteria for risk significance are ... consistent with Regulatory Guide 1.174 [Reference 7.4.50] guidance.” The plant-specific risk significance screening in

⁸ Even the lower value of 0.01 is considered conservative based on Ref. 8, which cites several examples where non-proceduralized actions by plant personnel averted core damage during severe fires. Of the 25 fires reviewed, none resulted in core damage.

⁹ These criteria include available time and equipment; environmental conditions; procedural guidance; and nature of training.

Revision 0 states that “the criteria for determining that component combinations are not risk significant are as follows:

- If the change in core damage frequency (delta-CDF) for each component combination for any fire zone is less than $1E-7$ per reactor year, AND
- If the delta-CDF for each component combination is less than $1E-6$ per reactor year for the plant, i.e., sum of delta-CDF for all fire zones where circuits for the component combinations (circuits for all) are routed, AND
- If the delta-CDF for each fire zone is less than $1E-6$ per reactor year for the plant, i.e., the sum of delta-CDF for all combinations of circuits in the fire zone.”

Of these three criteria, the most stringent is the first, requiring the delta-CDF to be $<1E-7$ /yr. This seems to be the appropriate criterion to apply to the Six-Factor Frequency of Core Damage since this is the preliminary screening stage.¹⁰ In Table 5-2, neither of the shaded boxes satisfies this criterion exclusively, while the unshaded boxes may satisfy this criterion in certain cases.

5.2.3 Final Screening Table

Restricting the values for challenging fires (G), fire suppression (S), CCDP (C), and the factor for number of vulnerable zones (Z) as shown via the point assignments below,¹¹ the cases where this criterion is satisfied are indicated in Table 5-3. These correspond to the cases where preliminary “screening to green” can be assumed successful.¹²

5.2.3.1 Steps to Use Table 5-3

1. Determine the fire frequency. Use either the generic fire zone frequency or the fire frequency refined by the component-based fire frequency tool in the FPSDP.
2. Determine the probability of spurious actuation, from the FPSDP. If multiple spurious actuations are involved, no more than two of the spurious actuation probabilities should be multiplied together.
3. Determine the block on the table that corresponds to the fire frequency and probability of spurious actuation.

¹⁰ For this preliminary screening delta-CDF is conservatively approximated by CDF itself.

¹¹ Each point is roughly equivalent to a factor of ten reduction or the negative exponent of a power of 10, e.g., 1 point corresponds to $1E-1 = 0.1$, 2.5 points correspond to $1E-2.5 = 0.003$

¹² “Screening to green” in the FPSDP indicates a finding of very low risk-significance that need not be processed further.

4. Determine if the fire is challenging and, if so, to what degree. Use the fire type for the single largest fire source in the zone. For example, a zone with both small and large fires would be considered subject to large fires only (i.e., there is no combination).
5. Determine the fire suppression factor. If both manual and automatic suppression can be credited, the more effective (automatic) is the only one receiving credit (i.e., there is no combination).¹³
6. Determine the CCDP. If no mitigation capability remains, assume a CCDP = 1.
7. Determine the number of vulnerable zones.
8. Sum the points as assigned below to determine if the zone can be screened to green.

Challenging Fires (G)

Large fires = 0 point
Moderate fires = 1 point
Small fires = 2 points

Fire Suppression (S)

None fully creditable = 0 point
Only manual fully creditable = 1 point¹⁴ (reduced to 0 point for energetic electrical or oil fires)
Automatic fully creditable = 2 points (reduced to 1 point for energetic electrical or oil fires)

CCDP (C)

No mitigation capability creditable = 0 point
Only an automatic steam-driven train or operator actions with $0.05 < \text{HEP} < 0.5$ creditable = 1 point¹⁵
A train providing 100% of a specified safety function creditable = 2 points

¹³ Credit is reduced for energetic electrical and oil fires.

¹⁴ As mentioned earlier, detection must be present in the fire zone to take credit for manual suppression.

¹⁵ As mentioned earlier, the credit for operator actions is based on additional criteria being satisfied, including available time and equipment; environmental conditions; procedural guidance; and nature of training.

Factor for Number of Vulnerable Zones (Z)

Greater than five zones = 0 point

Five zones or less = 0.5 point

As shown in Table 5-3, screening at this preliminary stage is not possible if the fire frequency is HIGH and the probability of spurious actuation is HIGH or MEDIUM. All other combinations may be screenable if the point criteria are satisfied.

5.2.3.2 Relative Ranking Evaluation

For analyses where all zones screen, Table 5-4 can be used to evaluate which zone is likely to be the most risk-significant. Table 5-4 converts the F*P maximum frequencies from Table 5-1 into their point equivalents for each F*P pairing.¹⁶ The pairing point equivalent should be added to the total point credits from the preliminary screening to establish the total risk-significance of each zone. The zone with the lowest point total is viewed as the most risk-significant. At least this one zone should be processed through the FPSDP to verify the validity of the tool, i.e., to verify that the tool did not give a false positive. These FPSDP results, and not the results from the preliminary screening tool, should be used to determine the risk-significance of the finding in Phase 2 of the FPSDP.

5.2.4 Example Application

The following example, somewhat exaggerated for illustration purposes, presents the use of the preliminary screening tool. Assume an FPSDP inspection finding that cables for a pressurized water reactor (PWR) power-operated relief valve and its accompanying block valve are routed through the following five fire zones: the auxiliary building, battery room, cable spreading room, emergency diesel generator room, and main control room. Fire damage to the cables can result in the spurious opening of these valves. The cables are thermoset throughout and are encased in an armor jacket only in the battery room. Table 5-6 assigns a probability of spurious actuation of 0.6 to thermoset cables for which no other information is known, which lies in the HIGH range in Table 5-3. Spurious actuation in an armored thermoset cable is considered virtually impossible, corresponding to the VERY LOW range.

The auxiliary building and emergency diesel generator room are protected by automatic sprinkler systems. The switchgear room has an automatic Halon-1301 system. The battery room and main control room have smoke detectors but rely on hand-held extinguishers and hoses for manual fire suppression.

¹⁶ Recall that each point is roughly equivalent to a factor of ten reduction, or the negative exponent of a power of 10. Thus, the F*P pairing for HIGH-HIGH in Table 1 (1/yr = 1E-0/yr) receives 0 point in Table 4, while that for LOW-VERY LOW (1E-5/yr) receives 5 points.

5.2.4.1 Auxiliary Building

Table 5-5 indicates a generic fire frequency for an auxiliary building of 0.04/yr, which lies in the HIGH range in Table 5-3. Since the corresponding probability of spurious actuation is also HIGH, this zone cannot be screened using this tool.

5.2.4.2 Battery Room

Table 5-5 indicates a generic fire frequency for a battery room of 0.004/yr, which lies in the MEDIUM range. Since the cable is armored in this room, the probability of spurious actuation is virtually nonexistent, corresponding to the VERY LOW range. Table 5-3 indicates that preliminary screening is possible for this zone with > 3 points.

Small fires can be expected in the battery room, which earns 2 points from Table 5-7 for fire size (G). Only manual suppression can be credited because of the portable fire extinguishers and automatic detection, producing 1 point for fire detection/suppression (S). No mitigation capability is creditable since both DC trains could be lost in a battery room fire; no point is assigned from Table 5-8 for CCDP (C).¹⁷ There are a total of 5 vulnerable zones, so 0.5 point is assigned for the number of vulnerable zones (Z). The points for the battery room total to 3.5, therefore permitting preliminary screening.

5.2.4.3 Cable Spreading Room - Cables Only

Table 5-5 indicates a generic fire frequency for a cable spreading room with cables only of 0.002/yr, which lies in the LOW range. With no other information known, the thermoset cable has a probability of spurious actuation of 0.6 from Table 5-6, i.e., lying in the HIGH range in Table 5-3. As a result, >4.5 points are needed to screen this zone.

Small fires can be expected in the cable spreading room, which earns 2 points from Table 5-7 for fire size. The automatic Halon extinguishing system results in a credit of 2 points for fire detection/suppression. A remote shutdown station can be credited, meriting 1 point from Table 5-8 for CCDP.¹⁸ There are a total of 5 vulnerable zones, so 0.5 point is assigned. The points for the cable spreading room total to 5.5, therefore permitting preliminary screening.

¹⁷ This conservative assumption of total loss of DC power is for illustration only.

¹⁸ A human error probability for Operator Action between 0.05 and 0.5 is assumed for operator actions at a remote shutdown station, which yields a credit of 1 point. As per Table 8, this credit also assumes that: (1) sufficient time is available; (2) environmental conditions allow access, where needed; (3) procedures describing the appropriate operator actions exist; (4) training is conducted on the existing procedures under similar conditions; and (5) any equipment needed to perform these actions is available and ready for use.

5.2.4.4 Emergency Diesel Generator Building

Table 5-5 indicates a generic fire frequency for an emergency diesel generator room of 0.03/yr, which lies in the HIGH range. With no other information known, the thermoset cable has a probability of spurious actuation of 0.6 from Table 5-6, i.e., lying in the HIGH range in Table 5-3. As a result, this zone cannot be screened using this tool.

5.2.4.5 Main Control Room

Table 5-5 indicates a generic fire frequency for a main control room of 0.008/yr, which lies in the MEDIUM range. With no other information known, the thermoset cable has a probability of spurious actuation of 0.6 from Table 5-6, i.e., lying in the HIGH range in Table 5-3. As a result, >5.5 points are needed to screen this zone.

Moderate-sized fires are expected in the main control room due to the large number of cables and electrical equipment present. Therefore, 1 point is assigned from Table 5-7 for fire size. The portable fire extinguishers and automatic smoke detection merit 1 point fire detection/ suppression. One of two completely independent and redundant trains providing 100% of the specified safety function (Residual Heat Removal)¹⁹ remains fully creditable, meriting 2 points from Table 5-8 for CCDP. There are a total of 5 vulnerable zones so 0.5 point is assigned. The points for the main control room total to only 4.5, therefore preventing preliminary screening.

5.2.4.6 Conclusions

Only the Battery Room and Cable Spreading Room could be screened using this tool. The remaining zones would require more detailed analyses to assess each delta-CDF through the FPSDP. In this example the cables ran through fire zones with different fire initiator frequencies, cable types (and therefore spurious actuation probabilities), potential fire sizes, suppression systems, and core damage mitigation capabilities. The example illustrates that it is easier to screen zones with lower fire initiator frequencies and probabilities of spurious actuation than zones with higher values. Fire zones with lower F*P pairings require less credit from the "additional considerations" (G*S*C*Z) to satisfy the screening threshold of delta-CDF < 1E-7/yr.

5.2.5 Summary

This risk screening tool can be applied to fire-induced, circuit spurious actuation inspection findings that arise from the FPSDP. These findings typically involve the multiple fire zones through which the circuits pass. To streamline the FPSDP, the tool screens zones where the "circuit issue" is expected to be of very low risk-significance based on (1) the fire frequency in the zone where the

¹⁹ Residual Heat Removal need not be the only safety function to achieve safe shutdown. This is an assumption for illustration only.

circuits are located; (2) the probability of spurious actuation; and (3) automatic or manual suppression, or an alternate means to achieve hot shutdown.

The tool estimates six factors to calculate the frequency of core damage: (1) zonal fire frequency; (2) spurious actuation probability; (3) challenging fire factor; (4) probability of non-suppression; (5) CCDP; and (6) factor based on number of vulnerable zones. The tool determines if a fire zone, once it has been assigned to a fire frequency-spurious actuation probability pairing (i.e., the first two factors), can be screened at a maximum delta-CDF threshold of $1E-7$ /yr based on a point system for the remaining four factors.

TABLE 5-1. Maxima for the Pairings F*P (With Round off to the Nearest "3" or "1" for Convenience)		Fire frequency (F)		
		HIGH, ≥ 0.03 /yr but ≤ 1 /yr	MEDIUM, ≥ 0.003 /yr but < 0.03 /yr	LOW, < 0.003 /yr
Probability of spurious actuation (P)	HIGH, ≥ 0.3 but ≤ 1	1/yr	0.03/yr	0.003/yr
	MEDIUM, ≥ 0.03 but < 0.3	0.3/yr	0.009/yr (~0.01/yr)	9E-4/yr (~0.001/yr)
	LOW, ≥ 0.003 but < 0.03	0.03/yr	9E-4/yr (~0.001/yr)	9E-5/yr (~1E-4/yr)
	VERY LOW, < 0.003	0.003/yr	9E-5/yr (~1E-4/yr)	9E-6/yr (~1E-5/yr)

TABLE 5-2. Maxima That Result from Maximum Credits for G (0.01), S (0.01), C (0.01) and Z (0.9), i.e., a Joint Credit of $9E-7$		Fire frequency (F)		
		HIGH, ≥ 0.03 /yr but ≤ 1 /yr	MEDIUM, ≥ 0.003 /yr but < 0.03 /yr	LOW, < 0.003 /yr
Probability of spurious actuation (P)	HIGH, ≥ 0.3 but ≤ 1	9E-7/yr	3E-8/yr	3E-9/yr
	MEDIUM, ≥ 0.03 but < 0.3	3E-7/yr	9E-9/yr	9E-10/yr
	LOW, ≥ 0.003 but < 0.03	3E-8/yr	9E-10/yr	9E-11/yr
	VERY LOW, < 0.003	3E-9/yr	9E-11/yr	9E-12/yr

TABLE 5-3. Point Requirements for Screening (Note use of ">" vs. "≥," i.e., points must EXCEED numbers shown)		Fire frequency (F)		
		HIGH, ≥0.03/yr but ≤1/yr	MEDIUM, ≥0.003/yr but <0.03/yr	LOW, <0.003/yr
Probability of spurious actuation (P)	HIGH, ≥0.3 but ≤1	Do not screen	Screen to green with > 5.5 points	Screen to green with > 4.5 points
	MEDIUM, ≥0.03 but <0.3	Do not screen	Screen to green with > 5 points	Screen to green with > 4 points
	LOW, ≥0.003 but <0.03	Screen to green with > 5.5 points	Screen to green with > 4 points	Screen to green with > 3 points
	VERY LOW, <0.003	Screen to green with > 4.5 points	Screen to green with > 3 points	Screen to green with > 2 points

DRAFT

TABLE 5-4. Establishing Relative Risk Ranking When All Zones Preliminarily Screen¹⁷				
Fire frequency (F)	Probability of spurious actuation (P)	Points		
		Preliminary screen total	Table 4-1 equivalents	Risk-ranking total
HIGH	HIGH	(Zone A - 4)	0	(Zone A - 4)
	MEDIUM		0.5	
	LOW	(Zone B - 3)	1.5	(Zone B - 4.5)
	VERY LOW		2.5	
MEDIUM	HIGH	(Zone C - 2)	1.5	(Zone C - 3.5)
	MEDIUM		2	
	LOW	(Zone D - 2.5) (Zone E - 3)	3	(Zone D - 5.5) (Zone E - 6)
	VERY LOW		4	
LOW	HIGH		2.5	
	MEDIUM	(Zone F - 3.5)	3	(Zone F - 6.5)
	LOW		4	
	VERY LOW	(Zone G - 1.5)	5	(Zone G - 6.5)

Table 5-4 includes an example (items in parentheses) where none of a total of seven zones satisfied the preliminary screening criteria of Table 5-3. When ranked relative to one another using the point equivalents from Table 5-1, Zone C proved to be of highest relative risk-significance (lowest total points, 3.5). At a minimum, Zone C would be processed through Phase 2 of the FPSDP (followed by Zone A, Zone B, etc., if the analyst chose to process more).

TABLE 5-5. Generic Location Fire Frequencies	
Room Identifier	Generic Fire Frequency (Range)
Auxiliary Building (PWR)	4E-2 (HIGH)
Battery Room	4E-3 (MEDIUM)
Cable Spreading Room - Cables Only	2E-3 (LOW)
Cable Spreading Room - Cables Plus Other Electrical Equipment	6E-3 (MEDIUM)
Cable Vault or Tunnel Area - Cables Only	2E-3 (LOW)
Cable Vault or Tunnel Area - Cables Plus Other Electrical Equipment	6E-3 (MEDIUM)
Containment - PWR or Non-inerted Boiling Water Reactor (BWR)	1E-2 (MEDIUM)
Emergency Diesel Generator Building	3E-2 (HIGH)
Intake Structure	2E-2 (MEDIUM)
Main Control Room	8E-3 (MEDIUM)
Radwaste Area	1E-2 (MEDIUM)
Reactor Building (BWR)	9E-2 (HIGH)
Switchgear Room	2E-2 (MEDIUM)
Transformer Yard	2E-2 (MEDIUM)
Turbine Building - Main Deck (per unit)	8E-2 (HIGH)

TABLE 5-6. Probabilities of Spurious Actuation Based on Cable Type and Failure Mode (Range)			
State of Cable Knowledge	Thermoset	Thermoplastic	Armored
No available information about cable type or current limiting devices	0.6 (HIGH)		
Cable type known, no other information known (NOI)	0.6 (HIGH)		0.15 (MEDIUM)
Inter-cable interactions only	0.02 (LOW)	0.2 (MEDIUM)	0 (VERY LOW)
In conduit, cable type known, NOI	0.3 (HIGH)	0.6 (HIGH)	(VERY LOW)
In conduit, inter-cable only	0.01 (LOW)	0.2 (MEDIUM)	
In conduit, intra-cable	0.075 (MEDIUM)	0.3 (HIGH)	

TABLE 5-7 General Fire Scenario Characterization Type Bins Mapped to Fire Intensity Characteristics						
Fire Size Bins	Generic Fire Type Bins with Simple Predefined Fire Characteristics (Points Assigned)					
	Small Electrical Fire (2 points)	Large Electrical Fire (1 point)	Indoor Oil-Filled Transformers (0 point)	Very Large Fire Sources (0 point)	Engines and Heaters (2 points)	Solid and Transient Combustibles (2 points)
70 kW	50 th %ile fire				50 th %ile fire	50 th %ile fire
200 kW	95 th %ile fire	50 th %ile fire			95 th %ile fire	95 th %ile fire
650 kW		95 th %ile fire	50 th %ile fire	50 th %ile fire		
2 MW			95 th %ile fire			
10 MW				95 th %ile fire		

TABLE 5-8. Total Unavailability Values for SSD Path-Based Screening CCDP	
Type of Remaining Mitigation Capability	Screening Unavailability Factor (Points Assigned)
<p>1 Automatic Steam-Driven Train: A collection of associated equipment that includes a single turbine-driven component to provide 100% of a specified safety function. The probability of such a train being unavailable due to failure, test, or maintenance is assumed to be approximately 0.1 when credited as "Remaining Mitigation Capability."</p>	0.1 (1 point)
<p>1 Train: A collection of associated equipment (e.g., pumps, valves, breakers, etc.) that together can provide 100% of a specified safety function. The probability of this equipment being unavailable due to failure, test, or maintenance is approximately 0.01 when credited as "Remaining Mitigation Capability."</p>	0.01 (2 points)
<p>Operator Action Credit: Major actions performed by operators during accident scenarios (e.g., primary heat removal using bleed and feed, etc.). These actions are credited using three categories of human error probabilities:</p> <p>(1) Operator Action = 1.0, which represents no credit given; (2) Operator Action = 0.1, which represents a failure probability between 0.05 and 0.5; and (3) Operator Action = 0.01, which represents a failure probability between 0.005 and 0.05.</p> <p>Credit is based upon the following criteria being satisfied:</p> <p>(1) sufficient time is available; (2) environmental conditions allow access, where needed; (3) procedures describing the appropriate operator actions exist; (4) training is conducted on the existing procedures under similar conditions; and (5) any equipment needed to perform these actions is available and ready for use.</p>	1.0 (0 point), 0.1 (1 point), or 0.01 (2 points)

5.3 PLANT-SPECIFIC RISK SIGNIFICANCE SCREENING

Based on the evaluations performed in Section 5.2 and Section 3 of this document, the licensee may determine that additional safety significance analysis is warranted. The NRC's revised Fire Protection SDP (FPSDP) [Ref 7.4.45] is a useful tool for this purpose; it will be used by NRC inspectors evaluating the significance of circuit failure findings. It calculates the change in Core Damage Frequency for the finding. Other deterministic or probabilistic means may be employed, including plant-specific PRA calculations. Plant-specific PRA calculations should utilize the results of EPRI Report 1008239, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities."

5.3.1 EPRI/NEI Test Results

EPRI TR-1006961, "Spurious Actuation of Electrical Circuits due to Cable Fires, Results of an Expert Elicitation" (Reference 7.4-39) is referenced in both the preliminary screening and detailed screening in the determination of delta-CDF. More information about these results is provided here.

The expert panel report provides a general methodology for determining spurious operation probabilities. P_{SA} is given by the product:

$$P_{SA} = P_{CD} * P_{SACD}$$

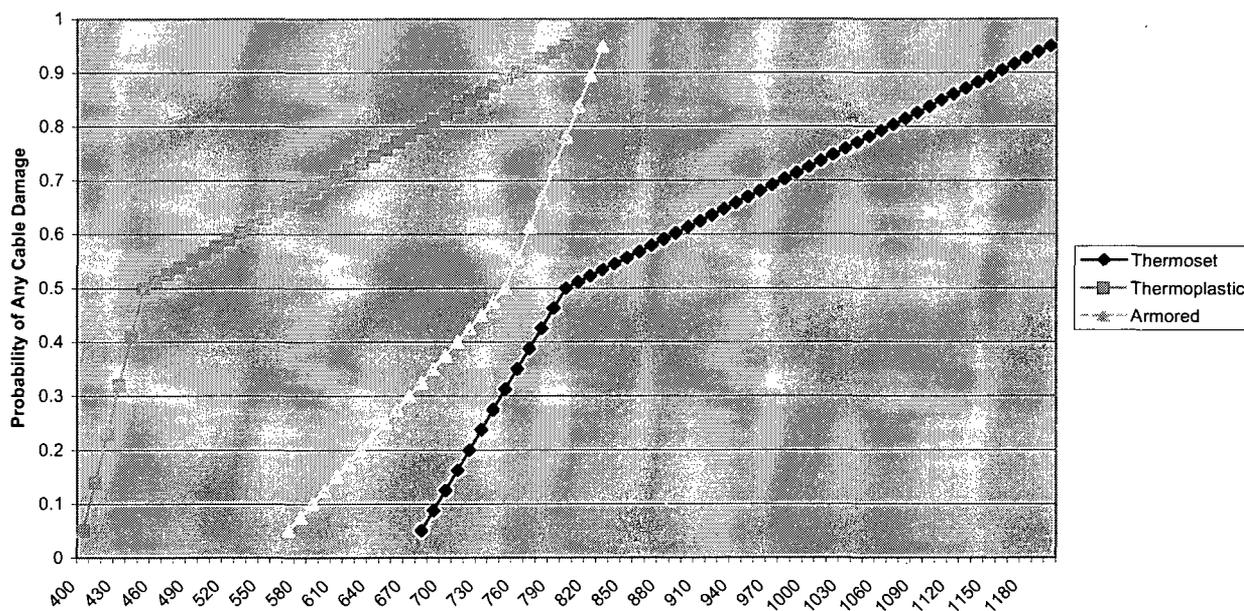
P_{CD} = The probability of cable damage given a specified set of time-temperature and fire-severity conditions, and

P_{SACD} = The probability of spurious actuation given cable damage

P_{CD} can be calculated using fire modeling, taking into account the factors affecting damage and the expected time response for manual suppression. Additionally, the expert panel report provides fragility curves for cable damage versus temperature for thermoset, T-plastic and armored cables. This curve is provided below:

FIGURE 5-2

Fragility Curves for Thermoset, Thermoplastic, and Armored Cable Anchored to the 5%, 50%, and 95% Probability Values for P_{CD} (Reference 6.4.39 Figure 7-1)



There is a considerable body of test information on cable damageability tests, the results of which are not significantly different from these curves. Information on cable damageability is available from these other tests that the analyst may use in lieu of this curve.

This figure is not used in the preliminary screening process, meaning $P_{CD} = 1$ and the spurious operation probability is conservatively estimated as P_{SACD} . For the detailed screening (Section 5.3), P_{CD} can be factored in, given analysis is performed to determine maximum cable temperature for the fire scenario being analyzed. The pilot reports did not use P_{CD} for either screening process.

P_{SACD} can be estimated using Table 5-9. Some general guidance on this is as follows:

- Values in the table, other than B-15, assume control power transformers (CPTs) or other current limiting devices are in the circuit. To determine the probability of

a spurious actuation without a CPT or other current limiting device in the circuit, the listed value should be multiplied by a factor of 2 * $[P_{SACD(B-15)}/P_{SACD(B-1)}]$.

- Based on the Reference 7.5-39, two P_{SACD} (P_{SA}) values used in the fire PRA should be taken as independent events, provided the phenomena occur in different conductors – thus, the two PRA probabilities should be multiplied together.

Additional guidance on the use of this table is provided in the expert panel report (Reference 7.4-39).

EPRI TR-1003326, *Characterization of Fire-Induced Circuit Failures: Results of Cable Fire Testing*, provides supplemental information to the expert panel report. This report provides detailed analysis for each of the tests and characterizes the factors affecting circuit failures in much more detail than the expert panel report. One area discussed by this report is duration of spurious operation events. The test data used for the EPRI report shows that a majority of the circuit failures resulting in spurious operation had a duration of less than 1 minute. Less than 10% of all failures lasted more than 5 minutes, with the longest duration recorded for the tests equal to 10 minutes. The results of the testing described in this report are reflected in RIS 2004-03.

DRAFT

**TABLE 5-9
(SEE REFERENCE 6.4-39, TABLE 7-2)
SUMMARY OF THE PROBABILITIES (P_{SACD})**

Case #	Case	Short Description	P_{SACD} Best Estimate	High Confidence Range	Discussion Reference
P_{SACD} BASE CASE					
B-1	P_{SACD} base case	M/C Tset cable intra-cable	0.30	0.10 - 0.50	7.2.3.1
B-2	P_{SACD} base case	1/C cable, Tset, inter-cable	0.20	0.05 - 0.30	7.2.3.2
B-3	P_{SACD} base case	M/C with 1/C, Tset, Inter-cable	0.01	0.005 - 0.020	7.2.3.3 as modified by EPRI test report
B-4	P_{SACD} base case	M/C with M/C, Tset inter-cable	0.001 - 0.005		7.2.3.4 as modified by EPRI test report
P_{SACD} VARIANTS					
Thermoplastic Variants					
B-5	P_{SACD} variant	Same as #B-1 except thermoplastic	0.30	0.10 - 0.50	7.3.1, last paragraph
B-6	P_{SACD} variant	Same as #B-2 except thermoplastic	0.20	0.05 - 0.30	7.3.1, last paragraph
B-7	P_{SACD} variant	Same as #B-3 except thermoplastic	0.10	0.05 - 0.20	7.3.1, last paragraph
B-8	P_{SACD} variant	Same as #B-4 except thermoplastic	0.01 - 0.05		7.3.1, last paragraph
Armored Variant					
B-9	P_{SACD} variant	Same as #B-1 except armored	0.075	0.02 - 0.15	7.3.2 bullet 5
B-10	P_{SACD} variant	Same as #B-1 except armored cable with fuses (see 7.3:2)	0.0075	0.002 - 0.015	7.3.2 bullet 6
Conduit Variants					
B-11	P_{SACD} variant	Same as #B-1 except in conduit	0.075	0.025 - 0.125	7.3.3 last bullet
B-12	P_{SACD} variant	Same as #B-2 except in conduit	0.05	0.0125 - 0.075	7.3.3 last bullet
B-13	P_{SACD} variant	Same as #B-3 except in conduit	0.025	0.0125 - 0.05	7.3.3 last bullet
B-14	P_{SACD} variant	Same as #B-4 except in conduit	0.005 - 0.01		7.3.3 last bullet
Control Power Transformer (CPT) Variant					
B-15	P_{SACD} variant	Same as #B-1 except without CPT	0.60	0.20 - 1.0	7.4.1

5.3.2 Large Early Release Frequency Evaluation (LERF)

Screening of any component combination requires the consideration of LERF prior to screening. LERF screening can be performed quantitatively or qualitatively, depending on the availability of quantitative analysis. The quantitative screening criteria for LERF are an order of magnitude lower than CDF:

- No LERF review is needed if the screened scenario is shown to have a CDF < $1E-08$ with a sum less than $1E-07$. For these scenarios, even if containment function has failed, the LERF screening criteria have been met.
- If quantitative LERF analysis is available to meet the criteria above, then this analysis can be used to demonstrate LERF screening criteria have been met.
- If no quantitative LERF analysis is available, then a qualitative evaluation can be performed. This analysis should show that containment function will remain intact following the fire scenario, and that a LERF event given core damage is unlikely. Barriers to containment release should be reviewed to ensure that they are free of fire damage.

Qualitative evaluation of LERF should consider the characteristics of LERF given core damage, and what failures would be required. For example, a PWR large dry containment may have a low probability of LERF, even if all containment fans, coolers, spray and igniters have failed. In this case, containment isolation may be the only containment function required to be reviewed for a qualitative LERF review. Another example of ice condenser plants might require igniters and fans to prevent a likely LERF event. In this case, operation of the igniters and fans following the fire scenario would need to be reviewed.

Factors used in screening component combinations against the LERF criteria above should also be considered in the uncertainty evaluation discussed below.

5.3.3 Uncertainty and Sensitivity Analysis

The intent of the screening process and associated analysis is to demonstrate with reasonable assurance that the risk from a circuit failure scenario is below the acceptance criteria described in Regulatory Guide 1.174 (Ref. 7.4.50). The decision must be based on the full understanding of the contributors to the risk and the impacts of the uncertainties, both those that are explicitly accounted for in the results and those that are not. The consideration of uncertainty is a somewhat subjective process, but the reasoning behind the decisions must be well documented. The types of uncertainty are discussed in Regulatory Guide 1.174. Guidance on what should be addressed for the screening process above is discussed below.

Uncertainty analysis may include traditional parameter uncertainty, or may include model or completeness uncertainty considerations. For scenarios involving circuit failures, parameter uncertainty can become less important than

other types of uncertainty. These scenarios typically involve a single accident sequence and a limited number of cutsets. Thus the calculated mean value would be very close to the mean value calculated using parametric distributions. Model and parameter uncertainty is sometimes more effectively treated with sensitivity analysis rather than statistical uncertainty. Sensitivity analysis for this application is discussed below.

Generally, it should be possible to argue on the basis of an understanding of the contributors to the risk that the circuit failure scenario is an acceptable risk. The contributors include the defense-in-depth attributes, plus additional considerations such as spatial information, the type of cable failures required, whether the failure needs to be maintained, etc.

- The closer the scenario risk is to the acceptance criteria, the more detail is required for the assessment/screening and the uncertainty. In contrast, if the estimated risk for a scenario is small in comparison to the acceptance criteria, a simple bounding analysis may suffice with no need for detailed uncertainty analysis.

Factors to be considered in the uncertainty and sensitivity analysis include:

- a) Sensitivity of the results to uncertainty of the factors in the risk equation. This includes factors such as initiating event frequency, suppression probabilities, severity factors, circuit failure probabilities, factors affecting LERF, etc.
- b) Fire modeling uncertainty
- c) Uncertainty of physical location of cables and equipment.

Uncertainty and sensitivity discussions should include any conservative assumptions made as a part of the analysis. For example, if fire modeling is not performed, and conservative assumptions are made about fire spread and/or damage, this should be noted.

5.4 INTEGRATED DECISION MAKING

The results of the different elements of the analysis above must be considered in an integrated manner. None of the individual analysis steps is sufficient in and of itself, and the screening of a circuit failure scenario cannot be driven solely by the numerical results of the PRA screening. They are but one input into the decision making and help build an overall picture of the implications of the circuit failures being considered. The PRA has an important role in putting the circuit failures into the proper context as it impacts the plant as a whole. The PRA screening is used to demonstrate the acceptance criteria have been satisfied. As the discussion in the previous section indicates, both qualitative and quantitative arguments may be brought to bear. Even though the different pieces of the process are not combined in a formal way, they need to be formally documented.

The integrated decision process therefore includes consideration of the following:

- The screening PRA results
- Safety margins and defense-in-depth
- Uncertainty of the results.

5.4.1 Defense-In-Depth and Safety Margins Considerations

The information in Section 5.4.4.1 is derived from Appendix A to NFPA 805, 2001 Edition, and Ref. 7.4.50. These methods should be applied to issues that are screened out either after the application of Tables 5-1 through 5-3, or after the quantitative risk significance screen in Section 5.3.

5.4.1.1 Defense-In-Depth

Defense-in-depth is defined as the principle aimed at providing a high degree of fire protection and nuclear safety. It is recognized that, independently, no one means is complete. Strengthening any means of protection can compensate for weaknesses, known or unknown, in the other items.

Balance among DID elements is a cornerstone of risk-informed applications, and is described in Ref. 7.4.50, Section 2.2.1.1. This document provides the following guidance:

- If a comprehensive risk analysis is done, it can be used to help determine the appropriate extent of defense in depth (e.g., balance among core damage prevention, containment failure, and consequence mitigation) to ensure protection of public health and safety.
- Further, the evaluation should consider the impact of the proposed licensing basis change on barriers (both preventive and mitigative) to core damage, containment failure or bypass, and balance among defense in depth attributes.

For fire protection, defense-in-depth is accomplished by achieving a balance of the following:

- Preventing fires from starting
- Detecting fires rapidly, controlling and extinguishing promptly those fires that do occur
- Providing protection for SSCs important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the shutdown of the plant

For nuclear safety, defense-in-depth is accomplished by achieving a balance of the following:

- Preventing core damage
- Preventing containment failure
- Mitigating consequence

For fire protection and fire PRA, both traditional fire protection DID and traditional nuclear safety DID are represented. Fire protection DID has been treated in the past as a balance. Fire areas with likely fires have automatic suppression, areas with less likely and smaller fires do not have automatic suppression, some areas allow transient combustible storage and some do not, etc. The DID review in this document attempts to balance both the level of traditional fire protection DID and the DID for protection of public health and safety (CDF and LERF).

Consistency with the defense-in-depth philosophy is maintained if the following acceptance guidelines, or their equivalent, are met:

1. A reasonable balance is preserved among 10 CFR 50 Appendix R DID elements.
2. Over-reliance and increased length of time or risk in performing programmatic activities to compensate for weaknesses in plant design is avoided.
3. Pre-fire nuclear safety system redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system and uncertainties (e.g., no risk outliers). (This should not be construed to mean that more than one safe shutdown train must be maintained free of fire damage.)
4. Independence of defense-in-depth elements is not degraded.
5. Defenses against human errors are preserved.
6. The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.

It should be noted that all elements of fire protection DID may not exist for beyond design basis fire scenarios. For example, a CDP of 1.0 is possible if enough fire barriers are breached. Such beyond design basis scenarios, however, should be demonstrated to be of less risk significance, with certainty. A scenario with all elements of DID, and a CDF of $9E-08$ /year would be treated differently than a scenario with a CDP of 1.0, and a CDF of $9E-08$ /year. In the end, the balance results in consideration of all aspects of the component combination, including the risk, DID, SM, uncertainty, and other relevant issues.

Defense-in-depth review for multiple spurious operations should consider whether the scenario affects more than one element of DID. The example above with a CDP at or near 1.0 may be considered unacceptable if detection/suppression is ineffective. For example, if we found a scenario from a fire inside a cabinet, where suppression prior to damage to all target cables was unlikely, and the CDP was near 1, then DID would be inadequate. In most cases, this lack of DID would correspond to a high calculated risk, since the DID elements for fire protection are integrated into the risk calculation. However, if the risk calculation relies heavily

on a low fire frequency to screen the scenario, the risk calculation could screen such a scenario. The DID review would, however, not show a balance between DID and risk, and the scenario would not screen.

Applying a DID review to a screening process needs to account for conservatism in the screening. It is common to use a screening assignment of 1.0 for CDP or manual suppression during screening in order to perform the analysis with minimal resources. The DID review needs to qualitatively assess these factors to assure DID is maintained if a quantitative assessment is not available. Additional analysis may be required to complete the DID assessment in this case, since the information available may not have been sufficient to perform a quantitative assessment.

The above criteria and discussion should be used to evaluate whether defense-in-depth is maintained if a potential fire-induced circuit failure is screened out.

5.4.1.2 Safety Margins

The licensee is expected to choose the method of engineering analysis appropriate for evaluating whether sufficient safety margins would be maintained if the fire induced circuit failure were screened out. An acceptable set of guidelines for making that assessment is summarized below. Other equivalent acceptance guidelines may also be used. With sufficient safety margins (Reference 7.4.50):

- Codes and standards or their alternatives approved for use by the NRC are met.
- Safety analysis acceptance criteria in the licensing basis (e.g., FSAR, supporting analyses) are met, or provide sufficient margin to account for analysis and data uncertainty.

5.4.2 Corrective Action

If, when all evaluation phases are completed, the Δ CDF for a component or a component pair remains greater than or equal to $1E-6$ per reactor year for all fire areas or the Δ CDF for a fire area remains greater than or equal to $1E-6$ per reactor year for all component pairs within the fire area (summing in each case only the Screen 5 results), further analysis using detailed plant fire PRA models or actions to reduce the summed Δ CDF below $1E-6$ /year will be evaluated. The complexity of possible corrective measures can be kept to a minimum by defining the additional risk reduction needed to render the Δ CDF less than $1E-7$ per reactor year for any fire area. As an example, if a potential spurious actuation has been determined to have a Δ CDF of $1E-5$ per reactor year for any fire area after completing the screening process, a corrective action that applies an additional reduction factor of at least 100 would result in an acceptable configuration.

Component combinations or fire areas that do not meet the screening criteria above should be placed within the plant's Corrective Action Program (see Section

1.1 of this document). Evaluation of the corrective action should be performed using the existing plant procedures and criteria, and using the screening analysis results as part of the evaluation. If the component combination or fire area is within the existing licensing basis develop a compliance strategy or disposition to mitigate the effects due to fire damage for each component or its circuit. Any regulatory reporting should be in accordance with existing regulations.

5.4.3 Documentation

The accurate and comprehensive documentation of this assessment will be prepared and maintained as a retrievable plant record following established practices. The documentation should be maintained in accordance with existing plant procedures.

As discussed in Chapter 4 above, the documentation is referenced or included in the Fire Safe Shutdown Analysis for the area or areas affected by the MSO

5.5 PRA Quality

5.5.1 Applicability of the ANS FPRA Standard

The ANS Fire PRA Standard (which is being integrated into the ASME Combined PRA Standard) provides high level and supporting requirements for all steps performed in a detailed PRA used for MSO analysis. The applicability and use of the Fire Standard would depend somewhat on the Fire PRA process used, as discussed in the following sections.

In general, as the PRA results for an MSO approach the acceptance criteria described above, and as conservatism is removed from the analysis, the applicable capability category for the analysis can be increased. As the discussion below points out, if the screening method above is used, no capability category in the Fire Standard can be met. As more detailed Fire PRA is performed, the capability category may be Category 1 for lower risk MSOs or MSOs analyzed using conservative PRA assumptions, or may be Category 2 for detailed Fire PRA results approaching the acceptance criteria above. This general philosophy may not be applicable to all SRs, and a review of SRs not meeting Category 2 for this last example would have to include an assessment of the impact of a lower capability category on the results.

5.5.1.1 Screening Fire PRA

If an MSO or group of MSOs is screened using the preliminary screening method as described in Sections 5.2 above, the Fire Standard requirements do not apply. The method is conservative, and review against the standard would result in a "not met" assessment for many of the supporting requirements.

5.5.1.2 Focused Scope Fire PRA

If the Fire SDP or NUREG/CR-6850 is used to analyze the MSO, then the applicable supporting requirements of the standard can be reviewed against the analysis. However, many of the Fire Standard SRs are not applicable to a Focused-Scope Fire PRA, since the focused scope analyzes the fire features related to the MSO alone, and not associated with the whole plant or whole room risk estimate. For example, if none of the MSO analysis involved Hydrogen Fires, Bus Duct Fires, Reactor Coolant Pump Fires, etc., then the various SRs related to these fires or areas containing these fires may not need to be reviewed for the MSO analysis.

For a Focused-Scope Fire PRA, only the applicable SRs would need to be reviewed in support of the MSO analysis. Additionally, SRs that are reviewed may not be applied in a similar level of detail as a full Fire PRA. For example, non-suppression analyzed for an individual scenario would be reviewed against the applicable SRs. However, the SRs may be applicable to many other possible scenarios not associated with the MSOs. The review of the SR would be limited to the application, and as a result, the associated grade for the SR would only be assigned for the limited scope review. As a result, the Peer Review scope would need to be specified and documented as a part of the overall MSO documentation process. This includes both the scope of the SRs reviewed or not reviewed and the limitations or scope of each of the reviewed SRs.

5.5.1.3 Full Fire PRA

If a full Fire PRA is performed, and the MSO scenario analysis is included in the full Fire PRA, then all of the Fire PRA Standard SRs would apply. As with any application, SRs where a not met or Category I is assessed would need to be documented as a part of the MSO analysis, demonstrating the associated F&O does not affect the analysis results.

5.5.2 Peer Review of the Focused-Scope or Full Fire PRA

A peer review of the focused-scope Fire PRA is required once the initial screening of MSOs is complete. The peer review will differ considerably from a peer review of a complete Fire PRA in the following aspects:

- 1) The focused-scope Fire PRA will contain screening analysis as described above, which is not designed to meet the Fire PRA standard Supporting Requirements. The screening analysis is not reviewed against any of the Fire PRA Standard SRs.
- 2) The detailed Fire PRA for MSO scenarios is an analysis of the MSO scenarios only, and would not provide a Fire PRA for a Fire Area or Compartment. As such, the Fire PRA would only apply specific Fire PRA steps needed to show the MSO risk is low. The corresponding Fire PRA standard requirements for the applied steps would be applicable for the peer review, but other steps would not need to be reviewed. Additionally, many of the SRs reviewed would only be applicable to the MSOs analyzed, and not to the entire plant.

Prior to the performance of a peer review against a Focused-Scope Fire PRA, the expected scope should be documented by a pre-review of the MSO analysis results. This scope would then be used to determine the number and capability of the Fire PRA Peer Review Team. Upon completion of the peer review, the limitations of the review for each SR should also be specified in the documentation.

6 DEFINITIONS

The following definitions are consistent with NRC-recognized definitions.

The numbers in brackets [] refer to the IEEE Standards in which the definitions are used. Refer to Section 2 of IEEE Standard 380-1975 for full titles.

Those definitions without a specific reference are consistent with those specified in reference 7.4.32.

Associated circuits

Generic Letter 81-12 – Those cables (safety related, nonsafety related, Class 1E, and non-Class 1E) that have a physical separation less than that required by Appendix R Section III.G.2 and have one of the following:

Common Power Source

A common power source with the shutdown equipment (redundant or alternative) and the power source is not electrically protected from the circuit of concern by coordinated breakers, fuses, or similar devices, or

Spurious Operation

A connection to circuits of equipment whose spurious operation would adversely affect the shutdown capability (e.g., Residual Heat Removal/Reactor Coolant System isolation valves, Automatic Depressurization System valves, Pressure-Operated Relief Valves, steam generator atmospheric valves, instrumentation, steam bypass, etc.), or

Common Enclosure

A common enclosure (e.g., raceway, panel, junction, etc.) with the shutdown cables (redundant or alternative), and are not electrically protected by circuit breakers, fuses or similar devices, or will allow the propagation of the fire into the common enclosure.

Cable

IEEE Standard 100-1984 – A conductor with insulation, or a stranded conductor with or without insulation and other coverings (single-conductor cable) or a combination of conductors insulated from one another (multiple-conductor cable). [391]

Circuit

IEEE Standard 100-1984 – A conductor or system of conductors through which an electric current is intended to flow. [391]

Circuit failure modes

The following are the circuit failure modes that are postulated in the post-fire safe shutdown analysis as a result of a fire:

Hot Short

A fire-induced insulation breakdown between conductors of the same cable, a different cable or from some other external source resulting in a compatible but undesired impressed voltage or signal on a specific conductor.

Open Circuit

A fire-induced break in a conductor resulting in a loss of circuit continuity.

Short-to-Ground

A fire-induced breakdown of a cable's insulation system resulting in the potential on the conductor being applied to ground/neutral.

Cold Shutdown Repair

Repairs made to fire damaged equipment required to support achieving or maintaining cold shutdown for the required safe shutdown path.

Conductor

IEEE Standard 100-1984 – A substance or body that allows a current of electricity to pass continuously along it. [210, 244, 63] *Clarification:* a single “wire” within a cable; conductors could also be considered a circuit or a cable.

Design Basis Fire

A postulated event used in the post-fire safe shutdown analysis. See Exposure Fire.

Emergency Control Station

Location outside the main control room where actions are taken by operations personnel to manipulate plant systems and controls to achieve safe shutdown of the reactor. [NRC RIS 2005-30]

Enclosure

IEEE Standard 380-1975 – An identifiable housing such as a cubicle, compartment, terminal box, panel, or enclosed raceway used for electrical equipment or cables. [384]

Exposure Fire

SRP Section 9.5.1 – An exposure fire is a fire in a given area that involves either in-situ or transient combustibles and is external to any structures, systems, or components located in or adjacent to that same area. The effects of such fire (e.g., smoke, heat, or ignition) can adversely affect those structures, systems, or components important to safety. Thus, a fire involving one train of safe shutdown equipment may constitute an exposure fire for the redundant train located in the same area, and a fire involving combustibles other than either redundant train may constitute an exposure fire to both redundant trains located in the same area.

Fire Area

Generic Letter 86-10 – The term "fire area" as used in Appendix R means an area sufficiently bounded to withstand the hazards associated with the fire area and, as necessary, to protect important equipment within the fire area from a fire outside the area.

In order to meet the regulation, fire area boundaries need not be completely sealed with floor to ceiling and/or wall-to-wall boundaries. Where fire area boundaries were not approved under the Appendix A process, or where such boundaries are not wall-to-wall or floor-to-ceiling boundaries with all penetrations sealed to the fire rating required of the boundaries, licensees must perform an evaluation to assess the adequacy of fire area boundaries in their plants to determine if the boundaries will withstand the hazards associated with the area and protect important equipment within the area from a fire outside the area.

Fire Barrier

SRP Section 9.5 – those components of construction (walls, floors, and their supports), including beams, joists, columns, penetration seals or closures, fire doors, and fire dampers that are rated by approving laboratories in hours of resistance to fire and are used to prevent the spread of fire.

Fire Frequency (F_f)

The frequency of fires with a potential to damage critical equipment if left alone.

Fire Protection Design Change Evaluation

The process replacing the 50.59 evaluation process (described in NEI 02-03) that is used by a licensee to document compliance with the fire protection license condition to assure that changes to the fire protection program do not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

Fire Protection Program

10 CFR 50, Appendix R, Section II.A – the fire protection policy for the protection of structures, systems, and components important to safety at each plant and the procedures, equipment, and personnel required to implement the program at the plant site. The fire protection program shall extend the concept of defense-in-depth to fire protection in fire areas important to safety, with the following objectives:

- Prevent fires from starting.
- Rapidly detect, control, and promptly extinguish those fires that do occur.
- Provide protection for structures, systems, and components important to safety so that a fire that is not promptly extinguished by the fire suppression activities will not prevent the safe shutdown of the plant.

Fire Zone

The subdivision of fire area(s) for analysis purposes that is not necessarily bound by fire-rated barriers.

Free of Fire Damage

It is expected that the term “free of fire damage” will be further clarified in a forthcoming Regulatory Issue Summary. Until this occurs, NRC recommends using the following guidance in Regulatory Guide 1.189:

“The structure, system, or component under consideration is capable of performing its intended function during and after the postulated fire, as needed, without repair.”

Generic Letter 86-10 Fire Hazards Evaluation

A technical engineering evaluation used to evaluate equivalency of fire protection features to those required by the regulations or to evaluate fire protection features that are commensurate with the potential fire hazard. For plants licensed prior to 1979, these evaluations may form the basis for an Appendix R exemption request or support a plant change evaluation using accepted regulatory processes. For plants licensed after January 1, 1979, these evaluations may be used in conjunction with a fire protection design change evaluation to alter the current licensing basis or they may be submitted to the NRC for review and acceptance as a deviation request. (Note: Previously approved deviation requests may be altered using a fire protection design change evaluation without resubmittal to the NRC.)

High Impedance Fault

Generic Letter 86-10 – electrical fault below the trip point for a breaker on an individual circuit. See “Multiple High Impedance Fault.”

High/Low Pressure Interface

Refer to Appendix C to this document.

Hot Short

See "Circuit failure modes."

Isolation Device

IEEE Standard 380-1975 – A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits. [384]

Local Operation

Operation of safe shutdown equipment by an operator outside the Main Control Room when automatic, remote manual, or manual operation are no longer available (e.g. opening of a motor operated valve using the hand wheel).

Operator Manual Action

Action performed by operators to manipulate components and equipment from outside the main control room to achieve and maintain post-fire hot shutdown, not including "repairs."

Multiple High Impedance Fault(s)

A condition where multiple circuits fed from a single power distribution source each have a high impedance fault. See Appendix B.1.

Open Circuit

See 'Circuit Failure Modes'.

Probability of Spurious Actuation (P_{SA})

The probability of undesirable spurious operation(s) of the component, or of component being potentially impacted by the fire-induced circuit failure.

Raceway

IEEE Standard 380-1975 – Any channel that is designed and used expressly for supporting wires, cable, or busbars. Raceways consist primarily of, but are not restricted to, cable trays, conduits, and interlocked armor enclosing cable. [384]

Remote Control

Plant design features that allow the operation of equipment through a combination of electrically powered control switches and relays. Remote control can typically be performed from the control room or from local control stations, including the remote shutdown panel and other locations with control capability outside the control room.

Remote Manual Operation

Operation of safe shutdown equipment on the required safe shutdown path using remote controls (e.g., control switches) specifically designed for this purpose from a location other than the main control room.

Remote Shutdown Location

A plant location outside the control room with remote control capability for shutdown.

Remote Shutdown Panel

The panel included within the plant design for the purpose of satisfying the requirements of 10 CFR 50 Appendix A General Design Criterion 19. If electrical isolation and redundant fusing are provided at this location, it may also be suitable for use in achieving and maintaining safe shutdown for an event such as a control room fire.

Repair Activity

Those actions required to restore operation to post-fire safe shutdown equipment that has failed as a result of fire-induced damage. Repairs may include installation, removal, assembly, disassembly, or replacement of components or jumpers using materials, tools, procedures, and personnel available on site (e.g., replacement of fuses, installation of temporary cables or power supplies, installation of air jumpers, the use of temporary ventilation). Credit for repair activities for post-fire safe shutdown may only be taken for equipment required to achieve and maintain cold shutdown. Repairs may require additional, more detailed instructions, including tools to be used, sketches, and step-by-step instructions for the tasks to be performed. Repair activities are intended to restore functions and not equipment since the equipment may be destroyed in a fire event. Repair activities may rely on exterior security lighting or portable lighting if independent 8-hour battery backed lighting is unavailable.

Required Safe Shutdown Path

The safe shutdown path selected for achieving and maintaining safe shutdown in a particular fire area. This safe shutdown path must be capable of performing all of the required safe shutdown functions described in this document.

Required Safe Shutdown System

A system that performs one or more of the required safe shutdown functions and is, therefore, a part of the required safe shutdown path for a particular fire area.

Required Safe Shutdown Equipment/Component

Equipment that is required to either function or not malfunction so that the required safe shutdown path will be capable of achieving and maintaining safe shutdown in a particular fire area and meet the established regulatory criteria.

Required Safe Shutdown Cable/Circuit

Cable/circuit required to support the operation or prevent the maloperation of required safe shutdown equipment in a particular fire area.

Safe Shutdown

[Reference 7.4.38] A shutdown with (1) the reactivity of the reactor kept to a margin below criticality consistent with technical specifications, (2) the core decay heat being removed at a controlled rate sufficient to prevent core or reactor coolant system thermal design limits from being exceeded, (3) components and systems necessary to maintain these conditions operating within their design limits, and (4) components and systems necessary to keep doses within prescribed limits operating properly.

[Reference 7.4.14] For fire events, those plant conditions specified in the plant Technical Specifications as Hot Standby, Hot Shutdown, or Cold Shutdown.

For those plants adopting NFPA 805, the term "safe shutdown" is not explicitly defined. Please refer to the discussion of "Nuclear Safety Performance Criteria" in NFPA 805 for more information about performance criteria that, if met, provide reasonable assurance in the event of a fire that the plant is not placed in an unrecoverable condition.

Safe Shutdown Capability

Redundant

Any combination of equipment and systems with the capability to perform the shutdown functions of reactivity control, inventory control, decay heat removal, process monitoring and associated support functions when used within the capabilities of its design.

Alternative

For a given fire area/zone where none of the redundant safe shutdown capability are “free of fire damage” and dedicated equipment is not provided, the shutdown strategy used is classified as alternative.

Dedicated

A system or set of equipment specifically installed to provide one or more of the post-fire safe shutdown functions of inventory control, reactivity control, decay heat removal, process monitoring, and support as a separate train or path.

Safe Shutdown Equipment/Component

Equipment that performs a function that is required for safe shutdown either by operating or by not mal-operating.

Short-to-Ground

See “Circuit Failure Modes.”

Spurious Operation

The possible inadvertent operation or repositioning of a piece of equipment.

DRAFT

7 REFERENCES

7.1 NRC GENERIC LETTERS

- 7.1.1 80-45: Proposed Rule Fire Protection Program for Nuclear Power Plants
- 7.1.2 80-48: Proposed Rule Fire Protection Program for Nuclear Power Plants
- 7.1.3 80-56: Memorandum and Order RE: Union of Concerned Scientists Petition
- 7.1.4 80-100: Resolution of Fire Protection Open Items
- 7.1.5 81-12: Fire Protection Rule, dated February 20, 1981
- 7.1.6 81-12: Clarification of Generic Letter 81-12, Letter from the NRC to PSE&G, dated April 20, 1982, Fire Protection Rule - 10 CFR 50.48(c) - Alternate Safe Shutdown - Section III.G.3 of Appendix R to 10 CFR 50
- 7.1.7 82-21: Tech Specs for Fire Protection Audits
- 7.1.8 83-33: NRC Positions on Appendix R
- 7.1.9 85-01: Fire Protection Policy Steering Committee Report
- 7.1.10 86-10: Implementation of Fire Protection Requirements, dated April 24, 1986
- 7.1.11 86-10: Supplement 1 to Generic Letter, Implementation of Fire Protection Requirements
- 7.1.12 88-12: Removal of Fire Protection Requirements from Tech Specs
- 7.1.13 88-20: Supplement 4 IPEEE
- 7.1.14 89-13: Supplement 1 Biofouling of Fire Protection Systems
- 7.1.15 92-08: Thermo-Lag Fire Barriers
- 7.1.16 93-06: Use of Combustible Gases in Vital Areas
- 7.1.17 95-01: Fire Protection for Fuel Cycle Facilities

7.2 BULLETINS

- 7.2.1 75-04: Browns Ferry Fire
- 7.2.2 77-08: Assurance of Safety

7.2.3 81-03: Flow Blockage Due to Clams and Mussels

7.2.4 92-01: Failure of Thermo-Lag

7.2.5 92-01: Supplement 1 Failure of Thermo-Lag

7.3 NRC INFORMATION NOTICES

7.3.1 80-25: Transportation of Pyrophoric Uranium

7.3.2 83-41: Actuation of Fire Suppression System causing Inoperability of Safety-Related Equipment, June 22, 1983

7.3.3 83-69: Improperly Installed Fire Dampers

7.3.4 83-83: Use of Portable Radio Transmitters Inside Nuclear Power Plants

7.3.5 84-09: Lessons learned from NRC Inspections of Fire Protection Safe Shutdown Systems (10 CFR 50, Appendix R), Revision 1, March 7, 1984

7.3.6 84-16: Failure of Automatic Sprinkler System Valves to Operate

7.3.7 84-92: Cracking of Flywheels on Fire Pump Diesel Engines

7.3.8 85-09: Isolation Transfer Switches and Post-fire Shutdown Capability, January 31, 1985

7.3.9 85-85: System Interaction Event Resulting in Reactor Safety Relief Valve Opening

7.3.10 86-17: Update – Failure of Automatic Sprinkler System Valves

7.3.11 86-35: Fire in Compressible Material

7.3.12 86-106: Surry Feedwater Line Break

7.3.13 86-106: Supplement 1 Surry Feedwater Line Break

7.3.14 86-106: Supplement 2 Surry Feedwater Line Break

7.3.15 86-106: Supplement 3 Surry Feedwater Line Break

7.3.16 87-14: Actuation of Fire Supp. Causing Inop of Safety Related Ventilation

7.3.17 87-49: Deficiencies in Outside Containment Flooding Protection

7.3.18 87-50: Potential LOCA at High and Low Pressure Interfaces from Fire Damage, October 9, 1987

7.3.19 88-04: Inadequate Qualification of Fire Barrier Penetration Seals

- 7.3.20 88-04: Supplement 1 Inadequate Qualification of Fire Barrier Penetration Seals
- 7.3.21 88-05: Fire in Annunciator Control Cabinets
- 7.3.22 88-45: Problems in Protective Relay and Circuit Breaker Coordination, July 7, 1988
- 7.3.23 88-56: Silicone Fire Barrier Penetration Seals
- 7.3.24 88-60: Inadequate Design & Installation of Watertight Penetration Seals
- 7.3.25 88-64: Reporting Fires in Process Systems
- 7.3.26 89-52: Fire Damper Operational Problems
- 7.3.27 90-69: Adequacy of Emergency and Essential Lighting, October 31, 1990
- 7.3.28 91-17: Fire Safety of Temporary Installations
- 7.3.29 91-18: Resolution of Degraded & Nonconforming Conditions
- 7.3.30 91-37: Compressed Gas Cylinder Missile Hazards
- 7.3.31 91-47: Failure of Thermo-Lag
- 7.3.32 91-53: Failure of Remote Shutdown Instrumentation
- 7.3.33 91-77: Shift Staffing at Nuclear Power Plants
- 7.3.34 91-79: Deficiencies in Installing Thermo-Lag
- 7.3.35 91-79: Supplement 1
- 7.3.36 92-14: Uranium Oxide Fires
- 7.3.37 92-18: Loss of Remote Shutdown Capability During a Fire, February 28, 1992
- 7.3.38 92-28: Inadequate Fire Suppression System Testing
- 7.3.39 92-46: Thermo-Lag Fire Barrier Special Review Team Final Report
- 7.3.40 92-55: Thermo-Lag Fire Endurance Test Results
- 7.3.41 92-82: Thermo-Lag Combustibility Testing
- 7.3.42 93-40: Thermal Ceramics Fire Endurance Tests
- 7.3.43 93-41: Fire Endurance Tests - Kaowool, Interam
- 7.3.44 93-71: Fire at Chernobyl Unit 2

- 7.3.45 94-12: Resolution of GI 57 Effects of Fire Prot. Sys. Actuation on SR Equipt.
- 7.3.46 94-22: Thermo-Lag 3-Hour Fire Endurance Tests
- 7.3.47 94-26: Personnel Hazards From Smoldering Material in the Drywell
- 7.3.48 94-28: Problems with Fire-Barrier Penetration Seals
- 7.3.49 94-31: Failure of Wilco Lexan Fire Hose Nozzles
- 7.3.50 94-34: Thermo-Lag Flexi-Blanket Ampacity Derating Concerns
- 7.3.51 94-58: Reactor Coolant Pump Lube Oil Fire
- 7.3.52 94-86: Legal Actions Against Thermal Science Inc.
- 7.3.53 94-86: Supplement 1
- 7.3.54 95-27: NRC Review of NEI Thermo-Lag Combustibility Evaluation Methodology
- 7.3.55 95-32: Thermo-Lag 330-1 Flame Spread Test Results
- 7.3.56 95-33: Switchgear Fire at Waterford Unit 3
- 7.3.57 95-36: Problems with Post-Fire Emergency Lighting
- 7.3.58 95-36: Supplement 1
- 7.3.59 95-48: Results of Shift Staffing Survey
- 7.3.60 95-49: Seismic Adequacy of Thermo-Lag Panels
- 7.3.61 95-49: Supplement 1
- 7.3.62 95-52: Fire Test Results of 3M Interam Fire Barrier Materials
- 7.3.63 95-52: Supplement 1
- 7.3.64 96-23: Fire in Emergency Diesel Generator Exciter
- 7.3.65 97-01: Improper Electrical Grounding Results in Simultaneous Fires
- 7.3.66 97-23: Reporting of Fires at Fuel Cycle Facilities
- 7.3.67 97-37: Main Transformer Fault
- 7.3.68 97-48: Inadequate Fire Protection Compensatory Measures
- 7.3.69 97-59: Fire Endurance Tests of Versawrap Fire Barriers

- 7.3.70 97-70: Problems with Fire Barrier Penetration Seals
- 7.3.71 97-72: Problems with Omega Sprinkler Heads
- 7.3.72 97-73: Fire Hazard in the Use of a Leak Sealant
- 7.3.73 97-82: Inadvertent Control Room Halon Actuation

7.4 OTHER RELATED DOCUMENTS

- 7.4.1 10 CFR 50.48 Fire Protection (45 FR 76602)
- 7.4.2 10 CFR 50 Appendix A GDC 3 Fire Protection
- 7.4.3 10 CFR 50 Appendix R Fire Protection for Operating Nuclear Power Plants
- 7.4.4 Branch Technical Position APCS 9.5-1 Guidelines for Fire Protection
- 7.4.5 Appendix A to Branch Tech Position 9.5-1 Guidelines for Fire Protection
- 7.4.6 NUREG-0800 9.5.1 Fire Protection Program
- 7.4.7 NRC Insp. Procedure 64100 Postfire Safe Shutdown, Emergency Lighting, Oil Collection
- 7.4.8 NRC Insp. Procedure 64150 Triennial Postfire Safe Shutdown Capability
- 7.4.9 NRC Insp. Procedure 64704 Fire Protection Program
- 7.4.10 NUREG/BR-0195 Enforcement Guidance
- 7.4.11 NUREG-75/087 Standard Review Plan (No revision level listed)
- 7.4.12 NUREG-75/087 Standard Review Plan, Rev. 1
- 7.4.13 NUREG-75/087 Standard Review Plan, Rev. 2
- 7.4.14 Reg Guide 1.120 Fire Protection Guidelines for Nuclear Power Plants
- 7.4.15 Reg Guide 1.120 Rev. 1, Fire Protection Guidelines for Nuclear Power Plants
- 7.4.16 Reg Guide 1.189 Fire Protection for Operating Nuclear Power Plants
- 7.4.17 NUREG-0654 Criteria for Preparation of Emergency Response Plans
- 7.4.18 Temporary Instruction 2515/XXX Fire Protection Functional Inspection
- 7.4.19 SECY-82-13B (4/21/82) Fire Protection Schedules and Exemptions
- 7.4.20 SECY-82-267 (6/23/82) FP Rule for Future Plants

- 7.4.21 SECY-83-269 FP Rule for Future Plants
- 7.4.22 SECY-85-306 Recommendations Regarding the Implementation of App R to 10 CFR 50
- 7.4.23 NRC Temp Instruction 2515/62 Inspection of Safe Shutdown Requirements of 10 CFR 50
- 7.4.24 NRC Temp Instruction 2515/61 Inspection of Emergency Lighting & Oil Collection Requirements
- 7.4.25 NUREG-0050, 2/76; Recommendations Related to Browns Ferry Fire
- 7.4.26 NRC Letter (12/82), Position Statement on Use of ADS/LPCI to meet Appendix R Alternate Safe Shutdown Goals, discusses need for exemption if core uncover occurs.
- 7.4.27 SECY-93-143 Assessment of Fire Protection Programs
- 7.4.28 SECY-95-034 Re-assessment of Fire Protection Programs
- 7.4.29 SECY-96-134 Fire Protection Regulation Improvement
- 7.4.30 Appendix S Proposed Rulemaking
- 7.4.31 NRC letter to NEI dated March 11, 1997; general subject NRC positions on fire-induced circuit failures issues
- 7.4.32 NEI letter to NRC dated May 30, 1997, general subject industry positions on fire-induced circuit failures issues
- 7.4.33 GE-NE-T43-00002-00-02, Revision 0, "Generic Guidance for BWR Post-Fire Safe Shutdown Analysis," November 1999
- 7.4.34 NFPA 805, "Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants," November 2000 ROP
- 7.4.35 NSAC-179L, "Automatic and Manual Suppression Reliability Data for Nuclear Power Plant Fire Risk Analyses", February 1994
- 7.4.36 EPRI TR-100370, "Fire-Induced Vulnerability Evaluation (FIVE)", April 1992
- 7.4.37 EPRI TR-105928, "Fire PRA Implementation Guide", December 1995
- 7.4.38 ANSI/ANS-52.1-1983 "Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants" and ANSI/ANS-51.1-1983 "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants"
- 7.4.39 SU-105928, "Guidance for Development of Response to Generic Request for Additional Information on Fire Individual Plant Examination for External Events"

(IPEEE), a Supplement to EPRI Fire PRA Implementation Guide (TR-105928)"
EPRI, March 2000

- 7.4.40 EPRI Report 1006961, "Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of An Expert Elicitation"
- 7.4.41 EPRI Report 1003326, "Characterization of Fire-Induced Circuit Faults: Results of Cable Fire Testing"
- 7.4.42 NRC Memorandum J. Hannon to C. Carpenter, "Proposed Risk-Informed Inspector Guidance for Post-Fire Safe-Shutdown Associated Circuit Inspections," March 19, 2003, ADAMS Accession Number ML030780326
- 7.4.43 NRC Paper to ANS Topical Meeting on Operating Reactor Safety, Preliminary Screening of Fire-Induced Circuit Failures for Risk Significance," November, 2004
- 7.4.44 EPRI Report 1003111, Fire Events Database and Generic Ignition Frequency Model for U.S. Nuclear Power Plants"
- 7.4.45 NRC Inspection Manual Chapter 0609, Appendix F, "Fire Protection Significance Determination Process," May 2004
- 7.4.46 NEI 00-01, Revision 0, "Guidance for Post-Fire Safe Shutdown Analysis," May 2003
- 7.4.47 NRC Regulatory Guide 1.75, "Physical Independence of Electric Systems," Revision 2, September 1978
- 7.4.48 Raughley, W., and G. Lanik, "Operating Experience Assessment - Energetic Faults in 4.16 kV to 13.8 kV Switchgear and Bus Ducts That Caused Fires in Nuclear Power Plants, 1986-2001," NRC Office of Nuclear Regulatory Research, February 2002
- 7.4.49 Nowlen, S., and M. Kazarians, "Risk Methods Insights Gained from Fire Incidents," NUREG/CR-6738, September 2001
- 7.4.50 NRC Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," Revision 1, November 2002.
- 7.4.51 NEI 04-06, Draft Revision K, "Guidance for Self-Assessment of Circuit Failure Issues," October 2003
- 7.4.52 NUREG/CR-6850, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities Volume 1 and 2, Draft for Public Comment."
- 7.4.53 ANSI/ANS-58.6-1983 and 1996, "Criteria for Remote Shutdown for Light Water Reactors"

- 7.4.54 ANSI/ANS-58.11-1983 “Cooldown Criteria for Light Water Reactors”
- 7.4.55 ANSI/ANS-59.4-1979 “Generic Requirements for Light Water Reactor Nuclear Power Plant Fire protection”
- 7.4.56 NRC Letter to Licensees dated June 19, 1979 “Staff Position – Safe Shutdown Capability”
- 7.4.57 NRC Letter to BWROG dated December 12, 2000 “BWR Owners Group Appendix R Fire Protection Committee Position of SRVs + Low Pressure Systems Used As ‘Redundant’ Shutdown Systems Under Appendix R (Topical Report GE-NE-T43-0002-00-03-R01) TAC No. MA8545)” [ML003776828]

7.5 ADMINISTRATIVE LETTERS

- 7.5.1 95-06 Relocation of Technical Specification Administrative Controls

7.6 REGULATORY ISSUE SUMMARIES

- 7.6.1 2004-03, Risk-Informed Approach for Post-Fire Safe-Shutdown Associated Circuit Inspections

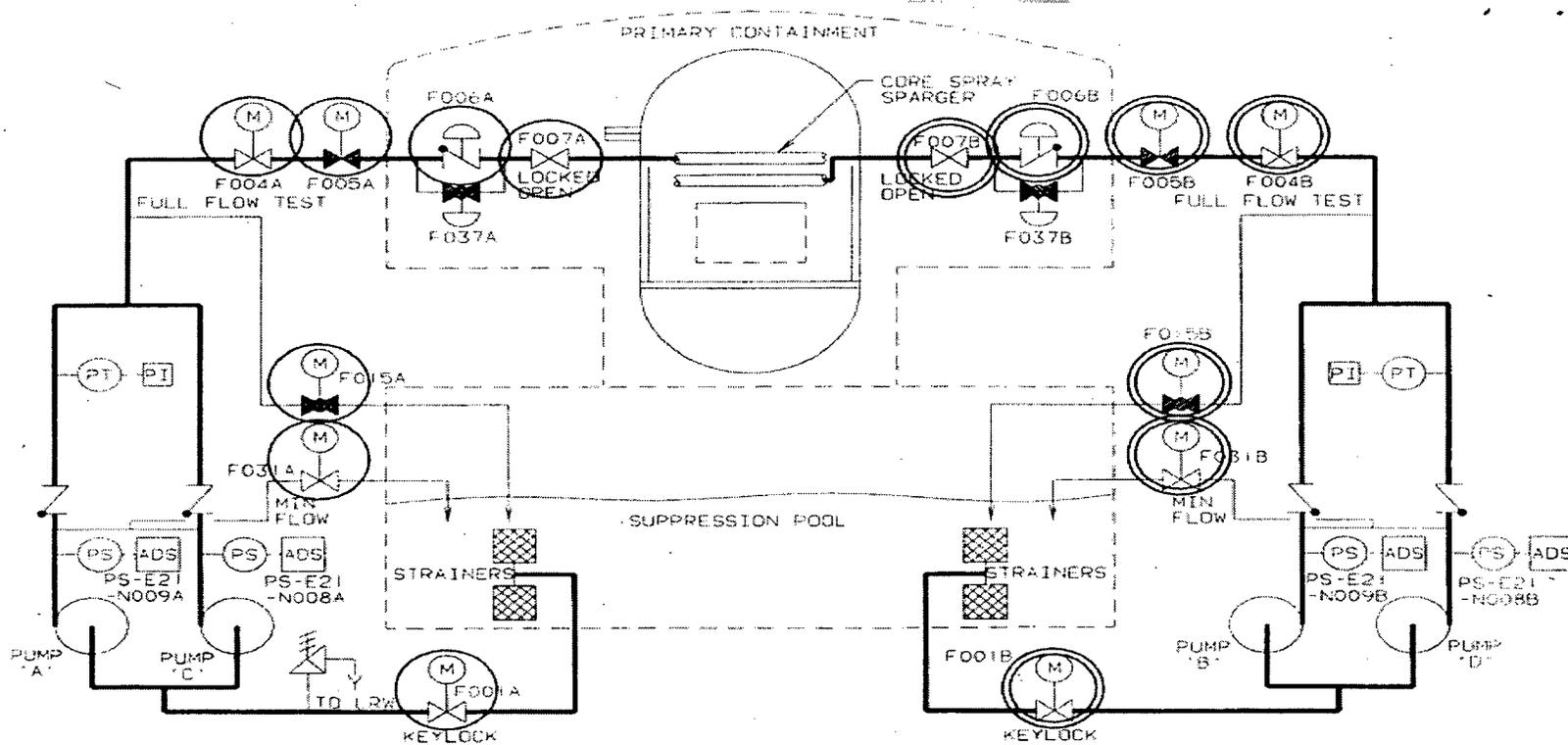
Attachment 1

Example of Typical BWR Safe Shutdown Path Development

Safe Shutdown Path 1	Safe Shutdown Path 2	Safe Shutdown Path 3
<u>Reactivity Control</u>	<u>Reactivity Control</u>	<u>Reactivity Control</u>
CRD (Scram Function) Manual Scram and/or Operator Manual Action to remove RPS Power or to vent the instrument air header	CRD (Scram Function) Manual Scram and/or Operator Manual Action to remove RPS Power or to vent the instrument air header	CRD (Scram Function) Manual Scram and/or Operator Manual Action to remove RPS Power or to vent the instrument air header
<u>Pressure Control</u>	<u>Pressure Control</u>	<u>Pressure Control</u>
Manual ADS/SRVs using available Control Room and Remote Switches	SRVs using the available Remote Shutdown Panel and Remote Switches	Manual ADS/SRVs using available Control Room and Remote Switches
<u>Inventory Control</u>	<u>Inventory Control</u>	<u>Inventory Control</u>
Core Spray	RCIC RHR LPCI	RHR LPCI
<u>Decay Heat Removal</u>	<u>Decay Heat Removal</u>	<u>Decay Heat Removal</u>
RHR Supp. Pool Cooling Mode Service Water Core Spray, Alt. SDC Mode	RHR Supp. Pool Cooling Mode Service Water RHR Shutdown Cooling Mode	RHR Supp. Pool Cooling Mode Service Water RHR, Alt. SDC Mode
<u>Process Monitoring</u>	<u>Process Monitoring</u>	<u>Process Monitoring</u>
Supp. Pool Monitoring Nuc. Boiler Instru.	Supp. Pool Monitoring Nuc. Boiler Instru.	Supp. Pool Monitoring Nuc. Boiler Instru.
<u>Associated Support Functions</u>	<u>Associated Support Functions</u>	<u>Associated Support Function</u>
<u>Cooling Systems</u>	<u>Cooling Systems</u>	<u>Cooling Systems</u>
RHR Room Coolers Service Water Pumphouse HVAC EDG HVAC	RHR Room Coolers RCIC Room Coolers Service Water Pumphouse HVAC EDG HVAC	RHR Room Coolers Service Water Pumphouse HVAC EDG HVAC
<u>Electrical</u>	<u>Electrical</u>	<u>Electrical</u>
EDGs or Offsite Power Electrical Distribution Equipment	EDGs or Offsite Power Electrical Distribution Equipment	EDGs or Offsite Power Electrical Distribution Equipment

Attachment 2

Annotated P&ID Illustrating SSD System Paths [BWR Example]



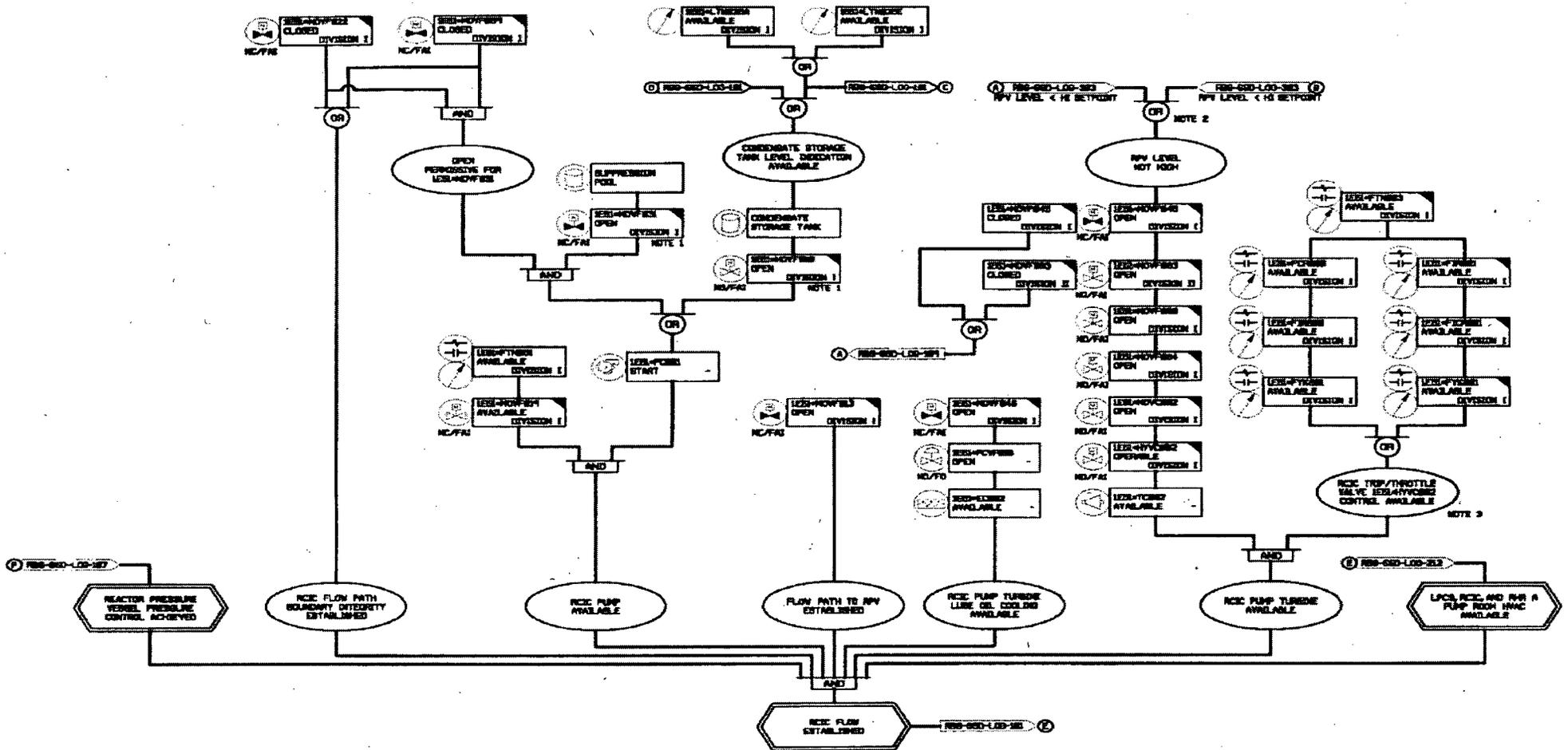
- DIV. I COMPONENTS
- DIV. II COMPONENTS

Attachment 3 (Continued)

A description of the Safe Shutdown Equipment List column headings is provided as follows:

Equipment ID	Identifies the equipment/component ID No. from the P&ID or one line diagram.
Logic Diagram	Identifies a safe shutdown logic diagram reference that may illustrate the relationship between the equipment and other system components
System	Identifies the Appendix R System of which the equipment is part.
Unit	Identifies the Unit(s) that the equipment supports.
Equipment Type	Identifies the type of equipment (e.g., MOV, pump, SOV).
SSD Path	Identifies the safe shutdown path(s) for which the equipment is necessary to remain functional or not maloperate.
Equipment Description	Provides a brief description of the equipment.
Equip FA	Identifies the fire area where the equipment is located.
Normal Mode	Identifies the position or mode of operation of the equipment during normal plant operation.
Shutdown Mode(s)	Identifies the position or mode of operation of the equipment during shutdown conditions.
High/Low	Identifies whether the equipment is considered part of a high/low pressure interface.
Air Fail	If applicable, identifies the position of equipment resulting from a loss of air supply.
Power Fail	Identifies the position of equipment resulting from a loss of electrical power.
Reference	Identifies a primary reference drawing (P&ID or electrical) on which the equipment can be found.

Attachment 4 Safe Shutdown Logic Diagram [BWR Example]



Attachment 5 (Continued)

A description of the Affected Equipment Report column headings is provided as follows:

Fire Area	Identifies the fire area where the equipment or cables are located.
Required Path(s)	Identifies the safe shutdown path(s) relied upon to achieve safe shutdown in the fire area.
FA Description	Provides a brief description of the fire area.
Suppression	Identifies the type of fire suppression (e.g. manual, auto, none) within the fire area.
Detection	Identifies the type of fire detection within the fire area.
System	Identifies the Appendix R System of which the equipment is part.
Unit	Identifies the Unit(s) that the equipment supports.
Logic Diagram	Identifies a safe shutdown logic diagram reference that may illustrate the relationship between the equipment and other system components.
Equipment ID	Identifies the equipment/component ID No. from the P&ID or one line diagram.
Equip Type	Identifies the type of equipment (e.g. MOV, pump, SOV).
SSD Path	Identifies the safe shutdown path(s) for which the equipment is necessary to remain functional or not maloperate.
Equip FA	Identifies the fire area where the equipment is located.
Equipment Description	Provides a brief description of the equipment.
Normal Mode	Identifies the position or mode of operation of the equipment during normal plant operation.
Shutdown Mode(s)	Identifies the position or mode of operation of the equipment during shutdown conditions.
High/Low	Identifies whether the equipment is considered part of a high/low pressure interface.
Air Fail	If applicable, identifies the position of equipment resulting from a loss of air supply.
Power Fail	Identifies the position of equipment resulting from a loss of electrical power.
Disp Code	A code that corresponds to specific compliance strategies and enables sorting and grouping of data.
Compliance Strategy	A brief discussion of the method by which the equipment is resolved to meet Appendix R compliance.

Attachment 6 (Continued)

A description of the Fire Area Assessment Report column headings is provided as follows:

Fire Area	Identifies the fire area where the cables or equipment are located.
Required Path(s)	Identifies the safe shutdown path(s) relied upon to achieve safe shutdown in the fire area.
System	Identifies the Appendix R System of which the equipment is part.
Unit	Identifies the unit(s) that the equipment supports.
Equipment ID	Identifies the equipment/component ID No. from the P&ID or one line diagram.
Logic Diagram	Identifies a safe shutdown logic diagram reference that may illustrate the relationship between the equipment and other system components
Equip Type	Identifies the type of equipment (e.g. MOV, pump, SOV).
FA Description	Provides a brief description of the fire area.
Suppression	Identifies the type of fire suppression (e.g. manual, auto, none) within the fire area.
Detection	Identifies the type of fire detection within the fire area.
Equip Type	Identifies the type of equipment (e.g. MOV, pump, SOV).
SSD Path	Identifies the safe shutdown path(s) for which the equipment is necessary to remain functional or not maloperate.
Equip FA	Identifies the fire area where the equipment is located.
Equipment Description	Provides a brief description of the equipment.
Normal Mode	Identifies the position or mode of operation of the equipment during normal plant operation.
Shutdown Mode(s)	Identifies the position or mode of operation of the equipment during shutdown conditions.
High/Low	Identifies whether the equipment is considered part of a high/low pressure interface.
Air Fail	If applicable, identifies the position of equipment resulting from a loss of air supply.
Power Fail	Identifies the position of equipment resulting from a loss of electrical power.
Cable	Identifies the safe shutdown cable located in the fire area.
Cable Funct	Identifies the function of the cable (e.g., power, control) and whether its failure can result in a spurious operation.
Disp Code	A code that corresponds to a specific compliance strategy and enables sorting and grouping of data.
Compliance Strategy	A brief discussion of the method by which the cable is resolved to meet Appendix R compliance.

APPENDIX A

SAFE SHUTDOWN ANALYSIS AS PART OF AN OVERALL FIRE PROTECTION PROGRAM

A.1 PURPOSE

This appendix discusses the significant improvements that have been made within nuclear industry fire protection programs since the Browns Ferry fire. The discussion will include what defense-in-depth features, in aggregate, constitute a complete and comprehensive fire protection program and what part the safe shutdown analysis plays in that aggregate.

A.2 INTRODUCTION

Each licensee's fire protection program is based on the concept of defense-in-depth. The Appendix R safe shutdown assumptions related to fire intensity and damage potential represent a conservative design basis in that they postulate conditions significantly beyond those that are ever expected to occur based on the existing defense-in-depth plant features. Fire damage and equipment failures, to the extent postulated in an Appendix R safe shutdown analysis, have never been experienced in an operating U.S. nuclear power plant. The worst-case fire ever experienced in a U.S. nuclear power plant was in 1975 at the Browns Ferry Nuclear Power Plant Unit 1. Changes made in the design of U.S. nuclear power plants since this fire have significantly improved the fire safety of these units such that the sequence of events that occurred at Browns Ferry is not expected to recur.

The sections that follow discuss the Brown's Ferry fire, the investigation of that fire, the recommendations made to prevent recurrence of such a fire and the improvement made by the U.S. nuclear power industry relative to these recommendations.

A.3 OVERVIEW

A.3.1 Browns Ferry Fire: Regulatory History

In March of 1975, a fire occurred at the Browns Ferry Nuclear Plant Unit 1. Due to unusual circumstances, the fire was especially severe in its outcome and resulted in considerable loss of systems and equipment with temporary unavailability of systems that would normally be utilized to safely shut down the plant for such events.

The severity of the fire caused the NRC to establish a review group that evaluated the need for improving the fire protection programs at all nuclear plants. The group found serious design inadequacies regarding general fire protection at Browns Ferry and recommended improvements in its report, NUREG-0050, "Recommendations Related to

Browns Ferry Fire" issued in February 1976. This report also recommended development of specific guidance for implementation of fire protection regulation, and for a comparison of that guidance with the fire protection programs at each nuclear facility.

The NRC developed technical guidance from the recommendations set forth in the NUREG and issued those guidelines as Branch Technical Position (BTP) APCSB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants," May 1976. The NRC asked each licensee to compare their operating reactors or those under construction with BTP APCSB 9.5-1 requirements and, in September 1976, informed the licensees that the guidelines in Appendix A of the BTP would be used to analyze the consequences of a fire in each plant area.

In September 1976, the NRC requested that licensees provide a fire hazards analysis that divided the plant into distinct fire areas and show that systems required to achieve and maintain cold shutdown are adequately protected against damage by a fire. Early in 1977 each licensee responded with a fire protection program evaluation that included a Fire Hazards Analysis. These evaluations and analyses identified aspects of licensees' fire protection programs that did not conform to the NRC guidelines. Thereafter, the staff initiated discussions with all licensees aimed at achieving implementation of fire protection guidelines by October 1980. The NRC staff has held many meetings with licensees, has had extensive correspondence with them, and has visited every operating reactor. As a result, many fire protection open items were resolved, and agreements were included in fire protection Safety Evaluation Reports issued by the NRC.

By early 1980, most operating nuclear plants had implemented most of the basic guidelines in Appendix A of the BTP. However, as the Commission noted in its Order of May 23, 1980, the fire protection programs had some significant problems with implementation. Several licensees had expressed continuing disagreement with the recommendations relating to several generic issues. These issues included the requirements for fire brigade size and training, water supplies for fire suppression systems, alternative and dedicated shutdown capability, emergency lighting, qualifications of seals used to enclose places where cables penetrated fire barriers, and the prevention of reactor coolant pump lubrication system fires. To resolve these contested subjects consistent with the general guidelines in Appendix A to the BTP, and to assure timely compliance by licensees, the NRC, in May of 1980, issued a fire protection rule, 10 CFR 50.48 and 10 CFR 50 Appendix R. NRC described this new rule as setting forth minimum fire protection requirements for the unresolved issues. The fire protection features addressed in the 10 CFR 50 Appendix R included requirements for safe shutdown capability, emergency lighting, fire barriers, fire barrier penetration seals, associated circuits, reactor coolant pump lubrication system, and alternative shutdown systems.

Following the issuance of Appendix R, the NRC provided guidance on the implementation of fire protection requirements and Appendix R interpretations at nuclear plants through Generic Letters, regional workshops, question and answer correspondence and plant specific interface. This guidance provided generic, as well as specific, analysis

criteria and methodology to be used in the evaluation of each individual plant's post-fire safe shutdown capability.

A.3.2 Fire Damage Overview

The Browns Ferry fire was a moderate severity fire that had significant consequences on the operator's ability to control and monitor plant conditions. Considerable damage was done to plant cabling and associated equipment affecting vital plant shutdown functions. The fire burned, uncontrolled, while fire fighting efforts, using CO₂ and dry chemical extinguishers, continued for approximately 7 hours with little success until water was used to complete the final extinguishing process.

During the 7-hour fire event period, the plant (Unit 1) experienced the loss of various plant components and systems. The loss of certain vital systems and equipment hampered the operators' ability to control the plant using the full complement of shutdown systems. The operators were successful in bringing into operation other available means to cool the reactor. Since both Units 1 and 2 depended upon shared power supplies, the Unit 2 operators began to lose control of vital equipment also and were forced to shut down. Since only a small amount of equipment was lost in Unit 2, the shutdown was orderly and without incident.

The results of the Browns Ferry fire event yielded important information concerning the effects of a significant fire on the ability of the plant to safely shut down. Although the Browns Ferry fire event was severe and the duration of the fire and the loss of equipment were considerable, the radiological impact to the public, plant personnel and the environment was no more significant than from a routine reactor shutdown. At both Unit 1 and Unit 2, the reactor cores remained adequately cooled at all times during the event.

Due to numerous design and plant operational changes implemented since 1975, including post-TMI improvements in emergency operating procedures, nuclear power plants in operation today are significantly less vulnerable to the effects of a fire event such as that experienced at Browns Ferry. Since 1975, a wide range of fire protection features, along with regulatory and industry guided design and procedural modifications and enhancements, has been implemented. The combination of these upgrades has resulted in a significant increase in plant safety and reliability, and, along with preventative measures, they help to ensure that events similar in magnitude to the Browns Ferry fire will not occur again. The improvements in plant design and procedural operations incorporated since the Browns Ferry fire are described below. The designs and operating procedures that existed at Browns Ferry at the time of the fire are also detailed.

A.3.3 Causes of the Browns Ferry Fire, its Severity and Consequences

The following factors contributed directly to the severity and consequences of the Browns Ferry fire.

- Failure to evaluate the hazards involved in the penetration sealing operation and to prepare and implement controlling procedures.

- Failure of workers to report numerous small fires experienced previously during penetration sealing operations, and failure of supervisory personnel to recognize the significance of those fires that were reported and to take appropriate corrective actions.
- Use of an open flame from a candle (used to check for air leaks) that was drawn into polyurethane foam seal in a cable penetration between the Reactor Building and the cable spreading room.
- Inadequate training of plant personnel in fire fighting techniques and the use of fire fighting equipment (e.g., breathing apparatus, extinguishers and extinguishing nozzles).
- Significant delay in the application of water in fighting the fire.
- Failure to properly apply electrical separation criteria designed to prevent the failure of more than one division of equipment from cable tray fires. Examples are:
 - Safety-related redundant divisional raceways were surrounded by nonsafety related raceways that became combustible paths routed between divisions (i.e., even though separation between redundant division cable trays was consistent with the specified horizontal and vertical required distances, the intervening space was not free of combustibles as required by the existing electrical separation criteria).
 - Contrary to electrical separation criteria, one division of safety related cabling was not physically separated from the redundant division due to cabling of one division routed in conduit within the "zone of influence" of the open redundant division cable tray. Proper application of electrical separation criteria requires that a tray cover or other barrier be installed on the top and/or bottom of the open redundant raceway or between redundant raceways to contain the fire within the open tray and not affect redundant division conduits.
 - Failure to properly separate redundant equipment indicating light circuits, leading to the loss of redundant equipment necessary for safe plant shutdown.
- Cabling utilized within the Browns Ferry raceway system included cable jacket and insulation materials that were less resistant to fire propagation (e.g., PVC, nylon, polyvinyl, nylon-backed rubber tape, and neoprene).

A.3.4 Fire Protection Program Improvements Since Browns Ferry

The Browns Ferry nuclear facility generally conformed to the applicable fire protection and electrical separation criteria and guidelines that existed when it was licensed to

operate by the NRC in 1968. However, the 1975 fire identified a number of areas concerning fire protection design, plant operating criteria, electrical separation and defense-in-depth considerations that required improvement. As described above, the NRC provided the industry with guidance for improvement of fire protection programs through BTP APCS 9.5-1, Appendix A, 10 CFR 50 Appendix R and other related regulatory correspondence. The improvements addressed in NRC guidance are as follows:

1. Fire Prevention Features:

- Fire hazards, both in-situ and transient, are identified and eliminated where possible, and/or protection is provided.
- Sufficient detection systems, portable extinguishers, and standpipe and hose stations have been provided. These systems are designed, installed, maintained, and tested by qualified fire protection personnel.
- Ignition sources controlled.

2. Fire Protection Features:

- Fire barriers and/or automatic suppression systems have been installed to protect the function of redundant systems or components necessary for safe shutdown.
- Surveillance procedures have been established to ensure that fire barriers are in place and that fire suppression systems and components are operable.
- Water supplies for fire protection features have been added, both for automatic and manual fire fighting capability.
- Automatic fire detection systems have been installed with the capability of operating with or without offsite power availability.
- Emergency lighting units with at least 8 hours' battery capacity were provided in those areas where safe shutdown system control was necessary as well as in access and egress areas thereto.
- Fire barrier qualification programs have been established to qualify and test prospective barrier materials and configurations to ensure that their fire endurance and resistivity is acceptable.

3. Fire Hazards Control:

- Administrative controls have been established to ensure that fire hazards are minimized.
- The storage of combustibles in safe shutdown areas has been prohibited or minimized. Designated storage areas for combustibles have been established.
- Transient fire loads such as flammable liquids, wood and plastic have been limited.
- The use of ignition sources is controlled through procedures and permits.
- Controls for the removal of combustibles from work areas, following completion of work activities, have been established.
- Proposed work activities are reviewed by in-plant fire protection staff for impacts on fire protection.
- Noncombustible or less flammable materials including penetration seals, cable jackets, fire retardant wood products, etc., are being used.
- Self-closing fire doors have been installed.
- Oil collection systems have been installed for reactor coolant pumps for containments that are not inerted.

4. Fire Brigade/Training:

- Site fire brigades have been established to ensure adequate manual fire fighting capability is available.
- A fire brigade training program has been established to ensure that the capability to fight potential fires is maintained. Classroom instruction, fire fighting practice and fire drills are performed at regular intervals.
- Fire brigade training includes:
 - Assignment of individual brigade member responsibilities
 - The toxic and corrosive characteristics of expected products of combustion
 - Identification and location of fire fighting equipment
 - Identification of access and egress routes
 - Proper use of fire fighting equipment to be used for electrical equipment fires, fires in cable trays and enclosures, hydrogen fires, flammable liquids fires, hazardous chemical fires, etc.
 - Proper use of communication, emergency lighting, ventilation and breathing equipment
 - Review of detailed fire fighting strategies and procedures.

5. Post-Fire Safe Shutdown Capability

- A comprehensive post-fire safe shutdown analysis program, using the methodology and criteria similar to those described in this report, has been established to ensure that post-fire safe shutdown capability is provided.
- Fire damage is limited so that one train of safe shutdown equipment necessary to achieve and maintain hot shutdown is protected and free from fire damage.
- Cabling for redundant trains of safe shutdown equipment is separated by 1- or 3-hour fire rated barriers. In areas where 1-hour rated barriers are used, additional protection is provided by fire detection and an automatic suppression system.
- Twenty feet of space, containing no intervening combustibles, is provided in lieu of barriers, where applicable. Additional protection is provided by fire detection and an automatic suppression system
- Where redundant trains of equipment, necessary for post-fire safe shutdown, are located in the same fire area and adequate protection for one train cannot be achieved, an alternative or dedicated fire safe shutdown system has been established as follows:

Alternative or dedicated fire safe shutdown systems are capable of achieving and maintaining subcritical reactivity conditions in the reactor, maintaining reactor coolant inventory, and achieving and maintaining hot or cold shutdown conditions within 72 hours.

- Process monitoring instrumentation is provided with the capability of directly monitoring those process variables necessary to perform and control post-fire safe shutdown functions.
- Supporting functions (cooling, lubrication, HVAC, etc.) necessary to ensure continued operation of post-fire safe shutdown systems/equipment are provided.

A.4 CONCLUSION

The changes made to the plant fire protection programs in response to the Browns Ferry fire as described above provide reasonable assurance that the plant design and operation will be safe from the effects of fire. When these changes are integrated into an approach similar to that outlined in the body of this document for assuring the ability to achieve and maintain post-fire safe shutdown, the result is a significantly enhanced plant design with emphasis on precluding any unacceptable consequences resulting from plant fires.

A.5 REFERENCES

- A.5.1 Branch Technical Position BTP APCSB 9.5-1, "Guidelines for Fire Protection for Nuclear Power Plants," May 1976
- A.5.2 NUREG-0050, "Recommendations Related to Browns Ferry Fire" issued in February 1976
- A.5.3 10 CFR 50.48 Fire Protection (45 FR 76602)
- A.5.4 10 CFR 50 Appendix R Fire Protection for Operating Nuclear Power Plants

DRAFT

APPENDIX B

DETERMINISTIC CIRCUIT FAILURE CRITERIA

B.1 PURPOSE

The purpose of this appendix is to provide the criteria and the justification for the criteria provided in Chapter 3 for evaluating circuit failures within a deterministic analysis. This appendix serves to identify the types of circuit failures that need to be considered as part of a deterministic analysis. It also identifies how these circuit failure types need to be considered in the various circuit types employed in a nuclear power plant. In addition, a sub-appendix provides information supporting the elimination of multiple high impedance faults from a plant's deterministic analysis criteria. Reference to and analysis of Industry and NRC sponsored fire test results is made to support the criteria related to whether certain circuit failures should be considered as credible in performing a deterministic evaluation.

B.2 INTRODUCTION

A Fire Protection Program (FPP) licensed to the deterministic requirements of 10CFR50, Appendix R; Appendix A to Branch Technical Position 9.5-1; or, NUREG 0800 Section 9.5-1 is based on the concept of fire protection defense-in-depth. The principles of fire protection defense-in-depth are as follows:

- Prevent fires from starting.
- Rapidly detect and suppress fires that do occur.
- Provide passive fire protection features to prevent fire spread and damage.

Within this envelope of fire safety, licensees also perform a SSA that demonstrates the ability to achieve and maintain safe shutdown in the event of a single fire in any plant fire area. The typical assumption associated with the deterministic SSA is that the fire damages any equipment or circuits contained within the fire area. This assumption, when evaluated in light of the defense-in-depth approach described above, is considered to be a conservative assessment of the upper bound potential for fire damage. This assumption is used as an alternative to specifying a design basis fire and assessing the impact of the design basis fire on the components and circuits in each fire area. Due to the level of conservatism inherent in this assumption, essentially all licensees assumed that not all fire failures within a given fire area occurred at the same time and, as a result, fire-induced impacts could be evaluated and mitigated on a one-at-a-time basis. Prior NRC Staff concurrence with this approach can be inferred from the numerous licensee safety evaluation reports that endorsed the approach either directly or tacitly.

In the 1990's, NRC Staff began to question the validity and level of conservatism associated with the assumption of being able to evaluate and mitigate fire-induced effects on safe shutdown equipment and cables on a one-at-a-time basis. This questioning was the genesis for a series of efforts on the part of both the NRC and the Industry to attempt to demonstrate and define the proper set of assumption to be used for a post-fire SSA. Included within the efforts undertaken by both NRC and the Industry was a series of cable fire tests. The initial cable fire tests were conducted by NEI/EPRI. Subsequent to the NEI/EPRI testing, the NRC conducted the CAROLFIRE cable testing program.

Each of these cable fire testing programs demonstrated that hot shorts resulting in spurious operations were possible. The probabilities developed to capture the likelihood of a hot short resulting in a spurious operation, however, were conditional and based on the subject cable being damaged by the fire. For thermoset cables, cable damage occurred when the cable temperature reached approximately 700°F. For thermoplastic cables, cable damage occurred when cable temperatures reached approximately 400°F. In either of these cases, cable failure was not instantaneous, but took approximately 15 to 30 minutes to occur. When cable damage did result in a hot short with the potential to cause a spurious operation, the hot short was typically of short duration lasting much less than 10 minutes in the worst case.

The initial cursory assessment of the test results was that they had demonstrated that multiple hot shorts and MSOs were, in fact, highly likely and that a SSA failing to include such multiple hot shorts and MSOs was deficient and potentially unsafe. This led to NRC issuing draft Generic Letter 2006-XX that would have required licensees to address all potential fire-induced circuit failures and hot short induced spurious operations occurring simultaneously.

This response to the cable fire test results is problematic for a number of reasons. First, implementing the criteria contained in Generic Letter 2006-XX, even ignoring the fact that such a criterion is totally unbounded and virtually impossible to define, would require defining multiple design basis fires for each fire area. The definition of a design basis fire in a deterministic analysis is in direct conflict with the assumption historically used by licensees and endorsed by the NRC of fire spread throughout the fire area. Second, using a conditional probability of a hot short and spurious operation predicated on the fire damaging the cable directly ignores all of the defense-in-depth fire protection program features that are highly likely to prevent cable damage from ever occurring. Third, when the defense-in-depth fire protection program features are combined with the results of the cable fire testing, the following conclusions are as supportable as those derived from the initial cursory assessment of the test results:

- The current assumption historically used in a post-fire SSA that all circuits within the fire area could be damaged is conservative. The tests results

showed that even at temperatures above 700°F, not all cables in each test were damaged. Certainly in most fire areas which are significantly larger than the test furnace, fire damage to cables will be restricted to those in close proximity to the fire.

- The conclusion above, which suggests that fire damage throughout the fire area will take sometime to develop as the fire spreads, when coupled with the fact that hot shorts and spurious operations in the fire tests took some amount of time to develop even for cables directly affected by the fire, suggests that an assumption of evaluation and mitigation of the effects of fire-induced circuit damage on a one-at-a-time basis is not that unreasonable for circuits with some degree of separation.
- The current assumption that each conductor in each cable within the fire area must be evaluated for the effects of a hot short, a short-to-ground and an open circuit is a conservative assumption, since the testing showed that not all conductors in all cables in the fire test actually experienced these fire-induced circuit failures.
- Finally, given the less than predictable response of any given conductor in any cable to the damaging effects of the fire, it seems overly conservative to assume that, universally, specific conductors within a number of cables will simultaneously experience the fire-induced effects necessary to results in the combination of spurious operations required to provide a specific system level spurious operation impact. The efficacy of single spurious operations has been clearly demonstrated by the cable fire testing. Due to the demonstrated potential for spurious operations seen in the cable fire testing, some degree of consideration of simultaneous impacts to multiple components as a result of fire-induced hot shorts is warranted, particularly for hot shorts within multi-conductor cables, but the need to consider all potential fire-induced circuit failures and hot short induced spurious operations occurring simultaneously is clearly not a viable conclusion that can be drawn from the cable fire testing. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

In this appendix, the cable fire test results will be examined to determine how the current deterministic criteria, historically used for post-fire SSA circuit failures, needs to be adjusted to maintain an appropriate level of fire safety and design conservatism.

B.3 CIRCUIT FAILURES CONSIDERED IN DETERMINISTIC ANALYSIS

B.3-1 Overview of Analysis:

A typical deterministic Appendix R analysis, as described in this document, includes the following steps:

- Identifying Required Safe Shutdown Systems
- Identifying Required Safe Shutdown Equipment

- Identifying Required Safe Shutdown Cables
- Identifying Physical Plant Locations for each
- Assuring **“One”** Safe Shutdown Path with the capability to achieve and maintain safe shutdown in the event of a single plant fire is available for each fire area.

In assuring the availability of a single safe shutdown path in each fire area, the following conservatisms typically apply:

- Fire areas represent large areas of the plant and damage throughout the fire area is assumed.
- All unprotected equipment and cables within the fire area are assumed to be damaged by the fire.
- All unexamined equipment and cables are not credited for mitigating the effects of fires.
- Equipment damage is assumed unless the damage, were it to be postulated, provided a benefit to achieving or maintaining safe shutdown.

In assessing the impact to post-fire safe shutdown in each fire area, the guidance in NEI 00-01 does the following:

- It provides a methodology for identifying equipment and cables of concern for Appendix R Safe Shutdown.
- It provides a means of mitigating every equipment impact and any impacts to the selected combinations of equipment impacts, MSOs, identified in Appendix G.
- It represents an approach that can be consistently applied by licensees throughout the entire industry.

B.3-2, Description of Circuits and Circuit Failure Characteristics:

The types of circuit failures considered in the guidance provided in this document are as follows:

- Open Circuit
- Short-to-Ground
- Hot Short
- High Impedance Fault (NEI CFITF has recommended that consideration of MHIFs be eliminated. Refer to Appendix B.1)

The types of circuits that can be affected by the circuit failure types described above are as follows:

- Power circuits that provide motive power to components once a control circuit properly aligns the component to its bus.

- Primary control circuits that provide operating signals to specific components.
- Secondary logic circuits that provide input through auxiliary contacts to primary control circuits based on instrumentation feedback from plant instruments.
- Control power to primary control and secondary logic circuits that provide the control power necessary for the primary control power and secondary logic circuits to function.
- Instrument circuits that provide either indication to operators or input to primary control or logic circuits.

Typically, an open circuit in any of the circuit types described above has the potential to result in a loss of function for the circuit type.

Similarly, a short-to-ground in any of the circuit types described above has the potential to result in a loss of function for the circuit and it has the additional potential to result in loss of power to components powered from electric sources upstream from the affected circuit. To address this potential, the NRC in Generic Letter 81-12 presented the concept of Associated Circuits – Common Power Supply. Associated Circuits – Common Power Supply is addressed by breaker/fuse coordination. Multiple High Impedance Faults (MHIF) are another way that fire-induced circuit failures can result in a loss of power to components powered from electric sources upstream from the affected circuit. With MHIF, even though all breakers and fuses may be properly coordinated, a combination of cable faults and running loads associated with circuits feed from a common bus, can result in a loss of the feeder breaker to the bus due to over current from the combination of fault and running currents. Appendix B.1 and the results of the NRC and Industry cable fire testing have concluded that the occurrence of MHIFs is not credible and, as such, it does not need to be included in the design criteria for post-fire safe shutdown circuit analysis. The concept of MHIFs was introduced in NRC Generic Letter 86-10.

Hot shorts have the potential to energize circuits from a source different than the power source designed for that purpose. As a result, hot shorts have the potential to spuriously start/stop or open/close components. Depending on the affected component and its function within the shutdown scheme, this starting/stopping or opening/closing could pose a potential impact to post-fire safe shutdown. Solenoids valves controlling the opening or closing of valves, for example, also have the potential to experience an undesired change of state as a result of an open circuit or short-to-ground.

Typically, any of the circuit failure types described above, should they be experienced by a component on the required safe shutdown path in a given fire area, will require mitigation. A component on the required safe shutdown path in a given fire area must be able to perform its required safe shutdown function. Since a hot short, a short-to-ground or an open circuit needs to be postulated for

any conductor in any affected safe shutdown cable in the fire area and since a short-to-ground or an open circuit will result in a loss of function, little analysis is required to conclude that such a potential cable impact is a concern that needs to be addressed.

Conversely, for components that are not specifically required to function in support of post-fire safe shutdown in a particular fire area, but whose malfunction can result in an impact to the systems and components that must function in support of post-fire safe shutdown, the hot short is the primary circuit failure of concern. This is true because hot shorts have the potential to cause equipment to change state to an undesired position that can result in conditions such as, flow diversions from reactor vessel make-up or decay heat removal systems being used in support of post-fire safe shutdown. The group of components falling into this category has been described by the NRC in Generic Letter 81-12 as Associated Circuit – Spurious Operation. Within the post-fire SSA, it becomes difficult to completely distinguish Safe Shutdown Components from components classified under Associated Circuits – Spurious Operation. This is true because many components are both. A Safety Relief Valve (SRV) in a BWR may be classified as a Safe Shutdown Component in a fire area where SRVs and Low Pressure Systems are used as the required safe shutdown path for achieving and maintaining post-fire safe shutdown. Conversely, that same SRV may be classified as an Associated Circuit – Spurious Operation in a fire area where a steam-driven RCIC System is used as the required safe shutdown path for achieving and maintaining post-fire safe shutdown. In this latter case, a spuriously opened SRV could be sufficient to remove the required motive steam from the reactor, thereby impacting the ability of RCIC to perform its required reactor vessel make-up function. As a result, in many licensees post-fire safe shutdown analyses, Safe Shutdown Components and Associated Circuits – Spurious Operation are not distinguished.

This appendix provides criteria for addressing each of the fire-induced circuit failures described above in each of the circuit types described above based on the traditional approach used for post-fire safe shutdown circuit analysis adjusted, as appropriate, by the results of the NRC and Industry cable fire testing.

B.4 INSIGHTS FROM CABLE FIRE TESTS

B.4-1 NEI/EPRI Cable Testing:

The conclusions of the NEI/EPRI Cable Fire Testing are documented in Section 14.4 of EPRI Report 1003326, Characterization of Fire-Induced Circuit Failures. Pertinent Key Observations and Conclusions from the EPRI Report are provided below:

- Given cable damage, single spurious operations are credible and multiple spurious operations cannot be ruled out. External cable hot shorts are also credible, but have a significantly lower probability of occurrence than do

internal hot shorts. An important outcome of the tests is that no external cable hot shorts produced a spurious operation in thermoset cable.

- Given that a hot short occurs in a multi-conductor cable, it is highly probable (over 80%) that multiple target conductor cables will be affected (i.e. multiple simultaneous dependent hot shorts).
- The proximity of conductors to each other is the predominant influence factor in determining fault mode. "Opportunity" must exist for two conductors to short together.
- No open circuit faults occurred during the Test Program. Open circuits do not appear to be a credible primary cable failure mode for fire-induced cable faults.
- Statistical characterization of fire-induced cable failures is achievable. General trends are predictable and primary influence factors are understood. However, probability estimates still carry a relatively high uncertainty.
- Definitive predictions of fire-induced circuit failure outcomes are not viable. The specific behavior and characteristics of any one fault cannot be predicted with full certainty. Failure mode is a function of localized conditions and subtle aspects of geometry and configuration. A full understanding of the fault dynamics and interdependencies is beyond the current state of knowledge.
- The dominant influence factors for the likelihood of spurious operations are: cable type; power supply characteristics; tray fill; conductor connection pattern.
- Cables do not fail immediately. The average time to failure exceeded 30 minutes for thermoset and armored cables and 15 minutes for thermoplastic cables. These statistics are meaningful and important in real world application of test results. The time frames show that early action in a fire is highly likely to be effective at accomplishing the desired function. Preplanned high value actions have a high probability of success and should reduce both likelihood and consequences of serious fires. Similarly, early pre-emptive action for high risk spurious operation components will significantly reduce the risk posed by these components.
- Spurious operations are a transient and finite event; ultimately circuit conditions will degrade to a point that a ground fault de-energizes the source conductor. Postulating that spurious operations will last indefinitely in the absence of intervening action appears to be unrealistic. Probability calculations for thermoset cable indicate that over 96% of all spurious operations will terminate within 10 minutes. This probability estimate carries an uncertainty of approximately 7% at the 95% confidence level.

The following insights can be gained from a review of the key observations and conclusions from the NEI/EPRI cable testing relative to various aspects of the criteria in NEI 00-01 Revision 1 applied in a post-fire SSA:

1.) Addressing Cable Faults **one-at-a-time** vs. **all together at the same time**:

The results of the Expert Opinion Elicitation conclude that the effects of hot shorts leading to spurious operations cannot be ignored. This conclusion is also echoed in the EPRI Report providing the testing results. The EPRI Report providing the results of the cable testing, however, also concludes that the predominant factor in determining cable fault mode is proximity. "Opportunity" must exist for two conductors to short together. Given the current regulatory requirements for divisional separation, proximity of cables for redundant trains should preclude the negative effect of multiple spurious operations at the component and system level. What the testing showed was that conductors within a common cable in a common cable tray could be affected simultaneously. Conductors for redundant trains are precluded from being run within a common cable or cable tray. Given that the approach outlined in NEI 00-01 Revision 1 applies the same criteria to all safe shutdown cables in the fire area, the approach is extremely conservative relative to the "proximity" findings of the EPRI/NEI Testing.

The EPRI/NEI Testing provides no positive indication that multiple spurious operations affecting multiple redundant trains is possible given the current nuclear power plant design and regulatory requirements for divisional separation. Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

2.) Addressing Cable Faults for all conductors in each safe shutdown cable:

The EPRI/NEI Testing provided information suggesting that the approach to post-fire safe shutdown outlined in NEI 00-01 Revision 1 is generally conservative. First of all, no cases involving open circuits were identified. The approach outlined in NEI 00-01 Revision 1 required that open circuits be postulated for each conductor in each safe shutdown cable on the required safe shutdown path in the fire area. Secondly, in the testing hot shorting in cables in conduit was deemed to be unlikely. The approach outlined in NEI 00-01 Revision 1 required the postulation of a hot short on each conductor in each safe shutdown cable regardless of the raceway type. Finally, in the testing inter-cable hot short were found to be highly unlikely. The approach outlined in NEI 00-01 Revision 1 required the postulation of inter-cable hot shorts.

The EPRI/NEI Testing has shown that the approach outlined in NEI 00-01 Revision 1 to fire-induced circuit failures is generally conservative. Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI

00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

3.) Duration and timing of the hot short causing a spurious operation:

Based on the testing, multi-conductor cable are more likely to experience conductor-to-conductor shorts than conductor-to-ground shorts. By postulating a hot short on each conductor in each safe shutdown cable, the approach outlined in NEI 00-01 Revision 1 addressed this. Given that redundant train functions are not included within the same cable, not combining the effects of these hot shorts is not viewed as a serious non-conservatism. Based on the testing, when these intra-cable conductor-to-conductor shorts occur, however, they take approximately 15 to 30 minutes to occur and they last for approximately 10 minutes. This aspect of the testing renders the criterion in the approach outlined in NEI 00-01 Revision 1 requiring the assumption of a hot short lasting until an action is taken to isolate the fault to be conservative. This aspect of the testing also validates assumption made by some licensees that time is available to take an action to mitigate the effect of a potential spurious operation.

The EPRI/NEI Testing has shown that the approach outlined in NEI 00-01 Revision 1 to fire-induced circuit failures is generally conservative.

4.) Affect of Testing on Prior Beliefs about other aspects of Fire-Induced Circuits Failures

The combined opinions of a number of the Expert Panel Members concluded that best estimate for the overall likelihood of a spurious operation for a thermoset cable (i.e. cable type used most predominantly in the industry) lies somewhere between 0.0001 [Brady Williamson] and 0.15 [Section 7.5.2, Technical Summary]. This is consistent with previously published information suggesting that the probability of a hot short/spurious operation was 0.068.

The testing confirmed that the degradation threshold temperature for thermoplastic cable was approximately 400°F and for thermoset cable was approximately 700°F. This is consistent with the previous test results, particularly the oven aging tests conducted at SNL years ago.

To a large extent, the EPRI/NEI Cable Testing has confirmed much of the collective wisdom available prior to the testing.

B.4-2 CAROLFIRE Cable Testing:

The conclusions of the CAROLFIRE Cable Fire Testing are documented in Section 9 of Volume 1 of the CAROLFIRE Test Results. Pertinent Key Observations and Conclusions from the CAROLFIRE Report are provided below:

- The following is Bin 2 Item A as quoted directly from the RIS:

"Intercable shorting for thermoset cables, since the failure mode is considered to be substantially less likely than intracable shorting."

Based on the available data with respect to Bin 2 Item A the CAROLFIRE project has reached the following conclusions:

Inter-cable shorting between two TS-insulated cables that could cause hot shorts and the spurious operation of plant equipment was found to be a plausible failure mode, although the likelihood of this failure mode is low in comparison to intra-cable short circuits leading to spurious operation. While no detailed statistical analysis has been performed, it appears that the conditional probability (give cable failure) of spurious operations arising from this specific failure mode is small in comparison to that previously estimated for spurious operations from intra-cable shorting.

- The following is Bin 2 Item B as quoted directly from the RIS:

"Intercable shorting between thermoplastic and thermoset cables, since this failure mode is considered less likely than intracable shorting of either cable type or intercable shorting of thermoplastic cables."

Based on the available data with respect to Bin 2 Item B the CAROLFIRE project has reached the following conclusions:

Inter-cable shorting between two a TP-insulated cable and a TS-insulated cable that could cause hot shorts and the spurious operation of plant equipment was found to be a plausible failure mode, although the likelihood of this failure mode is low in comparison to intra-cable short circuits leading to spurious operation. While no detailed statistical analysis has been performed, it appears that the conditional probability (give cable failure) of spurious operations arising from this specific failure mode is very small in comparison to that previously estimated for spurious operations from intra-cable shorting.

- The following is Bin 2 Item C as quoted directly from the RIS:

"Configurations requiring failures of three or more cables, since the failure time and duration of three or more cables require more research to determine the number of failures that should be assumed to be "likely".

Given the available data relevant to Bin 2 Item C, the CAROLFIRE project has reached the following conclusions:

The currently available data provide no basis for establishing an a - priori limit to the number of spurious operations that might occur during a given fire. We further find that the timing of spurious operation is a strong function of various case-specific factors including in particular the relative location of various cables relative to the fire source, the routing configuration (e.g., open cable trays or air drops versus conduits), the thermal robustness of the cables insulation material, and the characteristics of the fire source.

- The following is Bin 2 Item D as quoted directly from the RIS:

"Multiple spurious operations in control circuits with properly sized control power transformers (CPTs) on the source conductors, since CPTs in a circuit can substantially reduce the likelihood of spurious operation. Specifically, where multiple (i.e., two or more) concurrent spurious operations due to control cable damage are postulated, and it can be verified that the power to each impacted control circuit is supplied via a CPT with a power capacity of no more than 150 percent of the power required to supply the control circuit in its normal mode of operation (e.g., required to power one actuating device and any circuit monitoring or indication features)."

Given the available data relevant to Bin 2 Item D, the CAROLFIRE project has reached the following conclusions:

The currently available data provide no basis for establishing an a - priori limit to the number of spurious operations that might occur during a given fire even given that the circuit is powered by a "properly sized" CPT. We further find that, as with non-CPT cases, the timing of spurious operations is dependent on the timing of cable electrical failure which is in turn a strong function of various case-specific factors including the relative location of different cables relative to the fire source, the routing configuration (e.g., open cable trays or air drops versus conduits), the thermal robustness of the cables insulation material, and the characteristics of the fire source.

- The following is Bin 2 Item E as quoted directly from the RIS:

"Fire-induced hot shorts that must last more than 20 minutes to impair the ability of the plant to achieve hot shutdown, since recent testing strongly suggests that fire-induced hot shorts will likely self-mitigate (e.g., short to ground) in less than 20 minutes. This is of particular importance for devices such as air-operated valves (AOVs) or power-operated relief valves (POR Vs) which return to their de-energize position upon abatement of the fire-induced hot short."

Given the available data relevant to Bin 2 Item E, the CAROLFIRE project has reached the following conclusions:

While the available data cannot definitively support the conclusion that no hot short would ever persist for greater than 20 minutes, the available data do provide a strong basis for concluding that hot shorts lasting greater than 20 minutes are of at most very low probability. Hence we conclude that with high probability, hot short-induced spurious operation signals will clear within less than 20 minutes. We further conclude that on clearing of the hot short signal, the effects of the spurious operation on plant equipment could persist for a longer time depending on the nature of the impacted equipment. For example, a normally closed Motor Operated Valve might well remain open or partially open even after the hot short-induced spurious operation signal is mitigated whereas a Solenoid Operated Valve would return to its fail safe condition on mitigation of the hot short-initiated spurious operation signal.

The following insights can be gained from a review of the key observations and conclusions from the CAROLFIRE cable testing relative to various aspects of the criteria currently applied in a post-fire SSA:

1.) **Addressing Cable Faults *one-at-a-time* vs. *all together at the same time*:**

The results of the CAROLFIRE testing conclude that the probability of an inter-cable hot short, either thermoset to thermoset, thermoset to thermoplastic or thermoplastic to thermoplastic, is small to very small in comparison to that previously estimated for intra-cable hot shorts. Additionally, the CAROLFIRE testing provided no basis for establishing a limit on the number of spurious operations that might occur. The testing, however, did conclude that the one of the major factors in determining the potential for a hot short and/or spurious operation is the relative location of the cables to the fire source. This conclusion is almost identical with the NEI/EPRI testing that concluded that the predominant factor in determining cable fault mode is proximity. Opportunity" must exist for two conductors to short together. Given the current regulatory requirements for divisional separation, proximity of cables for redundant trains should preclude the negative effect of multiple spurious operations

at the component and system level. What the CAROLFIRE testing showed was that conductors within a common cable in a common cable tray could be affected simultaneously. Conductors for redundant trains are precluded from being run within a common cable or cable tray. Given that the approach outlined in NEI 00-01 Revision 1 applied the same criteria to all safe shutdown cables in the fire area, the approach is extremely conservative relative to the "proximity" findings of the CAROLFIRE testing.

The CAROLFIRE testing provides no positive indication that multiple spurious operations affecting multiple redundant trains is possible given the current nuclear power plant design and regulatory requirements for divisional separation. Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

2.) Addressing Cable Faults for all conductors in each safe shutdown cable:

The CAROLFIRE testing provided information suggesting that the approach outlined in NEI 00-01 Revision 1 to post-fire safe shutdown is conservative. In the testing, inter-cable hot shorting between cables was deemed to be far more unlikely than intra-cable hot shorting. The approach outlined in NEI 00-01 Revision 1 required the postulation of a hot short on each conductor in each safe shutdown cable regardless of the cable type. The approach outlined in NEI 00-01 Revision 1 required the postulation of inter-cable hot shorts.

The CAROLFIRE testing has shown that the approach outlined in NEI 00-01 Revision 1 to fire-induced circuit failures is generally conservative. Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

3.) Duration and timing of the hot short causing a spurious operation:

The CAROLFIRE testing provided no indication that hot shorts will last longer than 20 minutes. Therefore, the criterion in the approach outlined in NEI 00-01 Revision 1 requiring the assumption of a hot short lasting until an action is taken to isolate the fault is conservative.

The CAROLFIRE testing has shown that the approach outlined in NEI 00-01 Revision 1 to fire-induced circuit failures is generally conservative relative to the timing and duration of spurious operations.

4.) Affect of Testing on Prior Beliefs about other aspects of Fire-Induced Circuits Failures

The CAROLFIRE testing concluded that the probability of an inter-cable hot short is small to very small in comparison to probabilities previously determined for intra-cable hot shorts.

The CAROLFIRE Testing also provided no indication that all cables in a given temperature environment will behave similarly. The potential for cable damage and conductor to conductor hot shorting to occur is a function on many variables. Cable failures and hot short are random occurrences that cannot be accurately predicted by the analysis of a single variable such as temperature in the vicinity of the cable.

To a large extent, the CAROLFIRE testing has confirmed the collective wisdom available prior to the testing related to inter-cable hot shorts.

B.4--3 Overall Implications from the Cable Fire Testing:

Industry & NRC Cable Fire Testing conducted to date has:

- Demonstrated that many aspects of the criteria provided in NEI 00-01 Revision 1 are generally conservative. The exception to this is the treatment of multi-conductor cables with the potential to cause multiple simultaneous spurious operations. The simultaneous MSOs, as a result of the design and regulatory requirements for divisional separation, will impact only a single division of post-fire safe shutdown equipment.

Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

- Provided an indisputable basis for not requiring the types of changes to the post-fire safe shutdown fire-induced circuit failure criteria proposed by the NRC in draft Generic letter 2006-XX.
- Provided clear information that hot shorts resulting in spurious component operations can occur. MSOs are also possible, but the concern should be limited to multi-conductor cables with the potential to cause MSOs. The simultaneous MSOs, as a result of the design and regulatory requirements for divisional separation, will impact only a single division of post-fire safe shutdown equipment.

Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix

G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

- Provided valuable information suggesting that the occurrence of fire-induced hot shorts are affected by many variables. The postulation of multiple, simultaneous spurious operations affecting both divisions of safe shutdown equipment is highly unlikely given the divisional separation requirements applied in the design of a nuclear power plant.
- Provided valuable information that the occurrence of fire-induced hot shorts is a random event, not predictable by studying a single variable such as air temperature in the vicinity of a cable.
- Provided valuable information that the occurrence of fire-induced hot shorts that are not in close proximity to each other are unlikely to occur in a manner that supports the conditions required for MSOs without the prior intervention by other aspects of the Fire Protection Defense-in-Depth Program. MSOs are also possible, but the concern should be limited to multi-conductor cables with the potential to cause MSOs. The simultaneous MSOs, as a result of the design and regulatory requirements for divisional separation, will impact only a single division of post-fire safe shutdown equipment.

Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

- Provided valuable information regarding the types of fire-induced circuit failures that are most likely to occur given damage to the cable.
- Provided valuable information regarding the failure temperature of cables, the time to failure at that temperature, the length of time that a fire-induced hot short will be sustained and the fact that the hot shorts are, generally, followed by a short-to-ground.
- Provided valuable information suggesting that by using a fire-induced circuit failure approach like that outlined NEI 00-01 Revision 1 in the deterministic post-fire SSA reasonable assurance of the ability to achieve and maintain post-fire safe shutdown in the event of a plant fire will be attained.

B.5 CONCLUSIONS RELATIVE TO CIRCUIT FAILURE TYPES:

Despite the body of evidence from the NRC and Industry cable fire testing supporting the acceptability of the approach outlined in NEI 00-01 Revision 1, adjustments to the Revision 1 criteria will be made in Revision 2 to address those aspects of the NRC and Industry cable fire testing that suggest a change is warranted to increase the level of conservatism. The conclusions relative to the types of fire-induced circuit failures required to be considered in the deterministic post-fire SSA outlined in Revision 2 to NEI 00-01 are contained in Table B.1-0.

Based on the results of the cable fire testing, however, consideration of MSOs for selected cables and components may be warranted. Appendix G to NEI 00-01 provides a list of the MSOs that should be considered in a post-fire SSA.

B.6 CONCLUSIONS RELATIVE TO CIRCUIT TYPES:

The conclusions relative to the types of fire-induced circuit failures required to be considered in the deterministic post-fire SSA outlined in Revision 2 to NEI 00-01 for each circuit type are contained in Table B.2-0.

B.7 CONCLUSIONS:

The criteria provided in Table B.1-0 to this appendix describe the types of fire-induced circuit failures that need to be considered in a deterministic post-fire SSA. The information in Table B.2-0 provides information on how each of the fire-induced circuit failures described in Table B.1-0 needs to be considered in evaluating the impact of fire-induced circuit failures on a safe shutdown components control and power circuitry. The criteria provided in Table B.1-0, when combined with the information in Table B.2, provide a comprehensive method for assessing the response of an individual component to any fire-induced circuit failure. The information in Appendix G, MSOs, provides the criteria for combining the impacts to individual components into potential system and safe shutdown path impacts. The component level fire-induced circuit failure criteria, when combined with the information from Appendix G, MSOs, provides the criteria to assess the overall impact of fire on post-fire safe shutdown in a given fire area.

The overall conclusions of this appendix are as follows:

- Based on the review performed herein, neither the CAROLFIRE nor the EPRI/NEI Cable Functionality Tests yielded results that are drastically different than the collective wisdom available prior to the testing. In fact, it could be concluded that the results validated the positions held within the industry and documented in NEI 00-01 Revision 1 prior to the testing. Despite this, certain adjustments related to the treatment of multi-

conductor cables, as outlined in Tables B.1-0 and B.2-0, as outlined in Appendix G to NEI 00-01 Revision 2, will enhance the level of safety and add conservatism to the post-fire SSA.

- A clear design criteria for addressing fire-induced circuit failures in a post-fire SSA has not been provided in any NRC correspondence on the topic, including the proposed draft generic letter.
- Clear design criteria is need prior to any licensee being able to assess the level to which compliance is achieved.
- The driving need identified by the NRC for requiring a change in the current circuit failure criteria applied in the post-fire SSA is based on the information contained in NRC IN 99-17, the CAROLFIRE Cable Fire Testing Program and the EPRI/NEI Cable Functionality Fire Tests conducted in 2001. None of these sources provided an indication that multiple fire-induced spurious operation is likely.
- An independent and objective review of the information provided related to these two topics has been unable to identify a need for the changes proposed in draft NRC Generic Letter 2006-XX.
- A more plausible and effective way of addressing the issues identified in NRC IN 99-17, the CAROLFIRE Cable Fire Testing Program and the EPRI/NEI Cable Functionality Fire Tests would be to adopt the circuit failure criteria proposed in NEI 00-01 Revision 2.

Table B.1-0

Changes from Revision 1 to Revision 2 of NEI 00-01 based on NRC & Industry Cable Fire Testing

Discussion:

The criteria provided below describes the types of fire-induced circuit failures that need to be considered in a deterministic post-fire SSA. The information in Table B.2-0 provides information on how each of the fire-induced circuit failures described below needs to be considered in evaluating the impact of fire-induced circuit failures on a safe shutdown components control and power circuitry. The criteria provided below, when combined with the information in Table B.2-0, provides a comprehensive method for assessing the response of an individual component to any fire-induced circuit failure. The information in Appendix G, MSOs, provides the criteria for combining the impacts to individual components into potential system and safe shutdown path impacts. The component level fire-induced circuit failure criteria, when combined with the information from Appendix G, MSOs, provides the criteria to assess the overall impact of fire on post-fire safe shutdown in a given fire area.

The evaluation provided below begins with the current version of NEI 00-01 which is Revision 1. Using the insights gained from the NRC and Industry Cable Fire Testing, the table below shows how the original requirements of NEI 00-01 Revision 1 will be adjusted for inclusion into Revision 2 of NEI 00-01. The adjustments made to the fire-induced circuit failure criteria and the assumptions regarding the timing of damage to the individual circuits of concern are based on the results of the NRC and Industry Cable Fire Testing.

Cable Failure Type	NEI 00-01 Revision 1	NRC & Industry Test Results	NEI 00-01 Revision 2	Comments
Power Cables				
MHIF	Recommended elimination of need to address	No indication that these can occur in the combinations required to present a concern	Not Required to be included in a post-fire SSA.	Appendix B-1 provides additional justification for the industry position that consideration of multiple high impedance faults is not required. The results of the NRC & Industry cable fire testing reinforce the position outlined in Appendix B-1
3 phase hot shorts	Need to assess for Hi/Lo Pressure Interfaces	No indication that these can occur in the combinations required to present a concern	Need to assess for Hi/Lo Pressure Interface Valves only, due to the regulatory precedent for this issue.	Multiple hot shorts for high low pressure interface components are discussed in NRC Generic Letter 86-10. All licensees should have already addressed the 3-phase hot shorts on both hi/lo pressure interface valves simultaneously.
Proper polarity DC motor hot shorts	Need to assess for Hi/Lo Pressure Interfaces	No indication that these can occur in the combinations required to present a concern	Need to assess for Hi/Lo Pressure Interface Valves only, due to the regulatory precedent for this issue.	Multiple hot shorts for high low pressure interface components are discussed in NRC Generic Letter 86-10. All licensees should have already addressed the 3-phase hot shorts on both hi/lo pressure interface valves simultaneously.
Open Circuit	Need to assess for all safe shutdown components	No indication that these can occur, as a primary circuit failure	Need to assess for all safe shutdown components, due to the regulatory precedent for this issue.	10CFR 50 Appendix R Section III.G.2 requires consideration of open circuits.
Short-to-ground	Need to assess for all safe shutdown components. Need to assess for Associated Circuits – Common Power Supply.	Will occur as a primary circuit failure or as a sequel to a hot short of limited duration	Need to assess for all safe shutdown components. Need to assess for Associated Circuits – Common Power Supply.	10CFR 50 Appendix R Section III.G.2 requires consideration of shorts-to-ground. NRC Generic Letter 81-12 requires consideration of the upstream effects of hot shorts under the requirements for Associated Circuits – Common Power Supply.
Control Cables				
Open Circuit	Need to assess for all safe shutdown components	No indication that these can occur, as a primary circuit failure	Need to assess for all safe shutdown components	10CFR 50 Appendix R Section III.G.2 requires consideration of open circuits.
Short-to-ground	Need to assess for all safe shutdown components	Will occur as a primary circuit failure or as a sequel to a hot short of limited duration	Need to assess for all safe shutdown components.	10CFR 50 Appendix R Section III.G.2 requires consideration of shorts-to-ground.

Table B.1-0

Changes from Revision 1 to Revision 2 of NEI 00-01 based on NRC & Industry Cable Fire Testing

Cable Failure Type	NEI 00-01 Revision 1	NRC & Industry Test Results	NEI 00-01 Revision 2	Comments
Hot short ²⁰ - generic without consideration of cable and/or raceway characteristics	Need to assess for all safe shutdown components. In all cases, assumes the hot short potential exists unless proven otherwise.	The potential for a hot short is determined not only by presence in the fire area of concern, but also based on a time/temperature and duration thresholds for each occurrence.	Need to assess for all safe shutdown components. Additionally, the duration of the hot short may be limited to 20 minutes. After 20 minutes the hot short may be assumed to go to ground. At this point, the effects of a short-to-ground must be evaluated and addressed.	Table B.2-0 provides the criteria for the number of hot shorts that need to be considered in each components control circuitry. Appendix G of NEI 00-01 provides the criteria for which combinations of equipment impacts must be considered on a component/system level to address the issue of MSOs.
Inter-cable hot short - thermoset	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Very limited potential of occurrence. Probability is very low compared to intra-cable hot shorts.	Need to assess for all safe shutdown components.	See footnote 1 below.
Inter-cable hot short - thermoplastic	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Very limited potential of occurrence. Probability is very low compared to intra-cable hot shorts.	Need to assess for all safe shutdown components.	See footnote 1 below.
Intra-cable hot short - thermoset	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Potential to occur, if cable is damaged, but actual likelihood of occurrence is a function of many variables such that a given time/temperature environment does not necessarily guarantee occurrence.	Need to assess for all safe shutdown components.	See footnote 1 below.
Intra-cable hot short - thermoplastic	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Potential to occur, if cable is damaged, but actual likelihood of occurrence is a function of many variables such that a given time/temperature environment does not necessarily guarantee occurrence.	Need to assess for all safe shutdown components.	See footnote 1 below.
Inter-cable hot short - armored cable	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	No occurrences identified.	Not required to be addressed.	See footnote 1 below.
Intra-cable hot short - armored cable	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Potential to occur, if cable is damaged, but actual likelihood of occurrence is a function of many variables such that a given time/temperature environment does not necessarily guarantee occurrence.	Need to assess for all safe shutdown components.	See footnote 1 below.
Inter-cable hot short	Need to assess for all safe shutdown	Not required	Not required	See footnote 1 below.

²⁰ Hot shorts need to be addressed either generically or they can be addressed based on the characteristics of the cable type or cable/raceway type using the information from the sub-types listed below. If the hot short is addressed in a way that it takes credit for the cable and/or raceway type associated with the cable, then the important characteristics of the assessment must be included in the design configuration control program. This is required to be done so that as future plant changes are made with the potential to affect these important characteristics of the cable and/or raceway, the important characteristics are either maintained or a re-review of the condition is performed should they be changed.

Table B.1-0

Changes from Revision 1 to Revision 2 of NEI 00-01 based on NRC & Industry Cable Fire Testing

Cable Failure Type	NEI 00-01 Revision 1	NRC & Industry Test Results	NEI 00-01 Revision 2	Comments
- raceway to raceway	components. Not specifically addressed, but included under the overall criteria for addressing a hot short.			
Intra-cable hot short - conduit	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Potential to occur, if cable is damaged, but actual likelihood of occurrence is a function of many variables such that a given time/temperature environment does not necessarily guarantee occurrence.	Need to assess for all safe shutdown components.	See footnote 1 below.
Inter-cable hot short - thermoset to thermoplastic	Need to assess for all safe shutdown components. Not specifically addressed, but included under the overall criteria for addressing a hot short.	Very limited potential of occurrence. Probability is very low compared to intra-cable hot shorts.	Need to assess for all safe shutdown components.	See footnote 1 below.
Instrument Cables				
Open Circuit	Need to assess for all safe shutdown components.	Not specifically tested.	Need to assess for all safe shutdown components.	Assuring selected instruments (Reference NRC IN 84-09) are protected from the effects of fire in each fire area is an effective strategy for addressing the effects of a hot short using this criteria.
Short-to-ground	Need to assess for all safe shutdown components.	Not specifically tested.	Need to assess for all safe shutdown components.	Assuring selected instruments (Reference NRC IN 84-09) are protected from the effects of fire in each fire area is an effective strategy for addressing the effects of a short-to-ground using this criteria.
Hot short	Need to assess for all safe shutdown components.	Not specifically tested.	Need to assess for all safe shutdown components.	Assuring selected instruments (Reference NRC IN 84-09) are protected from the effects of fire in each fire area is an effective strategy for addressing the effects of an open circuit using this criteria.

Table B.2-0

Types of Fire-induced Circuit Failure Required for each Circuit Type

Cable Type	Impact of a Single Fire-induced Circuit Failure of this type	Effect of Multiple/Simultaneous Circuit Failures	Required Number for this Type of Circuit ²¹	Comments
Power Circuits [either ac or dc – discussions below are for ac power circuits. Similar discussions apply to dc, except that only two hot shorts are required.]				
Hot Short	No impact from a single hot short on a 3 phase cables	Spurious Operation of a single component with 3 hot shorts of the proper polarity on a 3 phase cable	There is no need to consider a hot short on power circuits, except for hi/lo pressure interface valves where 3 hot shorts of the proper polarity must be assumed.	NRC Generic Letter 81-12 discusses hi/lo pressure interfaces. NRC Generic Letter 86-10 addresses hot shorts on 3 phase cables for hi/lo pressure interface valves
Short-to-ground	Loss of power and potential for tripping of upstream loads	No additional impacts from multiple/simultaneous shorts-to-ground	Consider a single short-to-ground on each conductor in each affected cable. Need to address Associated Circuits – Common Power Supply.	Loss of upstream loads is addressed by the requirement of Generic Letter 81-12 for Associated Circuits – Common Power Supply [i.e. breaker coordination]
Open Circuit	Loss of power	No additional impacts from multiple/simultaneous open circuits	Consider a single open circuit on each conductor in each affected cable.	This effect is bounded by the effects of a short-to-ground, since the short-to-ground causes a loss of power and has the potential to affect upstream loads.
Primary Control Circuit [either ac or dc – discussions below are for ac power circuits. Similar discussions apply to dc]				
Hot Short	Spurious operation of the component	Spurious operation of the component from different conductors and/or cables in the primary or a secondary circuit. In almost all cases, however, for this to occur input from a hot short in a secondary control circuit is required. (See comment to the right.)	<p>Consider an individual, single hot short on each conductor in each affected cable in the circuit. Consider the combined effects of hot shorts if conductors are located in the same multiconductor cable in the primary circuit.</p> <p>For ungrounded DC circuits, if it can be shown that only two hot shorts of the proper polarity without grounding could cause spurious operation, no further evaluation is necessary except for any cases involving High/Low pressure interfaces. [Ref. GL 86-10 Encl. 2 Question 5.3.1]</p> <p>For cases involving direct current (DC) control circuits, consider the potential spurious operation due to failures of the control cables (even if the spurious operation requires two concurrent hot shorts of the proper polarity, e.g., plus-to-plus and minus-to-minus), when the source and target conductors are each</p>	The input from a secondary control power circuit will require a hot short in that circuitry. Both the hot short in the primary and secondary control circuit must co-exist and once the hot short in the secondary control circuit goes to ground the effect of this hot short on the primary circuit will be eliminated. Assuming this condition of sequentially selected fire-induced circuit damage is of sufficiently low probability to be considered unrealistic and beyond the required design basis given the results of the NRC & Industry Cable Fire Testing

²¹ The criteria for hot shorts in this column may be adjusted using the information from Table B.1-0 for the hot short sub-types. If the information on a particular hot short is used, then the important characteristics of the assessment must be included in the design configuration control program. This is required to be done so that as future plant changes are made with the potential to affect these important characteristics of the cable and/or raceway, the important characteristics are either maintained or a re-review of the condition is performed should they be changed.

Table B.2-0

Types of Fire-induced Circuit Failure Required for each Circuit Type

Cable Type	Impact of a Single Fire-induced Circuit Failure of this type	Effect of Multiple/Simultaneous Circuit Failures	Required Number for this Type of Circuit ²¹	Comments
Short-to-ground	Loss of control power/function in grounded circuits	For ungrounded circuits an additional concurrent shorts-to-ground may be required in order to cause a loss of control power.	located in the same multiconductor cable." [Ref. RIS 2004-03 Rev. 1] Consider an individual, single short-to-ground on each conductor in each affected cable in a grounded circuit. Consider the combined effects of shorts-to-ground if conductors are located in the same multiconductor cable in the primary circuit. Additionally, either assume a second short-to-ground exists in an ungrounded circuit resulting in a loss of control power or evaluate for an actual fire-induced cable impact with the potential to cause the second short-to-ground in the fire area.	For ungrounded circuits, two shorts-to-ground are required for the loss of control power. The recommended approach either assumes or evaluates for a second short-to-ground causing a loss of control power in the components control circuit for ungrounded circuits.
Open Circuit	Loss of a single control function, e.g. loss of manual start/stop, loss of auto-start/stop, loss of indication	Loss of multiple functions within the control circuit, e.g. loss of manual start/stop, loss of auto-start/stop, loss of indication	Consider an individual, single open circuit on each conductor in each affected cable in the circuit. Consider the combined effects of open circuits if conductors are located in the same multiconductor cable in the primary circuit.	This effect is bounded by the effects of a short-to-ground. Typically losing a single control function, other than indication, is sufficient to require a mitigation strategy for the affected cable. The simultaneous loss of multiple control functions within a single cable does not make the situation more adverse from a post-fire safe shutdown perspective, i.e. if a manual starting or stopping of a pump is the required safe shutdown function, assuming both occur simultaneously is no worse than assuming each occurs individually.
Secondary Control Circuits, including instrument signals to primary and secondary control circuits (either ac or dc - discussions below are for ac power circuits. Similar discussions apply to dc)				
Hot Short	Spurious operation of a primary component provided the contact that is closed has this direct effect on the primary circuit.	Spurious operation of a primary component provided the contacts that are closed have this direct effect on the primary circuit.	Consider an individual, single hot short on each conductor in each affected cable in the circuit. Consider the combined effects of hot shorts if conductors are located in the same multiconductor cable in the secondary circuit. For ungrounded DC circuits, if it can be shown that only two hot shorts of the proper polarity without grounding could cause spurious operation, no further evaluation is necessary except for any cases involving High/Low pressure interfaces. [Ref. GL 86-10 Encl. 2 Question 5.3.1]	The input from a secondary control power circuit will require a hot short in that circuitry. The hot short in the secondary control circuit must either have a direct effect on the primary circuit or it must co-exist with another hot short in the primary circuit. Once the hot short in the secondary control circuit goes to ground the effect of this hot short on the primary circuit will be eliminated. If, however, the component controlled by the primary circuit has already changed position, the spurious operation will not be reversed by the elimination of the hot short in the secondary circuit. Depending on the damage to the primary circuit by other fire-induced effects, reversal of the position of the spuriously operated component may be possible. For multiple hot shorts within secondary circuit to cause a spurious operation of the component controlled by the primary circuit, the

Table B.2-0

Types of Fire-induced Circuit Failure Required for each Circuit Type

Cable Type	Impact of a Single Fire-induced Circuit Failure of this type	Effect of Multiple/Simultaneous Circuit Failures	Required Number for this Type of Circuit ²¹	Comments
			<p>For cases involving direct current (DC) control circuits, consider the potential spurious operation due to failures of the control cables (even if the spurious operation requires two concurrent hot shorts of the proper polarity, e.g., plus-to-plus and minus-to-minus), when the source and target conductors are each located in the same multiconductor cable." [Ref. RIS 2004-03 Rev. 1]</p> <p>If multiple hot shorts in multi-conductor cables associated with secondary circuits can directly result in a spurious operation of a primary component that cannot occur due to a single hot short in the secondary circuit, then this must be addressed, unless the effect can be overridden by the operator in the Control Room. In making the determination about the operator's ability to override the effect of the multiple hot shorts in the secondary circuit, if an additional fire-induced circuit failure in a separate cable is required to defeat the operator capability, then it may be assumed that the override capability is available when needed by the operator.</p>	<p>multiple hot shorts must co-exist and either have a direct effect on the primary circuit or co-exist with another hot short in the primary circuit. This condition of sequentially selected fire-induced circuit damage is of sufficiently low probability to be considered unrealistic and beyond the required design basis given the results of the NRC & Industry Cable Fire Testing, except for the case of multi-conductor cables in secondary circuits that have a direct effect on the primary circuit and that cannot be overridden by an operator action in the Control Room without assuming any additional fire-induced circuit failures on a different cable.</p>
Short-to-ground	Loss of control power/function in grounded circuits	For ungrounded circuits an additional concurrent shorts-to-ground may be required in order to cause a loss of control power.	<p>Consider an individual, single short-to-ground on each conductor in each affected cable in a grounded circuit. Consider the combined effects of shorts-to-ground if conductors are located in the same multiconductor cable in the secondary circuit.</p> <p>Additionally, either assume a second short-to-ground exists in an ungrounded circuit resulting in a loss of control power or evaluate for an actual fire-induced cable impact with the potential to cause</p>	For ungrounded circuits, two shorts-to-ground are required for the loss of control power. The recommended approach either assumes or evaluates for a second short-to-ground causing a loss of control power in the components control circuit for ungrounded secondary circuits.

Table B.2-0

Types of Fire-induced Circuit Failure Required for each Circuit Type

Cable Type	Impact of a Single Fire-induced Circuit Failure of this type	Effect of Multiple/Simultaneous Circuit Failures	Required Number for this Type of Circuit ²¹	Comments
			the second short-to-ground in the fire area.	
Open Circuit	Loss of control function	No additional impacts from multiple/simultaneous open circuits.	Consider an individual, single open circuit on each conductor in each affected cable in the circuit.	This effect is bounded by the effects of a short-to-ground.
Control Power to Primary and Secondary Control Circuits (either ac or dc – discussions below are for ac power circuits. Similar discussions apply to dc)				
Hot Short	No impact on the circuit	No impact on the circuit	There is no need to consider hot shorts on control power to primary or secondary control circuits. It is unacceptable and non-conservative to assume that a hot short results in the availability of control power to a primary or secondary control circuit.	
Short-to-ground	Loss of control power/function with the potential for tripping of upstream loads	No additional impacts from multiple/simultaneous shorts-to-ground	Consider a single short-to-ground on each conductor in each affected cable. Assume a single short-to-ground in an ungrounded circuit results in a loss of control power.	
Open Circuit	Loss of control function	No additional impacts from multiple/simultaneous open circuits.	Consider a single open circuit on each conductor in each affected cable.	
Instrument Circuits				
Hot Short	Erroneous reading	No additional impact due to multiple hot shorts.	Consider an individual, single hot short on each conductor in each affected cable in the circuit. For instruments performing a control function, assume the signal affects the respective contact in the control circuit in a worst case manner for safe shutdown.	To address this for instruments providing an indication only function, for each fire area identify the specific instrumentation that is protected from the effects of fire. Capture this information in the post-fire safe shutdown procedure so that the operator can distinguish an erroneous fire-induced reading from a valid reading based by looking at the protected instrumentation. For instruments performing a control function, assume the signal affects the respective contact in the control circuit in a worst case manner for safe shutdown.
Short-to-ground	Loss of reading or control function	No additional impacts from multiple/simultaneous shorts-to-ground	Consider an individual, single short-to-ground on each conductor in each affected cable in a grounded circuit.	Assuring selected instruments (Reference NRC IN 84-09) are protected from the effects of fire in each fire area is an effective strategy for addressing the effects of a short-to-ground.
Open Circuit	Loss of reading or control function	No additional impacts from multiple/simultaneous open circuits.	Consider an individual, single open circuit on each conductor in each affected cable in the circuit.	Assuring selected instruments (Reference NRC IN 84-09) are protected from the effects of fire in each fire area is an effective strategy for addressing the effects of an open circuit.

APPENDIX B.1

JUSTIFICATION FOR THE ELIMINATION OF MULTIPLE HIGH IMPEDANCE FAULTS

B.1-1 PURPOSE

This appendix is provided to demonstrate that the probability of Multiple High Impedance Faults (MHIFs) is sufficiently low such that they do not pose a credible risk to post-fire safe shutdown when certain criteria are met.

This appendix analyzes and characterizes cable fault behavior with respect to the MHIF concern to determine if and under what conditions this circuit failure mode poses a credible risk to post-fire safe shutdown. In this capacity, the MHIF analysis is intended to serve as a generic analysis for a *Base Case* set of conditions. The base case approach is recognized as a viable means of establishing specific boundary conditions for applicability, thereby preserving the integrity of the analysis.

B.1-2 INTRODUCTION

B.1-2.1 Overview

In 1986 the NRC issued Generic Letter 86-10 [1] to provide further guidance and clarification for a broad range of 10 CFR 50 Appendix R issues. Included in the generic letter was confirmation that the NRC expected utilities to address MHIFs as part of the Appendix R associated circuits analysis.²² MHIFs are a unique type of common power supply associated circuit issue, as discussed in Section B.1-2.2 below.

Regulatory Guide 1.189 (Section 5.5.2) [2] reiterates the NRC's position that MHIFs should be considered in the evaluation of common power supply associated circuits. Of importance is the regulatory guide's endorsement of IEEE Standard 242, *IEEE Recommended Practices for Protection and Coordination of Industrial and Commercial Power Systems*, [7] as an acceptable means of achieving electrical coordination of circuit

²² A general discussion of associated circuits is contained in Section 2.2 and 3.3.2 of this guidance document. NRC intends that a future generic communication will clarify associated circuits.

protective devices. Confirmation of adequate electrical coordination for safe shutdown power supplies is the primary means of addressing common power supply associated circuits.

B.1-2.2 Defining the MHIF Concern

The MHIF circuit failure mode is an offshoot of the common power supply associated circuit concern. A common power supply associated circuit is considered to pose a risk to safe shutdown if a fire-induced fault on a non-safe shutdown circuit can cause the loss of a safe shutdown power supply due to inadequate electrical coordination between upstream and downstream overcurrent protective devices (e.g., relays, circuit breakers, fuses).

The accepted method for evaluating the potential impact of common power supply associated circuits is a *Coordination Study*. A coordination study involves a review of the tripping characteristics for the protective devices associated with the electrical power distribution equipment of concern – post-fire safe shutdown power supplies in this case. The devices are considered to “coordinate” if the downstream (feeder or branch circuit) device trips before the upstream (supply circuit) device over the range of credible fault current.²³ In conducting a traditional coordination study, each circuit fault is evaluated as a single event.

The concept of MHIFs deviates from baseline assumptions associated with conventional electrical coordination. The MHIF failure mode is based on the presumption that a fire can cause short circuits that produce abnormally high currents that are below the trip point of the individual overcurrent interrupting devices for the affected circuits. Faults of this type are defined by Generic Letter 86-10 as *high impedance faults* (HIFs). Under the assumed conditions, circuit overcurrent protective devices will not detect and interrupt the abnormal current flow. Consequently, the fault current is assumed to persist for an indefinite period of time. Since HIFs are not rapidly cleared by protective devices, the NRC position is that simultaneous HIFs should be considered in the analysis of associated circuits. The specific concern is that the cumulative fault current resulting from multiple simultaneous HIFs can exceed the trip point of a safe shutdown power supply incoming protective device, causing it to actuate and de-energize the safe

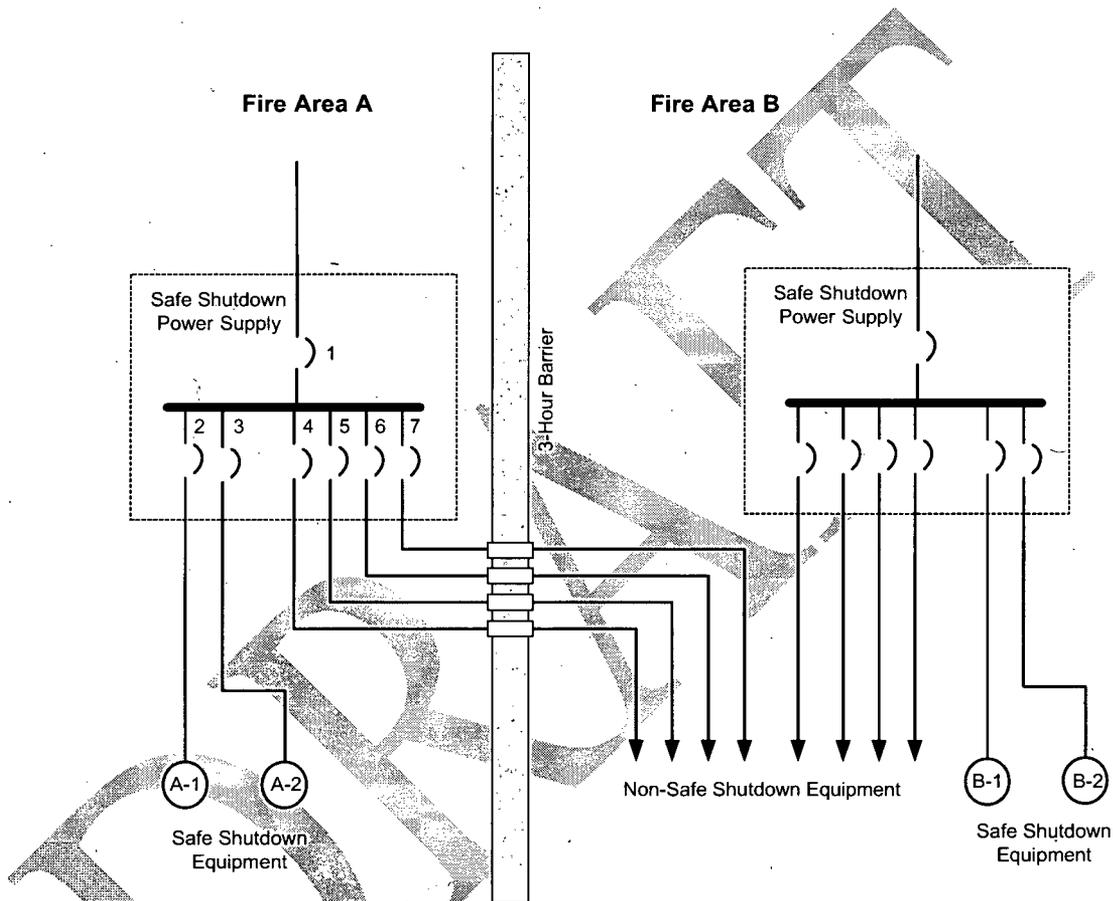
²³ The range of credible fault current includes short circuit current levels up to the maximum possible fault current for the configuration. For simplicity, the maximum credible fault current is usually based on a bolted fault at the downstream device. However, in some cases the maximum credible fault current is refined further by accounting for additional resistance of the cable between the downstream device and the fault location of concern.

shutdown power supply before the downstream (load-side) protective devices clear individual circuit faults.

Figure B.1-1 illustrates the MHIF failure mode. Note that the description of MHIFs assumes that redundant safe shutdown equipment is affected by the postulated fire. Detailed reviews can be conducted to determine exactly which cables and scenarios are potentially susceptible to MHIFs. However, this type of "spatial" analysis typically involves a highly labor-intensive effort to trace the routing of hundreds of non-safe shutdown cables. Furthermore, ongoing configuration control of such analyses is overly burdensome. For this reason, the preferred means of addressing the issue is at a system performance level, independent of cable routing. The systems approach offers a great deal of conservatism because, in actuality, not all circuits will be routed through every fire area and not all circuits are non-safe shutdown circuits.

DRAFT

Figure B.1-1
Example MHIF Sequence



Safe shutdown components A-1 and B-1 are redundant, as are A-2 and B-2. A fire in Fire Area B is assumed to render B-1 and B-2 inoperable, and thus A-1 and A-2 are credited as available for safe shutdown. Circuit Breakers 4 – 7 supply non-safe shutdown equipment via circuits that traverse Fire Area B. The fire is assumed to create high impedance faults on several of these circuits simultaneously. The nature of the faults is such that an abnormal current is produced in each circuit, but in each case the current is not sufficient to cause the affected branch feeder breaker to trip. The cumulative effect of the fault current flowing in each branch causes the incoming supply breaker (Circuit Breaker 1) to trip before the downstream breakers are able to isolate the individual faults. The safe shutdown power supply is de-energized, causing a loss of power to the credited safe shutdown equipment, A-1 and A-2.

B.1-2.3 Framework for Resolution

From inception, debate has persisted regarding the technical validity of MHIFs. The NRC's concern with MHIFs can be traced to a November 30, 1984, NRC internal correspondence [3]. The stated purpose of the correspondence was to "...present one paper which can be used in the evaluation of safe shutdown submittals." The paper describes the MHIF issue as an "...expansion on associated circuits" and describes the concern in much the same manner as covered in Section B.1-2.2 above. Noteworthy is that the document limits the issue to AC power circuits. The NRC's concern with MHIFs on AC power circuits does not appear to stem from any specific test data or operating experience. Rather, the concern is voiced as one of conservative judgment for a postulated failure mode in the absence of definitive information to the contrary.

With this understanding as a starting point, the framework for addressing the MHIF issue is based on the following tenets:

- A *Base Case* set of conditions must be defined to ensure the limits of applicability are bounded. Within the defined limits, the MHIF analysis serves as a generic evaluation and is considered to satisfy the regulatory requirement that high impedance faults be considered in the analysis of associated circuits.
- To ensure consistency and agreement in the fundamental bases for analysis, technical positions should be based on and referenced to test results, industry consensus standards, and NRC generated or approved documents. Test data and technical references must be representative of the *Base Case*.
- Elements of the analysis may be probabilistically-based and employ risk-informed arguments. This approach is deemed acceptable within the framework of a deterministic analysis and is not without precedent.²⁴ However, consistent with risk-informed decision making, consequence of failure shall be addressed by

²⁴ Generic Letter 86-10, Question 5.3.1 excludes on the basis of low probability the need to consider three-phase hot shorts and proper polarity hot shorts for ungrounded DC circuits in the analysis of spurious actuations (except for high/low pressure interfaces).

the

analysis.

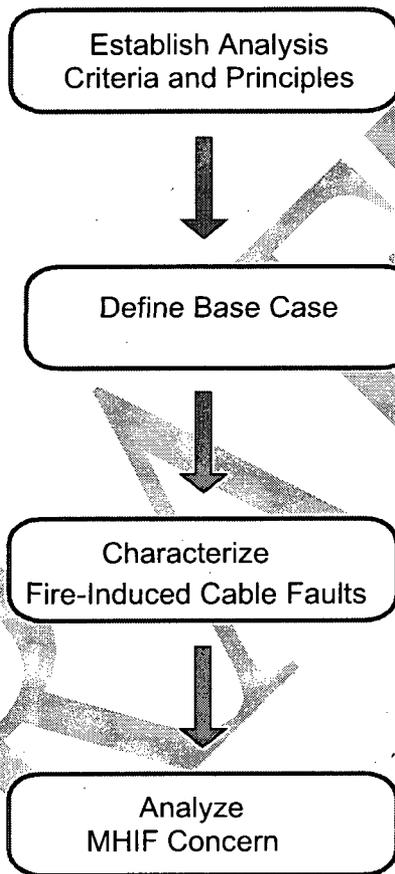
- Analysis uncertainty must be included in the evaluation to ensure conservative application of results.

B.1-3 ANALYSIS METHOD AND APPROACH

The approach for conducting this analysis is depicted by the flow chart of Figure B.1-2. A brief description of each step is provided. The most important aspect of this analysis is the ability to characterize fire-induced cable faults. Research and test data to accomplish this characterization for all voltage levels of interest has until recently been scant, forcing past assessments of MHIFs (both industry and NRC assessments) to make assumptions and extrapolate theories beyond a point that achieved general agreement. Test data from recent industry and NRC fire testing [3, 12] allows fault behavior to be characterized at a level not previously possible. Interpretation of test data and application of analysis results will follow accepted and prudent engineering principles, as set forth by consensus standards and other acknowledged industry references.

DRAFT

Figure B.1-2
MHIF Analysis Flow Chart



Step 1 – Establish Analysis Criteria and Principles: Analysis criteria and relevant engineering principles are identified. The rationale behind the analysis criteria is explained and the engineering principles relied upon to evaluate results are documented.

Step 2 – Define Base Case: A base case set of conditions is defined. These conditions establish the limits of applicability for the analysis.

Step 3 – Characterize Fire-Induced Cable Faults: Relevant fire test data and engineering research are analyzed to characterize fire-induced cable faults. Recent industry and NRC fire tests, as well as other credible industry tests and research studies, are considered in the evaluation.

Step 4 – Analyze MHIF Concern: The characteristic behavior of fire-induced faults is considered within the context of the MHIF concern to determine if and under what conditions MHIFs pose a credible risk to post-fire safe shutdown for the defined *Base Case* conditions. Analysis uncertainty is included in the evaluation.

B.1-4 ANALYSIS CRITERIA AND PRINCIPLES

The criteria and engineering principles that form the basis of this analysis are discussed below.

1. The legitimacy of the MHIF concern is centered on the premise that a fire can create HIFs that are not readily detected and cleared by the intended overcurrent protective device [1, 4]. Thus, characterizing the expected behavior of fire-induced faults is paramount in determining the potential risk posed by this failure mode. If fires are able to initiate faults that “hang up” and produce low-level fault currents (near or just below the trip device setting) for extended periods, MHIFs should be considered a viable failure mode. If, however, the faults do not exhibit this behavior, but instead reliably produce detectable fault current flow, a properly designed electrical protection scheme can be relied upon to clear the fault in a timely manner in accordance with its design intent. Based on this principle, the primary line of inquiry for this analysis is to quantitatively characterize fault behavior for the voltage classes of interest. Analysis uncertainty will be included in the assessment to further quantify the results.
2. MHIFs are not usually considered in the design and analysis of electrical protection systems, primarily because operating experience has not shown them to be a practical concern [6, 7, 10]. For this reason, industry has not established nor endorsed any particular analytical approach for MHIFs. Acknowledging the lack of consensus industry standards and conventions, this analysis relies on objective evidence and the application of recognized engineering principles; however, some element of engineering judgment is inevitable because of the unconventional nature of the analysis.

3. As constrained by the *Base Case* requirements, this analysis is considered sufficiently representative of nuclear plant electrical power system and protective device design, construction, and operation:
 - Regardless of make, model, or vintage, electrical protective devices conforming to the *Approval*, application, and test/maintenance requirements specified for the *Base Case* can be expected to function in the manner credited by this analysis [5, 7, 9].
 - Electrical power systems satisfying the design and performance requirements specified for the *Base Case* will respond to electrical faults in the manner assumed by this analysis [6, 7, 10].
4. This analysis assumes that electrical protection and coordination have been achieved following the guidance of ANSI/IEEE 242, or other acceptable criteria. Regulatory Guide 1.189 recognizes this ANSI standard as the primary reference for this subject. A more detailed investigation into supporting references listed by the standard reveals a substantial number of tests and research studies that have applicability to this MHIF analysis [13 – 22]. These documents provide additional insight into the expected behavior of high resistance electrical faults and accordingly are considered by this analysis. As these documents have essentially shaped the engineering basis for the ANSI/IEEE 242 recommended practices, they are considered viable and credible source references for this analysis.
5. The test data obtained from the recent industry and NRC tests [3, 7] is considered directly applicable to nuclear plant installations. The test parameters (including test specimens, circuit configuration, and physical arrangement) were specifically tailored to mimic a typical nuclear plant installation. The overall test plan was scrutinized by utility and NRC experts before implementation.
6. The actual impedance of a fault can vary widely and depends on many factors. These factors include such things as fault geometry, system characteristics, environmental conditions, and the circumstances causing the fault. Different fault impedances produce different levels of fault current; hence, electrical coordination studies generally consider a range of credible fault currents [7]. Circuit faults resulting from fire damage are highly dynamic, but do exhibit a predictable and repeatable pattern that can be characterized and explained by engineering principles and an

understanding of material properties. The same general characteristics have been observed by several different tests and studies [3, 12, 13 – 22].

7. The primary test data relied upon for this MHIF analysis is the recent nuclear industry and NRC fire tests [3, 12]. The electrical circuits for these tests were 120 V, single-phase, limited-energy systems. The analytical results for the 120 V data indicate these low energy circuits behave differently than high-energy circuits operating at distribution level voltages. The bases for this position are:
 - The ability of electrical system hardware to sustain and withstand local fault conditions decreases as the fault energy increases. Highly energetic faults on systems operating above 208 V release tremendous amounts of energy at the fault location. These faults are explosive in nature and will destroy equipment in a matter of seconds, as confirmed by recent industry experience. Conversely, fault energy associated with 120 V, single-phase systems is considerably less punishing to the equipment and will not necessarily cause immediate wide-spread damage.
 - Test results from the recent industry and NRC fire tests confirm a correlation between the rate of localized insulation breakdown and the available energy (applied voltage gradient and available fault current). For example, once insulation degradation began, the rate of breakdown for instrument cable was notably slower than the rate observed for cables powered by 120 V laboratory power supplies. The lower energy circuits are less able to precipitate the cascading failure of insulation that characteristically occurs during the final stages of insulation breakdown because the rate of energy transfer to the fault is lower. The final cascading failure of a 480 V power circuit can be expected to occur within milliseconds, where the final stage of insulation failure for a 120 V circuit might last several seconds, as demonstrated by the test results. Note that the final cascading failure is typically preceded by a period of much slower insulation degradation. During this phase of degradation, the cable can be expected to exhibit higher levels of leakage current; however, the leakage current levels are not sufficiently high to affect proper operation of power and control circuits. The point at which the slow, low-level degradation transitions to rapid breakdown and failure is termed the transition phase. (Cable failure characteristics are discussed in detail in Section B.1-6.1.)

- Arcing faults become increasingly more likely as system voltage increases because of the higher voltage gradient and longer creepage distances.²⁵ The “effective” current for arcing faults increases as a function of the applied voltage. A higher fault current will hasten the time for protective action. (The arcing fault phenomena are discussed in detail in Section B.1-6.2.)
8. High impedance faults on conductors of power systems operating at 480 V and above manifest themselves as arcing faults [13 – 22]. Thus, the analysis of postulated HIFs for these systems assumes an arcing fault (detailed discussion contained in Section B.1-6.1). The bases for this position are:
- With respect to cables, distances between energized conductors and between energized conductors and grounded surfaces are not appreciably different from 120 V systems. Thus, as insulation integrity is lost, the high voltage gradient associated with these systems more readily strikes an arc in the absence of a sufficient air gap.
 - As discussed in Item 7 above, the highly energetic nature of faults on higher voltage power systems results in a significant release of energy at the fault location, which rapidly elevates localized temperatures to vaporization levels. This large release of energy at the fault manifests itself in one of three ways:
 - Metal components are fused, thereby creating a bolted fault.
 - Material is vaporized and forcibly ejected, blowing the fault open
 - Material is vaporized and ejected, but the conductive vapor cloud allows an arcing fault to develop, which may or may not be sustained
 - The electrical power industry conducted numerous studies and tests pertaining to faults on high energy electrical power systems in the 1960s and 1970s. These efforts were sparked by a rash of significant property losses and extensive outages resulting from highly damaging electrical faults. These studies significantly increased our understanding of high energy faults and resulted in numerous changes to recommended electrical protection practices (primarily IEEE 242). High impedance, non-arcing faults were not observed by these studies.

²⁵ Creepage distance is defined as the shortest distance between two conducting parts measured along the surface of the insulating material.

B.1-5 BASE CASE AND APPLICABILITY

The intent of defining a *Base Case* is to establish set limits for application of the analysis results. This approach places measurable bounds on the analysis and ensures results are not inadvertently applied to conditions not considered in the study.

The following requirements constitute the *Base Case* conditions inherent in this analysis:

- The power supply in question must operate at a nominal AC or DC voltage greater than 110 V. Specifically, this analysis does not apply to AC and DC control power systems operating at 12 V, 24 V, or 48 V. Nor is the analysis applicable to instrument loops regardless of operating voltage.
- For the power supply in question, electrical coordination must exist between the supply-side overcurrent protective device(s) and load-side overcurrent protective devices of concern²⁶. Achievement of proper selective tripping shall be based on the guidance of IEEE 242, or other acceptable criteria.
- For 120 V AC and 125 V DC power supplies, in addition to adequate electrical coordination, a minimum size ratio of 2:1 shall exist between the supply-side protective device(s) and load-side devices of concern (for example, a distribution panel with a 50 A main circuit breaker cannot have any load-side breakers larger than 25 A). This stipulation adds additional margin to account for slower protective device clearing times of low-energy circuits.
- The electrical system must be capable of supplying the necessary fault current for sufficient time to ensure predictable operation of the overcurrent protective devices in accordance with their time-current characteristics.
- Each overcurrent protective device credited for interrupting fault current shall:

²⁶ Coordination is not required for circuits that are inherently not a common power supply associated circuit of concern – for example, a circuit that is entirely contained within the same fire area as the power supply itself. Similarly, coordination is only required up to the maximum credible fault current for the configuration, which might include an accounting of cable resistance between the load-side protective device and the fault location of concern.

- Be applied within its ratings, including voltage, continuous current, and interrupting capacity
 - Be *Listed* or *Approved* by a nationally recognized test laboratory (e.g., UL, ETL, CSA, etc.) to the applicable product safety standard (fuses, molded case circuit breakers, circuit protectors, GFI devices) or be designed and constructed in accordance with applicable ANSI and NEMA standards (protective relays, low and medium voltage switchgear)
- Proper operation of the overcurrent devices shall be ensured by appropriate testing, inspection, maintenance, and configuration control.

The electrical system associated with the power supply in question shall conform to a recognized grounding scheme. Recognized schemes include solidly grounded, high impedance or resistance grounded, or ungrounded.

B.1-6 CHARACTERIZATION OF FAULTS

B.1-6.1 Characterization of Fire-Induced Cable Faults for 120V Systems

This section contains an analysis of fault behavior for fire-induced faults on single-phase, 120 V systems. The primary source data for the analysis is recent industry and NRC fires tests conducted specifically to characterize fire-induced cable faults.

B.1-6.1.1 EPRI/NEI Fire Test Results

The EPRI/NEI fire tests are documented in EPRI Report 1003326, *Characterization of Fire-Induced Circuit Failures: Results of Cable Fire Testing* [12]. The functional circuits developed for this testing were heavily monitored, allowing significant insights into the nature and behavior of fire-induced cable faults.

B.1-6.1.1.1 Cable Failure Sequence

When driven to failure, cables followed a predictable and repeatable sequence. Initial degradation was first observed as a relatively slow reduction in insulation resistance down to approximately 10 k Ω – 1,000 Ω . At these levels the circuits remained fully functional and produced leakage current in the milliamp range. The next phase of degradation has been termed the *transition phase*. In the transition phase, the fault undergoes a cascade effect and the rate of insulation resistance (IR) degradation increases

significantly, causing fault resistance to drop rapidly. The circuit remains functional, but leakage current ramps upward quickly. The fault resistance associated with this phase is approximately 5 k Ω down to 600 Ω . Note that at 600 Ω the leakage current is only about 0.2 A, and the circuit is still functioning. The transition phase lasts from seconds to minutes. The final phase involves full failure of the cable. Insulation resistance drops to a very low level and leakage current now becomes fault current. The fault current escalates above the fuse rating, causing the fuse to open and de-energize the circuit. This final phase typically occurs within seconds or 10s of seconds for low-energy 120 V circuits. Figures B.1-3 and B.1-4 show current and fault resistance for a typical set of cables driven to failure.

Figure B.1-3
Fault Current for Fire-Induced Cable Failure

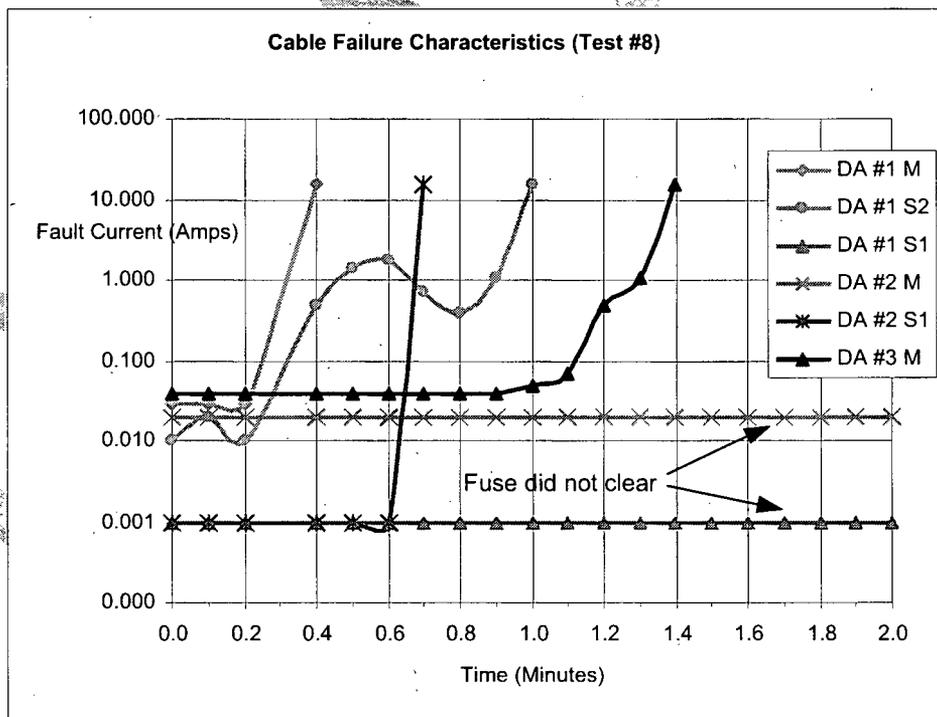
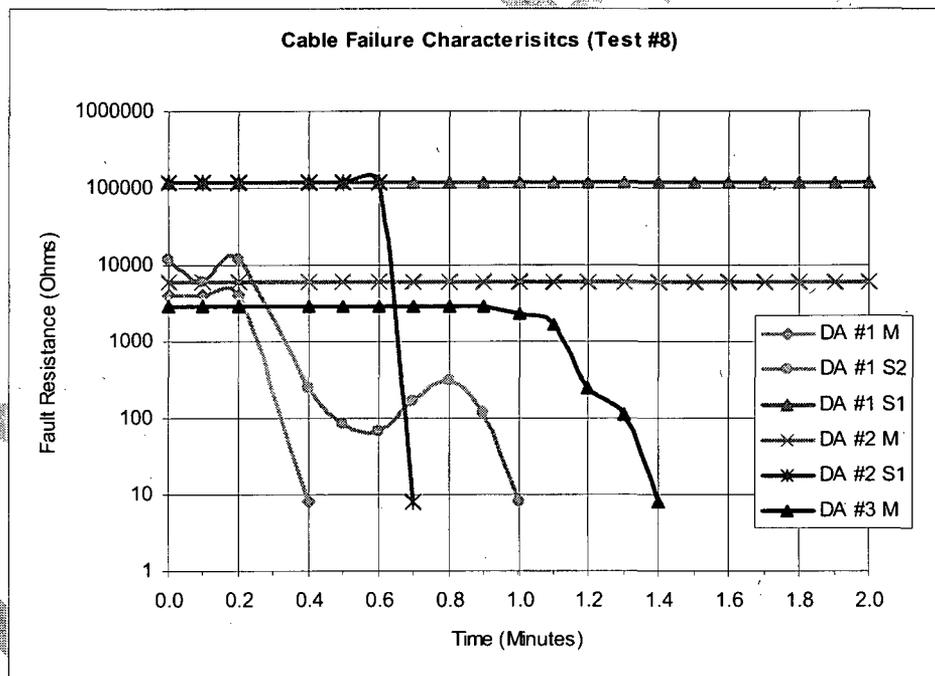


Figure B.1-4
Fault Resistance for Fire-Induced Cable Failure



The observed results can be explained by an understanding of the localized phenomena at the fault location. As the insulation degrades leakage current increases. At some point, the leakage current measurably contributes to localized heating, accelerating the rate of

insulation degradation. As current increases, the rate of degradation increases until it finally cascades to a full fault. Important in this observation is that the power source must be able to supply sufficient energy to drive the cascading effect to completion. Test circuits with limited current capacity demonstrated the same basic failure sequence; however, the final phase typically took longer and did not produce predictable final fault resistances. This behavior can be seen in the NRC/SNL data in which the test circuit was limited to 1.0 A. This observation leads to the *Base Case* condition that the power supply must be able to produce sufficient fault current to ensure the protective devices operate predictably.

A key observation of the failure characteristics is that once the insulation resistance enters the transition phase it does not "hang up" at an intermediate point; it cascades to full failure within seconds or 10s of seconds. From the data it appears that once leakage current exceeds about 0.2 A, the fault can be expected to cascade to levels that trigger protective action.

In a few cases this process was dynamic. The fault cascaded and produced a high fault current momentarily (a few seconds), but quickly subsided back to low levels. This cycle generally repeated itself two or three times before fault current ramped and remained high. Importantly, in no cases did fault current stabilize for an extended period at an intermediate level such that it was not detected and cleared by the fuse.

B.1-6.1.1.2 Fault Clearing Times

The fire test data was analyzed to establish a correlation between fault current level and the time required to clear the circuit fuse. The results of this tabulation are presented in Table B.1-1. The data here deals only with cases in which a fault caused the fuse to clear. Data for thermoset and thermoplastic cable are shown separately because the different insulation material exhibited slightly different characteristics.

The table provides statistics for the amount of time it took to clear the fuse once current had reached a certain threshold level. The clearing times are shown for three thresholds: 0.25 A, 1.0 A, and 2.0 A. The 0.25 A level was selected because it represents the approximate lower bound of the transition phase. 2.0 A was selected because it represents a current flow well below a value considered to pose a HIF concern for the established circuit. 1.0 A is an intermediate point that provides additional understanding.

The table is interpreted as follows: For thermoset cable, once fault current reached a level of 0.25 A, it took on average 0.46 minutes for the fuse to clear; once fault current reached 1.0 A it took on average 0.23 minutes to clear the fuse; and so on.

**Table B.1-1
 Fault Clearing Time**

Current Threshold	Time to Clear Fault (min)		
	0.25 A	1.0 A	2.0 A
Thermoset Cable			
Population	75	75	75
Average	0.46	0.23	0.14
Range	0.1 to 4.8	0.1 to 2.1	0.1 to 0.7
Std Dev	0.67	0.29	0.13
2 Std Dev	1.33	0.59	0.26
Thermoplastic Cable			
Population	39	39	39
Average	0.12	0.10	0.10
Range	0.1 to 0.3	0.1	0.1
Std Dev	0.07	0.00	0.00
2 Std Dev	0.14	0.00	0.00

The statistics presented in the table lend themselves to the following observations:

- The values contained in the table are highly conservative. The sample rate for the test monitoring system was limited to 0.1 min (6 sec). In many cases the fuse cleared between sample times. For these cases, the clearing time has been conservatively assigned a value of 0.1 min. This approach holds true for all values in that the maximum possible clearing time has been assigned. Inherent in this approach is that the analysis uncertainty associated with determining the statistical values is completely incorporated into the values.
- All cables that reached a minimum leakage current of 0.25 A ultimately cleared the fuse. This is evident in that the population for all three threshold currents is the same. This is an important observation because it demonstrates that once fault resistance has degraded to the transition point, the cascade effect dominates the ultimate outcome and the fault does not

then “hang up” at an intermediate resistance value that results in a prolonged abnormal low-level current flow.

- Once fault current surpassed 1.0 A, the cascade effect accelerated, as evidenced by the smaller delta between the 1.0 A to 2.0 A average and the 0.25 A to 1.0 A average.
- Once fault current for thermoset cable exceeded 2.0 A, the average clearing time was 0.14 min, with a 95% (2 standard deviations) upper bound of 0.4 min. From this it can be stated that 95% of the faults cleared within 24 sec.
- Thermoset cable fails much more quickly than thermoplastic cable.

B.1-6.1.1.3 Assessment of Probability

A different – and arguably better – way to tabulate the data is to determine the fraction of faults that were cleared by the fuse within a specified time. This tabulation is shown in Table B.1-2.

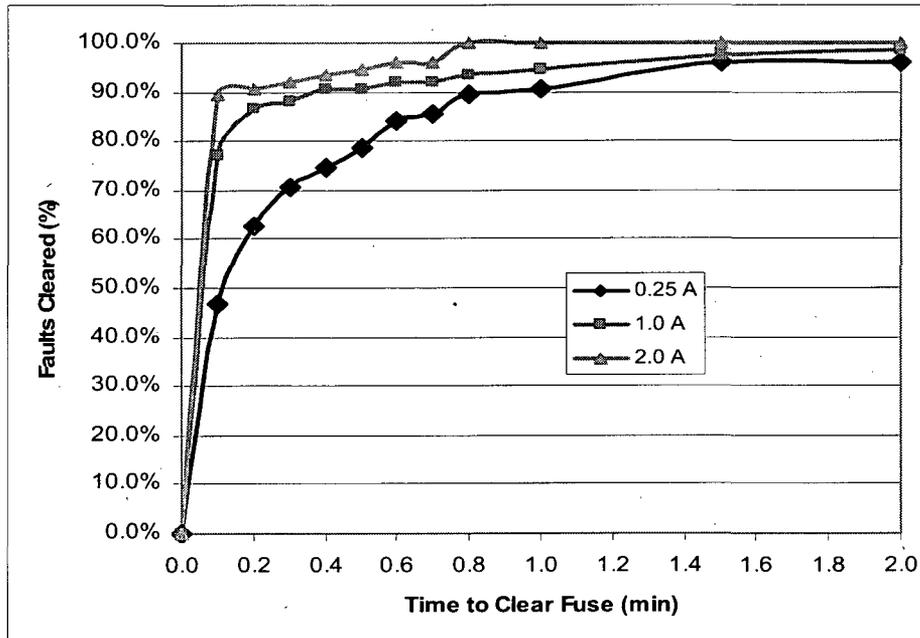
Viewed from this perspective, the data represents a go – no go or success – failure data set. In this format the data is readily analyzed in manner useful in addressing the MHIF concern. The table is interpreted as follows: For thermoset cable, once fault current reached a level of 0.25 A, 62.7% of the faults were cleared within 0.2 min; 78.7% of the faults were cleared within 0.5 min; and so on.

Table B.1-2
Probability of Clearing Faults Within a Specified Time

Time (min)	Percentage of Faults Cleared		
	0.25 A	1.0 A	2.0 A
Thermoset Cable			
0	0.0%	0.0%	0.0%
0.1	46.7%	77.3%	89.3%
0.2	62.7%	86.7%	90.7%
0.3	70.7%	88.0%	92.0%
0.4	74.7%	90.7%	93.3%
0.5	78.7%	90.7%	94.7%
0.6	84.0%	92.0%	96.0%
0.7	85.3%	92.0%	96.0%
0.8	89.3%	93.3%	100.0%
1.0	90.7%	94.7%	100.0%
1.5	96.0%	97.3%	100.0%
2.0	96.0%	98.7%	100.0%
Thermoplastic Cable			
0	0.0%	0.0%	0.0%
0.1	87.2%	100.0%	100.0%
0.2	94.9%	100.0%	100.0%
0.3	100.0%	100.0%	100.0%

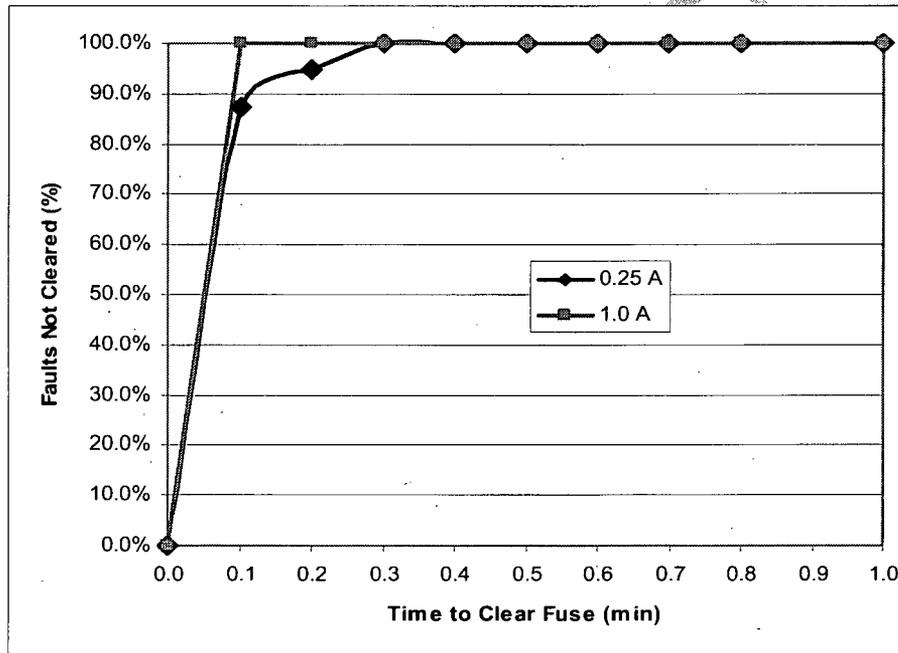
Figures B.1-5 and B.1-6 graphically illustrate the data contained in Table B.1-2.

Figure B.1-5
Percent Faults Cleared for Specified Time – Thermoset Cable



DRAFT

Figure B.1-6
Percent Faults Cleared for Specified Time – Thermoplastic Cable



The following observations can be made about the probability data:

- Faults for thermoplastic cable essentially degrade to full failure immediately. Given the limitations of the monitoring system sample rate (6 sec) and the conservative treatment of the data, it is suspected that the actual failure times are in the millisecond range and not seconds. On this basis the observations for thermoset cable are considered to bound the thermoplastic cable.
- Figure B.1-5 shows that the 1.0A curve is approaching the 2.0 A curve. This graphically illustrates that once current has surpassed the 1.0 A threshold, the cascade effect drives the outcome and full failure is inevitable. Again, with respect to the MHIF concern, this confirms that the inherent fault behavior does not support the concept that fault current can stabilize at some intermediate value. Once cascading

begins, the fault will progress to full failure, provided the system is capable of delivering sufficient energy to the fault.

- Once fault current reaches 2.0 A, 89% of the faults are cleared within 0.1 min and 100% of the faults are cleared within 0.8 min. Again, considering the limitations of the monitoring circuit, the actual times are less than indicated.
- From the 1A current threshold only one fault took longer than 2 min to clear – it cleared in 2.1 min.

B.2-6.1.1.4 Uncertainty Analysis

An uncertainty analysis of the data contained in Section B.1-6.1.1.3 is needed to establish a confidence level in the results. The dataset conforms to the requirements for a binomial distribution [23, 24], and thus a binomial confidence interval will be used to assess uncertainty. The confidence interval will be calculated at the 95% level. Only thermostat cable data is included in the calculation since it bounds the thermoplastic cable data.

The binomial confidence interval calculation is particularly punishing in this case because of the relatively small sample population and low number of failures. This factor adds additional margin to the calculated values of uncertainty.

The binomial confidence limits are calculated as follows:

$$P_l = 1 - \frac{x}{n} \pm z \sqrt{\left(\frac{1}{n}\right) x \left(\frac{x}{n}\right) x \left(1 - \frac{x}{n}\right)}$$

where: P_l = Probability confidence limits
 n = Sample population
 x = Number of observations failing criteria
 z = Desired confidence level factor (1.96 for 95%)

Table B.1-3 shows the calculated 95% confidence factors and Table B.1-4 shows the 95% lower confidence limit values for the dataset.

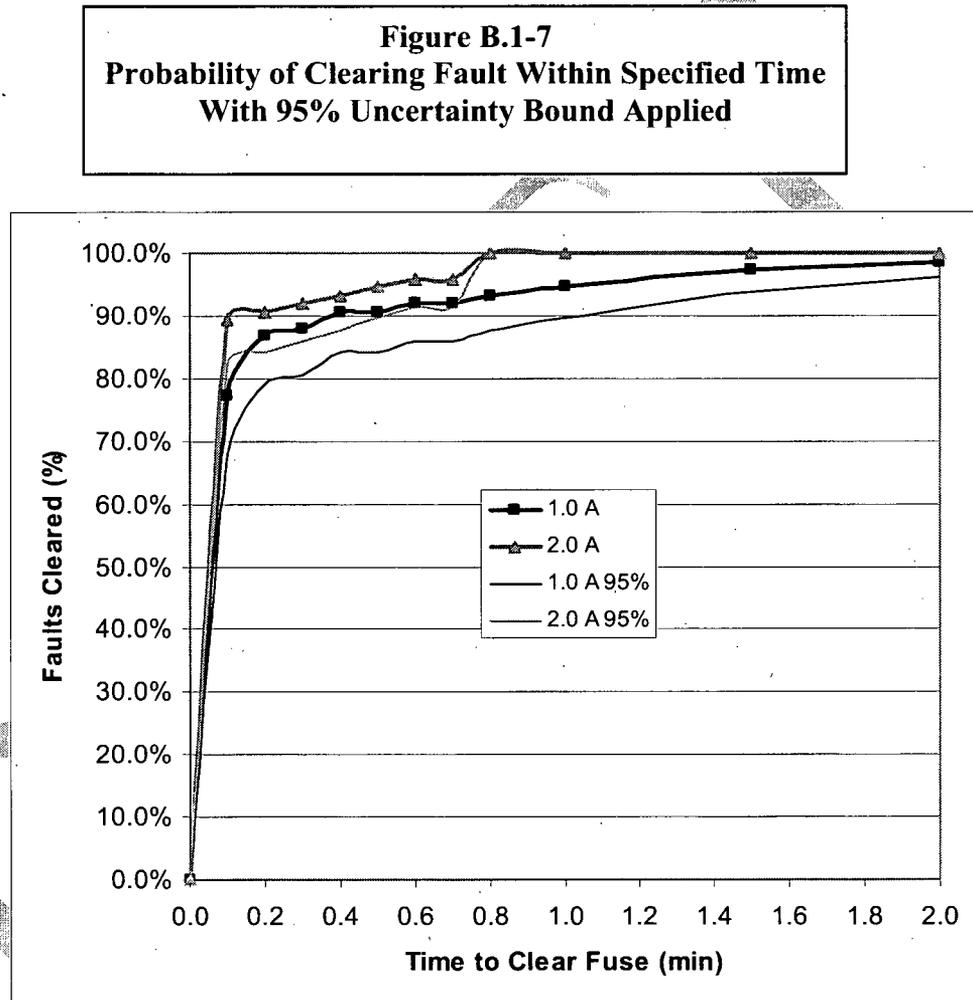
Table B.-3
Binomial Distribution 95% Confidence Factors

Time (min)	Binomial Distribution 95% Confidence Factors		
	0.25 A	1.0 A	2.0 A
0	0.0%	0.0%	0.0%
0.1	11.3%	9.5%	7.0%
0.2	10.9%	7.7%	6.6%
0.3	10.3%	7.4%	6.1%
0.4	9.8%	6.6%	5.6%
0.5	9.3%	6.6%	5.1%
0.6	8.3%	6.1%	4.4%
0.7	8.0%	6.1%	4.4%
0.8	7.0%	5.6%	0.0%
1.0	6.6%	5.1%	0.0%
1.5	4.4%	3.6%	0.0%
2.0	4.4%	2.6%	0.0%

Table B.1-4
Fault Clearing Time 95% Lower Confidence Limit

Time (min)	95% Lower Confidence Limit		
	0.25 A	1.0 A	2.0 A
0	0.0%	0.0%	0.0%
0.1	35.4%	67.9%	82.3%
0.2	51.7%	79.0%	84.1%
0.3	60.4%	80.6%	85.9%
0.4	64.8%	84.1%	87.7%
0.5	69.4%	84.1%	89.6%
0.6	75.7%	85.9%	91.6%
0.7	77.3%	85.9%	91.6%
0.8	82.3%	87.7%	100.0%
1.0	84.1%	89.6%	100.0%
1.5	91.6%	93.7%	100.0%
2.0	91.6%	96.1%	100.0%

Figure B.1-7 shows the 1.0 A and 2.0 A fuse clearing probabilities with the 95% confidence limits applied. Note that the $t = 0$ confidence limits have no real meaning since no fails have occurred at this point.



B.1-6.1.1.5 Leakage Current for Non-Failures

The data presented in Sections B.1-6.1.1.2 and B.1-6.1.1.3 demonstrates the behavior of faults for those cases in which the fuse did not clear. Just as important in addressing the MHIF concern is: What was the behavior for cases in which the fuse did not clear? The

key issue, of course, is whether any cases occurred in which fault current increased to a level of concern without triggering the fuse.

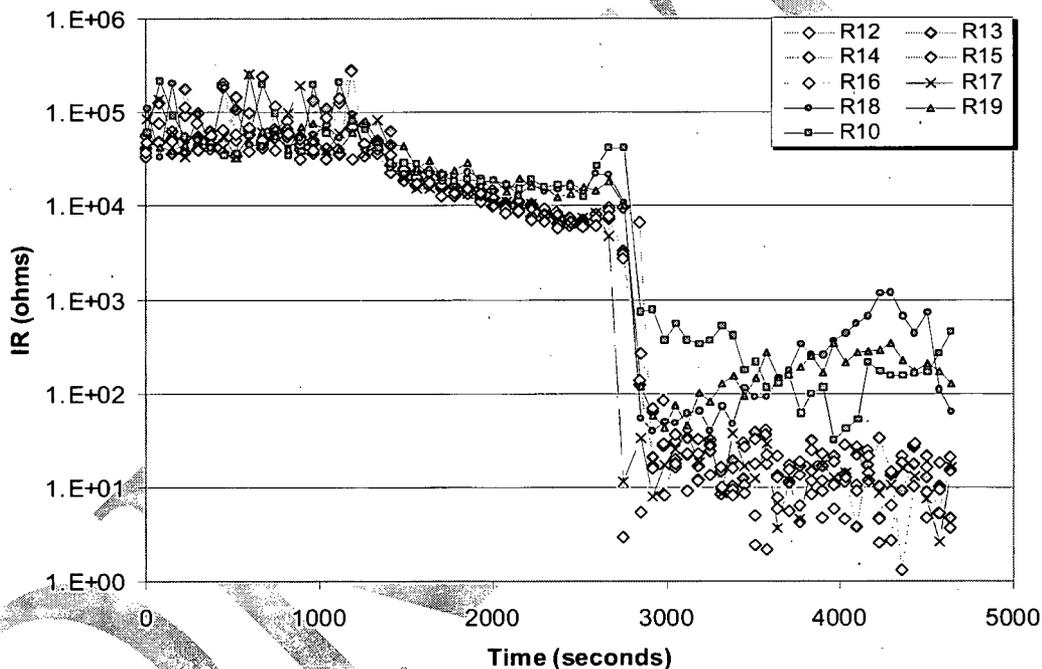
A review of the data for all cases in which the fuse did not clear indicates that the highest fault current observed without the fault ultimately cascading to full failure and clearing the fuse was 0.17 A, which correlates to a fault resistance of 700 Ω . No cases existed in which the failure progresses to the cascade point and did not ultimately fully fail.

B.1-6.1.2 NRC /SNL Fire Test Results

The NRC/SNL fire tests are documented in NUREG/CR-6776, *Cable Insulation Resistance Measurements Made During Cable Fire Tests* [3]. It is not intended that this analysis conduct a comprehensive review of the data associated with the NRC/SNL report. Rather, the test results are reviewed to ascertain any trends or insights different than observed in the EPRI/NEI test results.

The NRC/SNL test results show the same basic progression for cable failure. Insulation resistance drops predictably down to the 10 k Ω to 1,000 Ω range, at which points the failure cascades rapidly to full failure. The monitoring equipment sample rate was approximately 75 sec, and thus the measurements do not fully capture the dynamics of the cascade effect. Like the EPRI/NEI data, in many cases the IR is high one measurement then low for the subsequent measurement. The final IR values are more erratic than observed in the EPRI/NEI test data. This is attributed to the limited-energy circuit used for the testing. The circuit was designed to limit current to 1.0 A, which prevented the system from consistently driving faults to their conclusion. This observation further supports the *Base Case* requirement that the system be capable of supplying sufficient energy to the fault. A typical plot of insulation resistance from the NRC/SNL fire tests is shown in Figure B.1-8.

Figure B.1-8
Insulation Resistance Values for Typical Test Series
(Courtesy of USNRC and Sandia National Laboratories)



B.1-6.2 Characterization of Arcing Faults

As discussed in Section B.1-4.0, high impedance faults on systems operating at 480 V and above are manifested as arcing faults. Arcing-type faults are unique in their behavior and must be treated differently than conventional bolted faults [7, 13 – 22].

Arcing faults are characterized by relatively high fault impedance and low, erratic fault current. The rms current for an arcing fault can be substantially lower than the maximum available fault current (bolted fault). Arcing faults on high energy systems are extremely damaging and must be cleared rapidly to avoid extensive damage.

B.1-6.2.1 Fire as an Initiator of Arcing Faults

Operating history for electrical power systems shows the most common cause of arcing faults to be:

- Loose connections that overheat, causing minor arcing that escalates into an arcing fault
- Surface conduction due to dust, moisture, or other contaminants on insulating surfaces
- Electrical mishaps involving conducting materials (e.g., dropping a metal wrench into energized switchgear) or foreign objects in enclosures
- Insulation damage.

From a circuit failure perspective, fire is an external event with the propensity to damage any circuits in the vicinity of the fire; however, industry experience does not identify fire as a major initiator of faults on high energy systems. It is surmised that in many cases, operators take action to de-energize high voltage equipment before it is engulfed by an escalating exposure fires. Nonetheless, fire-induced arcing faults can occur on high energy systems and must be addressed.

B.1-6.2.2 Classification of Faults

Arcing faults may take the form of a line-to-line fault or a line-to-ground fault. Arcing faults include:

Three Phase (3-Ø) Systems: 3-Ø line-to-line
3-Ø line-to-ground
1-Ø line-to-line
1-Ø line-to-ground.

Single Phase (1-Ø) Systems: 1-Ø line-to-line
1-Ø line-to-ground.

Line-to-ground arcing faults pose less of a concern than line-to-line arcing faults for electrical distribution systems equipped with ground fault protection. Ground fault sensors may be set with high sensitivity to low magnitude currents because ground current is not expected under normal conditions. In contrast, line-to-line arcing faults can take longer to detect since the phase overcurrent devices are less capable of discriminating between a relatively harmless overload and a highly damaging, low-magnitude arcing fault.

Line-to-ground faults on solidly grounded electrical systems that are not equipped with ground fault sensors can produce faults that are not instantaneously cleared. Systems of this design rely on the phase overcurrent devices for protection, which do not offer the same degree of sensitivity to ground faults as do ground fault sensors. It is important to maintain perspective on this point. A highly energetic ground fault that is allowed to persist for even several seconds will generally cause widespread damage. Concern over this type of fault has initiated changes to recommended practices for protection against arcing ground faults. High-resistance grounded systems are generally not susceptible to damaging ground current flow because a grounding resistor or reactor limits the current to a very low level. Ungrounded systems require a fault on at least two phases to produce fault current flow. This type of fault is essentially a line-to-line fault.

Operating experience shows that arcing faults are most prevalent in metal-enclosed switchgear and open busways containing uninsulated bus bar. Insulated cables in conduit or tray more frequently suffer bolted faults. These characteristics are attributable to the nature of the arc. Arcing faults on uninsulated conductors tend to travel away from the source because of magnetic force interactions with the ionized arc. Movement of the arc minimizes the concentration of fault energy. In contrast, insulated cable does not allow rapid movement of the arc. Consequently, the arc energy and the damage it inflicts remain concentrated at the initial arc location, causing a more rapid degradation of the fault to a bolted fault.

B.1-6.2.3 Arc Voltage Drop and Waveshape

The arc voltage drop ranges from 100 – 150 volts for fault currents between 500 and 20,000 amps. The voltage is effectively constant over a wide range of current. The length of the arc for distribution level voltages varies but usually ranges between 1 and 2 inches.

Test data shows that the arc voltage waveshape is significantly distorted. The waveshape is initially sinusoidal and then quickly flattens at a magnitude of 100 – 150 volts, depending on the exact arc length and local conditions. The arc voltage waveshape does not increase in a linear fashion as a function of the system voltage. The voltage contains a significant third harmonic component, which is on the order of five times the normal value.

Once an arc is initiated, it extinguishes at current-zero and then reignites when instantaneous voltage reaches some threshold value. A key relationship exists between the reignition, or re-strike voltage, and the level of fault current. The lower the reignition voltage the higher the fault current. As reignition voltage approaches zero, fault current approaches its maximum value (bolted fault). And, as reignition voltage approaches system voltage, fault current approaches zero (open circuit). As a result of this inverse relationship, it is evident that higher reignition voltages represent more of a concern than lower voltages with respect to the MHIF concern. Analyses of distribution-level arcing faults generally assume a reignition voltage of 375 V (peak instantaneous). This voltage is considered a conservative practical upper limit for reignition based on typical system designs.

Arcing fault reignition has several important implications:

- Arcing faults with a reignition voltage above the system voltage are self-extinguishing. Thus, a lower threshold of fault current exists for which a fault can sustain itself beyond one cycle.
- An arc is not self-extinguishing at or above voltage levels with a peak instantaneous voltage greater than approximately 375 volts. 375 volts instantaneous corresponds to 265 volts rms.
- Sustained arcing faults on single phase 120/208 V AC systems are exceedingly rare. Two factors are involved: (1) the low system voltage reduces the likelihood of exceeding the reignition voltage, and (2) unlike three phase faults, periods of no current flow exist for single phase configurations, affording the ionized hot gasses a better chance of dissipating. This is not to say that arcing faults cannot occur at these voltage levels and cause equipment damage. It does, however, support a position that “sustained” arcing faults at this level very seldom occur.

- The fault current associated with arcing faults increases as a percentage of the bolted fault current as system voltage increases. This characteristic is due to the nature of the arc voltage, which remains relatively constant regardless of system voltage. Thus, the higher the system voltage, the longer will be the conduction portion of the arc ignition-extinguishment cycle.
- High impedance arcing faults are primarily an AC system phenomenon. The low-magnitude current associated with an arcing fault is largely due to the ignition – extinguishment cycle of the fault, which serves to lower the rms fault current. In a DC system, a periodic ignition – extinguishment cycle does not exist. Voltage is constant and thus current flows continuously once an arc is established.

B.1-6.2.4 Arc Fault Current

The current waveshape consists of non-continuous alternating pulses, with each pulse lasting about $\frac{1}{4}$ – $\frac{3}{4}$ of a cycle. The arc is extinguished each half cycle and reignited in the succeeding half cycle as discussed in Section B.1-6.2.3 above.

The generally accepted multipliers (expressed in % of bolted fault current) for estimating rms arcing fault current for 480/277 V systems are listed below. The multipliers are based on establishing the lower values of probable fault current for realistic values of arc voltage. Arc length is assumed to be 2 inches and arc voltage 140 V (line-to-neutral) / 275 V (line-to-line), independent of current. Neither of these assumptions is strictly true because of the dynamic movement of the arc and other configuration variables at the fault location. Thus, actual fault current may also vary. The estimated current values are, however, representative of the values produced during testing.

3-Ø Arcing Fault:	89%
Line-to-Line Arcing Fault:	74%
Line-to-Ground Arcing Fault:	38%

Note: Some industry papers addressing arcing fault protection suggest a multiplier of 19% for line-to-ground arcing faults. However, documented occurrences of cases below 38% appear exceedingly rare and appear to be associated with switchgear faults, which

tend to have longer arc lengths. The 38% value is considered reasonable for this assessment since the concern is with cables and not switchgear.

Minimum values of arcing fault current have not been established for medium voltage systems. However, as noted in Section B.1-6.2.3 above, the values will increase with system voltage, and as minimum will be higher than the 480 V values listed above. Practical experience indicates that arcing fault currents for medium voltage systems actually approach bolted fault levels.

B.1-6.2.5 Arc Energy

Even though the rms current for an arcing fault is less than that of a bolted fault, arcing faults can cause a great amount of damage. Most of the energy in the arc is released as heat at the arcing points; very little heat is conducted away from the arc by the conductors. In contrast, a bolted fault dissipates energy throughout all resistive elements in the distribution system and does not cause the concentrated energy release seen in arcing faults.

Fire can cause unspecified damage to cable and equipment insulation, which in turn can initiate an arcing fault in energized conductors. The failure sequence starts with a progressively decreasing insulation resistance. At some point under the applied voltage stress, the insulation allows sufficient leakage current to cause excessive localized heating in the insulation (usually at some minor imperfection in the cable). The localized heating escalates rapidly due to the high energy capacity of the system, and within moments conductor and insulation temperature reach their vaporization point. Conductive material is expelled, forming a vapor cloud in the vicinity of the fault. The vapor cloud readily conducts electricity and an arc is formed. The cloud of vaporized metal tends to quickly condense on surrounding surfaces, which creates a cascading effect for the arcing fault as additional arc paths are created. The loss of material due to vaporization contributes to the dynamic nature of arcing faults. Depending on the fault geometry and conditions, the arc might persist, blow open, or degrade to a bolted fault.

The amount of conductor vaporized during an arcing fault is directly related to the energy released at the fault. The industry-accepted correlation (supported by test results) is that 50 kW/sec of energy will vaporize approximately 1/20 in³ of copper. The significance of this characteristic is that arcing faults at medium voltage levels (above 1,000 V) cannot sustain themselves beyond a few seconds. The tremendous energy release at these higher voltages vaporizes conductor material so fast that the fault degrades almost immediately

or blows open. This category of fault can completely demolish equipment in a matter of seconds if not cleared.

B.1-7 ANALYSIS OF MHIFS

This section analyzes the MHIF concern within the framework of knowledge about fire-induced fault behavior developed in Section B.1-6. This characterization of fault behavior shows that faults manifest themselves differently at different voltage levels. Accordingly, the analysis conducted here is broken down by voltage classification.

B.1-7.1 Medium Voltage Systems (2.3 kV and Above)

Medium voltage systems at nuclear plants typically operate within the 2.3 kV to 13.8 kV range. Overcurrent protection for this class of equipment usually includes electro-mechanical or solid state overcurrent relays that actuate power circuit breakers. High voltage fuses may be used for some installations. Most systems also include sensitive ground fault detection designed to rapidly clear ground faults, which can be highly volatile and damaging.

HIFs for this class of power manifest themselves as arcing faults. The electrical properties and characteristics for arcing faults are discussed in Section B.1-6.2. The expected impact of arcing faults at the medium voltage level is addressed by the items below:

- The typical arc voltage drop of 100 – 150 volts is small in relation to the overall system voltage. Thus, an arcing fault at medium voltage levels will not appreciably reduce fault current in the same manner as it does for low-voltage systems. Based on the 480 V multipliers presented in Section B.1-6.2.4, very conservative assumed lower arcing fault currents of 40% (line-ground) and 80% (line-to-line) of the symmetrical rms bolted fault current produce highly damaging levels of current flow. An adequately designed protective system can be expected to clear faults at these levels very rapidly (within a few seconds). Systems coordinated in accordance with the guidance of ANSI/IEEE 242 (or other acceptable criteria) are considered to be adequately designed.
- Most all medium voltage power systems include sensitive ground fault protection devices. These devices are set to clear ground faults at very low levels (20 A – 100 A) – well below the assumed 40% lower fault current limit. Systems that are high

resistance grounded inherently limit fault current to a low value. Accordingly, these systems are designed to be extremely sensitive to ground fault current, and are expected to rapidly clear any type of ground fault.

- Certain cable runs may not be protected by overcurrent relays, but instead may use differential protection schemes. Differential protection is very sensitive and any cable protected this type of circuit will clear in-zone faults within milliseconds. Sensitivity varies, but is in the 10s to hundreds of amps and not thousands of amps.
- Arcing faults on medium voltage systems produce explosive energies. An arcing fault with an arc voltage of 140 volts (very conservative for this voltage level) and fault current of 2,000 A (also a conservative value) will vaporize copper conductor at a rate of:

$$\text{Volume Vaporized} = (140 \times 2.00 \times 1/20) / 50 = 0.4515 \text{ in}^3 \text{ copper / sec}$$

At this vaporization rate for busbar or cable, the fault conditions cannot be sustained for more than a few moments before the dynamic nature of the fault produces near bolted conditions or blows open.

- Operating experience shows that even with highly sensitive protection that clears arcing faults within a fraction of a second (or in the worst case seconds) severe localized damage is likely. Given the energies involved, from a hardware integrity perspective it is not plausible that arcing faults can be sustained for a prolonged period of time at medium voltage levels.

Conclusion

HIFs at medium voltage levels will manifest themselves as arcing faults. The minimum credible fault current produced by these faults will be rapidly detected by an adequately designed protective scheme and the fault will be cleared immediately, typically within milliseconds. The energies produced by arcing faults for this class of power system cannot be sustained by the hardware for more than a few seconds due to physical destruction of the conductor, insulating materials, and surrounding equipment. The analysis supports a conclusion that, for medium voltage power supplies conforming to the *Base Case*, the probability of MHIFs is sufficiently low to classify the failure mode as an incredible event that does not pose a credible risk to post-fire safe shutdown.

B.1-7.2 480 V – 600 V Low Voltage Systems

480 V systems are most common at nuclear plants; however, some 600 V systems exist. A variety of overcurrent protective devices are used for this class of equipment. Load centers are generally protected by low voltage power circuit breakers configured with an internal electro-mechanical or solid-state trip unit. Motor control centers and distribution panels typically contain molded case circuit breakers or fuses. Some 480 V systems are configured with separate ground fault detectors and some are not.

HIFs for this class of power manifest themselves as arcing faults. The electrical properties and characteristics for arcing faults are discussed in Section B.1-6.2. The expected impact of arcing faults at this voltage level is addressed by the items below:

- Credible lower limits for sustained arcing faults on 480 V systems are presented in Section B.1-6.2.4. Arcing fault currents of 38% (line-ground) and 74% (line-to-line) of the symmetrical rms bolted fault current produce damaging levels of current flow. An adequately designed protective system can be expected to clear faults at these levels rapidly (although maybe not instantaneously). Systems coordinated in accordance with the guidance of ANSI/IEEE 242 (or other acceptable criteria) are considered to be adequately designed. A worst-case example is developed below to substantiate this position.
- A worst-case scenario might involve an arcing ground fault on a solidly grounded system that is not configured with individual ground fault detection. Assume an end-of-line fault has a symmetrical rms bolted fault current of 5,000 A (highly conservative as most 480 V systems produce fault current in the range of 10 kA to 25 kA). This case would result in an arcing fault current of 1,900 A (.38 x 5,000). It is conceivable that this level of fault current might not trigger the instantaneous trip element of the affected overcurrent device; however, the inverse time element will assuredly detect and clear the fault as no realistic system contains feeders operating at 1,900 A continuous. In this case it is plausible that the fault might take 10 – 15 sec to clear. However, due to the destructive power this fault would unleash, it is doubtful that the hardware would survive these conditions.
- If the above scenario is postulated to occur at the switchgear, it is distinctly possible that the switchgear main breaker might not readily detect the fault, as these breakers can be rated at 800 A – 4,000 A. Literature documents such cases, and complete destruction of the switchgear was the outcome. However, switchgear and bus faults

requiring main breaker protective action are not of concern for the MHIF issue.

- 480 V systems configured with properly coordinated ground fault detection can be expected to clear low-level arcing ground faults immediately.
- As with medium voltage systems, arcing faults on 480 V systems produce tremendous energies at the fault location. An arcing fault with an arc voltage of 100 volts (conservative) and fault current of 1,900 A will vaporize copper conductor at a rate of:

$$\text{Volume Vaporized} = (100 \times 1,900 \times 1/20) / 50 = 0.190 \text{ in}^3 \text{ copper / sec}$$

Although not as severe as that seen on medium voltage systems, this vaporization rate for busbar or cable cannot be sustained, and the fault will progress rapidly to a bolted condition or will blow open as localized destruction escalates.

Conclusion

HIFs on 480 V – 600 V power systems manifest themselves as arcing faults. The minimum credible fault current produced by these faults will be detected by an adequately designed protective scheme and the fault will be cleared (although maybe not instantaneously). The energies produced by arcing faults for this class of power system cannot be sustained by the hardware for extended periods of time before physical destruction of the conductor, insulating materials, and surrounding equipment result in widespread and catastrophic damage. The analysis supports a conclusion that, for 480 V – 600 V power supplies conforming to the *Base Case*, the probability of MHIFs is sufficiently low to classify the failure mode as an incredible event that does not pose a credible risk to post-fire safe shutdown.

B.1-7.3 120 V and 208 V Systems

120 V systems are most often used for control and control power circuits; 208 V systems are typically associated with lighting, small motors, heaters, etc. 120 V single-phase circuits are of greatest interest for this study. For nuclear plant applications, overcurrent protective devices are generally molded case circuit breakers or fuses located within power distribution panels. The systems are most often powered by battery-backed inverters or relatively small transformers.

The recent industry and NRC fire tests confirm that the behavior of cable faults on 120 V systems is fundamentally different than that for faults on 480 V and higher systems. Theory predicts that sustained arcing faults at the 120 V level are not credible because the system is not able to repeatedly overcome the reignition voltage of 375 V. Indeed testing appears to confirm this point. This is not to say that arcing faults cannot occur at the 120 V level, but rather that they cannot be sustained. Arcing faults on 120 V systems have been said to be "sputtering" faults. They arc, extinguish, and then re-arc and extinguish in a random manner based on the local conditions and geometry at the fault. The test data identified two cases that may have fallen into this category. These cases are included in the data set analyzed in Section B.1-6.1. It is noteworthy that the current profiles for these cases show current to be erratic and unpredictable, but at no time did current rise to HIF levels and remain there for more than a few seconds. Ultimately, the fault in each case degraded to a low level and was cleared by the fuse. These faults may also have simply been a case in which the localized insulation breakdown effect shifted as a result of the fire dynamics. Regardless of the specific phenomena at work, these cases are included in the analysis.

The test data clearly shows that faults at these levels on average do not clear as rapidly as faults at higher voltages. With our understanding of fault behavior, the reason for this is somewhat intuitive. The applied voltage stress and available fault current are orders of magnitude lower than for higher voltage power systems. Hence, the local conditions are not nearly as violent and the cable failure sequence simply progresses at a slower rate. That is, the energy released at the fault is much lower, and thus the insulation is not driven to full failure as rapidly. Additionally, the magnetic forces at this level do not cause the dynamic effects (movement of conductors) observed for high energy system faults.

The electrical properties and characteristics for faults on 120 V systems are discussed in Section B.1-6.1. The expected impact of these faults is addressed by the items below:

- The test data indicates that 120 V faults do not manifest themselves in a manner conducive to sustained HIF conditions. Once the fault has progressed to a certain level, it cascades rapidly to full failure within seconds or 10s of seconds, as shown by the test data (summarized below). This phenomenon was observed consistently in all the EPRI/NEI test data and NRC/SNL data,

with the exception of instrument circuits,²⁷ which are not within the scope of this analysis. The transition region at which the cascading effect begins appears to range from approximately 10 k Ω to 1,000 Ω . But in all instances, when leakage current exceeded 0.25 A the fault was driven to failure and the fuse cleared. The 0.25 A (480 Ω fault resistance) threshold is important because this level of fault current (more appropriately classified as leakage current at this level) poses no conceivable risk for any realistic circuit with respect to the MHIF concern.

- This analysis uses 2 A as the benchmark value for fault current flow that represents a lower limit of current potentially of concern from a MHIF perspective. This value represents 67% of the test circuit continuous current capability (i.e., 3 A fuses). Analysis of the test data provides us with the following probabilities associated with the time frames for clearing faults once fault current has risen to 2 A. The 95% confidence level is also shown to quantify uncertainty in the data set.

²⁷ The inability of instrument power supplies to transfer appreciable energy to the fault appears to preclude rapid failure in some cases. The impact of this effect on instrument circuits is discussed in the NRC/SNL report [3].

Time (min)	Probability of Clearing Fault	95% Lower Confidence Limit
0.1	89.3%	82.3%
0.2	90.7%	84.1%
0.3	92.0%	85.9%
0.4	93.3%	87.7%
0.5	94.7%	89.6%
0.6	96.0%	91.6%
0.7	96.0%	91.6%
0.8	100.0%	100.0%
1.0	100.0%	100.0%

- The two key observations gleaned from the probability values are:
 - Over 80% of the faults are cleared in less than 0.1 min at a 95% confidence level
 - 100% of the faults (or nearly 100% if some margin is added for general uncertainty) clear within 0.8 min at a 95% confidence level
- The EPRI/NEI test data revealed NO cases in which the test circuit fuse failed to clear once current exceed 0.17 A (700 Ω fault resistance) – an important observation supporting the premise that faults do not “hang up” once cascade failure begins.
- The test circuits upon which the probability values are based contained 3 A fuses. A fair question to ask is whether the probability values are applicable to circuits with larger protective devices, for instance a 5 A or 10 A branch circuit fuse. Based on the fault characteristics, applying the results to high rated devices appears justified. Once current has passed 2 A, the fault resistance has degraded to a low level and the system, rather than the fault, becomes the primary determinant of the fault current magnitude. Provided the protective devices are adequately coordinated and the system provides sufficient fault current, the relative timing of the devices will be maintained over the entire fault current range. The important behavior here is that the faults do not “hang up” and thereby jeopardize the coordination scheme by producing fault currents below detectable levels.

Conclusion

A detailed analysis of fault behavior for 120 V systems indicates that these faults do not exhibit characteristics that are conducive to sustained HIF conditions. The analysis demonstrates that once fault current surpasses a certain threshold level, the fault repeatedly and reliably degrades to a low level that will trigger overcurrent protective action for an adequately designed system. This threshold level varies but appears to be near 0.2 A at the lower limit. This level of "abnormal current flow" does not pose a risk with respect to the MHIF failure mode and in fact does not even render the affected circuit inoperable. The fundamental fault characteristics upon which this conclusion is based were readily apparent in the EPRI/NEI tests and the NRC/SNL tests. Additionally, a similar utility-sponsored test conducted in 1987 revealed the same basic behavior [27]. The analysis supports a conclusion that, for 120 V power supplies conforming to the *Base Case*, the probability of MHIFs is sufficiently low to classify the failure mode as an incredible event that does not pose a credible risk to post-fire safe shutdown.

B.1-7.4 125 V and 250 V DC Systems

125 V and 250 V DC systems provide control power and motive power to essential equipment, including switchgear and motor control circuits, motor-operated and solenoid operated valves, instruments, and emergency lighting. Overcurrent protective devices are generally molded case circuit breakers or fuses located within power distribution panels. Low voltage power circuit breakers are sometimes used at the DC control centers.

The test data and industry information presented in Section B.1-6.0 apply to AC power systems and thus cannot be directly applied to DC systems. However, the well-understood differences between AC and DC power allow the results to be reasonably applied to DC systems as explained below:

- Arcing type faults on low voltage DC systems cannot be ruled out using the same logic applied to low voltage AC systems. Once an arc is struck on a DC system, it has no sinusoidal waveform to initiate the ignition-extinguishment cycle, and thus the concept of a minimum re-ignition voltage does not apply. However, high impedance arcing faults are primarily an AC system phenomenon. The low-magnitude current associated with an arcing fault is largely due to the ignition - extinguishment cycle of the fault, which serves to lower the rms fault current. In a DC system, fault current more readily flows without interruption once a short circuit begins. This continuous current flow is not conducive to prolonged, sporadic arcing conditions. Once the fault begins, theory predicts that it will quickly escalate in magnitude and will be

rapidly cleared by a properly designed protective system. Operating experience supports this theory in that high impedance arcing faults are not identified as a concern by industry standards and literature.

- For non-arcing faults on 125 V DC systems, the analytical results for 120 V AC systems can be conservatively applied. The key failure phenomenon observed in the test data is the cascading effect once leakage current exceeds the threshold level. Here again the continuous nature of DC power supports a position that energy will be transferred to the fault faster in a DC system because the voltage stress applied at the fault is constant and will precipitate a quicker breakdown of the insulation.
- As a second factor affecting the rate of cascade failure, the test data shows a correlation between available fault current and the expected clearing time. DC systems at nuclear power plants are battery-backed, and thus are capable of delivering high fault currents almost instantaneously. These fault currents are often an order of magnitude larger than exists on 120 V AC systems.
- Virtually all DC power distribution systems at nuclear plants operate ungrounded. Thus, ground faults are not of concern in a manner similar to AC power systems.
- Operating experience with faults on battery-backed DC power systems is that the fault will likely blow open but it can also quickly weld itself. In either case, whatever is going to happen happens almost instantaneously.

Conclusion

Test data and industry literature pertaining to fault characteristics for representative DC power systems are not readily available. However, a reasonable extrapolation of the analysis results for AC systems is accomplished using engineering rationale based on the differences between AC and DC power. The inherent characteristics of DC power do not introduce any known factors that preclude application of the analysis results to DC systems. To the contrary, DC power characteristics lend credence to a position that the AC results are conservative with respect to DC power system performance. Although not a technical basis, it is noteworthy that the NRC limits its stated concern with MHIF to AC power systems [4]. It would appear that NRC technical experts investigating the issue concur that the postulated phenomena are limited to AC power systems.

B.1-7.5 Failure Consequence Analysis

Elements of this MHIF evaluation contain risk-informed arguments. As such, it is prudent to assess not only likelihood of the postulated failure mode, but also the potential consequences of failure.

B.1-7.5.1 Loss of Safe Shutdown Power Supply

The MHIF failure mode can result in a safe shutdown power supply becoming de-energized, which in turn could potentially lead to de-energization of safe shutdown equipment. This failure mode is fundamentally different than electrical failures resulting from the direct effects of fire. The direct effect failure modes (i.e., shorts-to-ground, hot shorts, open circuits) cause circuit damage that can only be rectified through repairs. The MHIF failure mode is not unrecoverable in the sense that restoration involves resetting an overcurrent relay, closing a circuit breaker, or replacing a fuse. (It is acknowledged that fuse replacement is generally classified as a "repair activity" within the compliance guidelines for Appendix R. Nonetheless, from a "consequence" point of view, replacing a fuse – which typically requires no tool or a simple tool – is fundamentally different than a repair involving the replacement of cables and components.) It is understood that operators are credited with identifying the problem and taking steps to restore the affected power supply to service. Given that almost all safe shutdown power supplies require some local action for alternative shutdown or spurious operation mitigation, it is also probable that critical power supplies are covered by emergency lights and that access/egress paths have been considered. On this basis, the MHIF failure mode is considered to have a low consequence and is not a significant contributor to fire risk.

B.1-7.5.2 High-Low Pressure Interface Components

This analysis strives to maintain consistency with existing regulatory perspective. Accordingly, it is considered prudent that in applying this criteria, it be confirmed that a postulated MHIF does not have the capability to initiate an opening of a high/low pressure interface, due to the potentially severe consequences.

This constraint should not prove limiting in that high/low pressure interface components are most always designed to fail safe in the "closed" or "isolated" state and the MHIF failure mode will always involve de-energization.

B.1-8 CONCLUSIONS

This analysis investigates fire-induced circuit failure characteristics to determine if and under what conditions the MHIF failure mode poses a credible risk to post-fire safe shutdown. The analysis is based on objective test data and recognized engineering principles as documented in test reports, consensus standards, and other credible industry references. The analysis considers both likelihood and consequence, and also addresses analysis uncertainty for critical results.

A *Base Case* set of conditions has been established to define the limits of applicability for the analysis. Within the defined limits, this MHIF analysis is intended to serve as a generic evaluation and is considered to satisfy the regulatory requirement that high impedance faults be considered in the analysis of associated circuits. Circumstances that fall outside the defined *Base Case* will require a plant-specific analysis.

A detailed analysis of fault characteristics for the voltage levels of interest indicates that these faults do not exhibit characteristics that coincide with that of concern for MHIFs. The analysis supports a conclusion that the probability of MHIFs for power supplies conforming to the *Base Case* is sufficiently low to classify the failure mode as an incredible event that does not pose a credible risk to post-fire safe shutdown.

The results and conclusions of this analysis may be used to support a licensing basis change (using an approved regulatory process) under the following conditions:

- The power supply conforms to the *Base Case* requirements.
- The power supply will not cause opening of a high/low pressure interface boundary if de-energized.

B.1-9 REFERENCES

NRC Documents

1. Regulatory Guide 1.189, *Fire Protection for Operating Nuclear Power Plants*, U.S. Nuclear Regulatory Commission: April 2001.
2. Generic Letter 86-10, *Implementation of Fire Protection Requirements*, U.S. Nuclear Regulatory Commission: April 24, 1986.
3. F.J. Wyant and S.P. Nowlen, *Cable Insulation Resistance Measurements Made During Cable Fire Tests*, Sandia National Laboratories, Albuquerque, NM: June 2002. USNRC NUREG/CR-6776, SAND2002-0447P.
4. Olan D. Parr to ASB Members Note, dated November 30, 1984. Subject: Fire Protection Review Guidance.

Consensus Codes & Standards

5. ANSI/IEEE C37 Series Standards, *Power Energy: Switchgear Collection*, 1998 Edition.
6. IEEE 141-1993 (R1999), *IEEE Recommended Practice for Electric Power Distribution for Industrial Plant*. (Red Book)
7. ANSI/IEEE 242-1986 (2001), *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*. (Buff Book)
8. ANSI/IEEE 1015-1997, *IEEE Recommended Practice for Applying Low-Voltage Circuit Breakers Used in Industrial and Commercial Power Systems*. (Blue Book).
9. ANSI IEEE 383-1974 (R1980), *IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices and Connections for Nuclear Generating Stations*.
10. ANSI/NFPA 70, *National Electrical Code*, 2002 Edition.

11. NEMA ICS-1-1993, Table 7-2, "Clearance and Creepage Distance for Use Where Transient Voltage are Controlled and Known."

Industry Documents

12. *Characterization of Fire-Induced Circuit Failures: Results of Cable Fire Testing*, EPRI, Palo Alto, CA: 2002. 1003326.
13. J.R. Dunki-Jacobs, "The Effects of Arcing Ground Faults on Low-Voltage System Design," *IEEE Transactions on Industrial Applications*, Vol. IA-8 No. 3: May/June 1972, pp 223-230.
14. J.R. Dunki-Jacobs, "The Escalating Arcing Ground-Fault Phenomenon," *IEEE Transactions on Industrial Applications*, Vol. IA-22 No. 6: November/December 1986, pp 1156-1161.
15. L.E. Fisher, "Resistance of Low-Voltage Alternating Current Arc," *Conference Record of the 1970 Annual Meeting of the IEEE Industry and General Applications Group*: October 1970, pp 237-254.
16. J.A. Gienger, O.C. Davidson, and R.W. Brendel, "Determination of Ground-Fault Current on Common A-C Grounded-Neutral Systems in Standard Steel or Aluminum Conduit," *AIEE Transactions on Applications and Industry, Part II*, Vol. 79: 1960, pp84-90.
17. R.H. Kaufmann, "Some Fundamentals of Equipment Grounding Circuit Design," *AIEE Transactions on Applications and Industry, Part II*, Vol. 73: 1954, pp 227-231.
18. R.H. Kaufmann and J.C. Page, "Arcing Fault Protection for Low-Voltage Power Distribution Systems - Nature of Problem," *AIEE Transactions Part III, Power Apparatus and Systems*, Vol. 79 (Paper 60-83): June 1960, pp 160-167.
19. R.H. Kaufmann, "Ignition and Spread of Arcing Faults," *1969 Industrial and Commercial Power Systems and Electric Space Heating and Air Conditioning Joint Technical Conference*: May 1969, pp 70-72.

20. Kusko and S.M. Peeran, "Arcing Fault Protection of Low-Voltage Distribution Systems in Buildings," *Conference Record of the 1987 IEEE Industry Applications Society Annual Meeting*, Part I: October 1987, pp 1385-1389.
21. F.J. Shields, "The Problem of Arcing Faults in Low-Voltage Power Distribution Systems," *IEEE Transactions on Industrial and General Applications*, Vol. IGA-3 No. 1: January/February 1967, pp 15-25.
22. C.F. Wagner and L.L. Fountain, "Arcing Fault Currents in Low-Voltage A-C Circuits," *AIEE Transactions*, Part I, Vol. 67: 1948, pp166-174.

Miscellaneous

23. William, J. *Statistics for Nuclear engineers and Scientists, Part 1: Basic Statistical Inference*, Department of Energy, Washington DC: February 1981. WAPD-TM-1292.
24. Hahn, Gerald J. and Meeker, William O. *Statistical Intervals, A Guide for Practitioners*, John Wiley & Sons, Inc., Canada: 1991.
25. Stevenson, William D. *Elements of Power System Analysis*, McGraw-Hill: 1992.
26. *Power Plant Practices to Ensure Cable Operability*, EPRI, Palo Alto, CA: July 1992. NP-7485.
27. *Appendix R Multiple High Impedance Cable Fault Flame Test Report*, Philadelphia Electric Company, Philadelphia, PA: May 27, 1988.

APPENDIX C

HIGH / LOW PRESSURE INTERFACES

C.1 PURPOSE

The purpose of this appendix is to identify considerations necessary to address the issue of circuit analysis of high/low pressure interface components

C.2 INTRODUCTION

10 CFR 50 Appendix R analyses must evaluate the potential for spurious operations that may adversely affect the ability to achieve and maintain safe shutdown. A subset of components considered for spurious operation involves reactor coolant pressure boundary (RCPB) components whose spurious operation can lead to an unacceptable loss of reactor pressure vessel/Reactor Coolant System (RPV/RCS) inventory via an interfacing system loss of coolant accident (ISLOCA). Because an ISLOCA is a significant transient, it may be beyond the capability of a given safe shutdown path to mitigate. As a result of this concern, selected RCPB valves are defined as high/low pressure interface valve components requiring special consideration and criteria.

Note: As part of industry efforts to support transition of fire protection programs to 10 CFR 50.48(c) (NFPA 805), a Frequently Asked Question (FAQ) 06-0006 was written to clarify the definition of high/low pressure interface components. In the closure memo for FAQ 06-0006 dated March 12, 2007, the NRC stated:

"...the staff concluded that the definition provided in NEI-00-01 for the term "high-low pressure interface" is acceptable."

C.3 IDENTIFYING HIGH/LOW PRESSURE INTERFACE COMPONENTS

Regulatory Guidance

The criteria for defining high/low interface valve components are described in the following NRC documents.

Generic Letter 81-12 states, in part:

*The residual heat removal system is generally a low pressure system that interfaces with the high pressure primary coolant system. To preclude a LOCA through this interface, we require compliance with the recommendations of Branch Technical Position RSB 5-1. It is our concern that this single fire could cause the **two valves** to open resulting in a fire initiated LOCA.*

BTP RSB 5-1, Rev. 2 Dated July 1981 states in part:

B. RHR System Isolation Requirements

The RHR system shall satisfy the isolation requirements listed below.

- 1. The following shall be provided in the suction side of the RHR system to isolate it from the RCS.*
 - a. Isolation shall be provided by at least two power-operated valves in series. The valve positions shall be indicated in the control room.*
 - b. The valves shall have independent diverse interlocks to prevent the valves from being opened unless the RCS pressure is below the RHR system design pressure. Failure of a power supply shall not cause any valve to change position.*
 - c. The valves shall have independent diverse interlocks to protect against one or both valves being open during an RCS increase above the design pressure of the RHR system.*
- 2. One of the following shall be provided on the discharge side of the RHR system to isolate it from the RCS:*
 - a. The valves, position indicators, and interlocks described in item 1(a) thru 1(c) above,*
 - b. One or more check valves in series with a normally closed power-operated valve. The power-operated valve position shall be indicated in the control room. If the RHR system discharge line is used for an ECCS function, the power-operated valve is to be opened upon receipt of a safety injection signal once the reactor coolant pressure has decreased below the ECCS design pressure.*
 - c. Three check valves in series, or*
 - d. Two check valves in series, provided that there are design provisions to permit periodic testing of the check valves for leak tightness and the testing is performed at least annually.*

NRC Information Notice 87-50 reiterates:

Appendix R also states that for these areas, the fission product boundary integrity shall not be affected, i.e., there shall be no rupture of any primary coolant boundary. Thus, for those low pressure systems that connect to the reactor coolant system (a high pressure system), at least one isolation valve must remain closed despite any damage that may be caused by fire. Since the low pressure

system could be designed for pressures as low as 200 to 400 psi, the high pressure from the reactor coolant system (approximately 1000 to 1200 psi for BWRs and 2000 to 2200 psi for PWRs) could result in failure of the low pressure piping. In many instances, the valves at the high pressure to low pressure interface are not designed to close against full reactor coolant system pressure and flow conditions. Thus, spurious valve opening could result in a LOCA that cannot be isolated, even if control of the valve can be reestablished.

The NRC has taken the position that high/low pressure interface equipment must be evaluated to more stringent requirements than non-high/low pressure interfaces when considering spurious operations. The purpose of the requirements is to ensure that a fire-induced LOCA does not occur.

The NRC concern is one of a breach of the RCS boundary, by failure of the downstream piping due to a pipe rupture or other failures such as relief valve operations. However, if the spurious opening of RCS boundary valves cannot result in a pipe rupture or unintended relief valve operations (i.e., downstream piping is rated for the range of RCS pressures), then the subject boundary valves do not constitute high/low pressure interfaces. The following combinations of valves are typically considered as high/low pressure interface concerns:

- a. RCS to shutdown cooling system (e.g., Residual Heat Removal/Decay Heat Removal, etc.) suction valves.
- b. RCS letdown isolation valves (e.g., letdown to radwaste, condensate (BWRs), main condenser (BWRs) or volume control system (PWRs).
- c. RCS high point vent isolation valves

Note that not all of these valves meet the original criteria identified in GL 81-12, nor is RSB 5-1 applicable to each example. This expansion in scope is the result of conservative interpretations by licensees and the NRC as safe shutdown compliance strategies at individual plants have evolved.

Based on the above guidance, the following criterion is established to determine if a RCPB valve is considered a high/low pressure interface valve component: *A valve whose spurious opening could result in a loss of RPV/RCS inventory and, due to the lower pressure rating or other breaches such as relief valve operations on the downstream piping, an interfacing LOCA (i.e., pipe rupture in the low pressure piping).*

C.4 CIRCUIT ANALYSIS CONSIDERATIONS

The specific differences made in addressing circuit analysis of high/low pressure interface components are described in NRC Generic Letter 86-10, Question 5.3.1, which requests a clarification on the classification of circuit failure modes. The question and the response are provided below.

5.3.1 Circuit failure modes

Question

What circuit failure modes must be considered in identifying circuits associated by spurious actuation?

Response

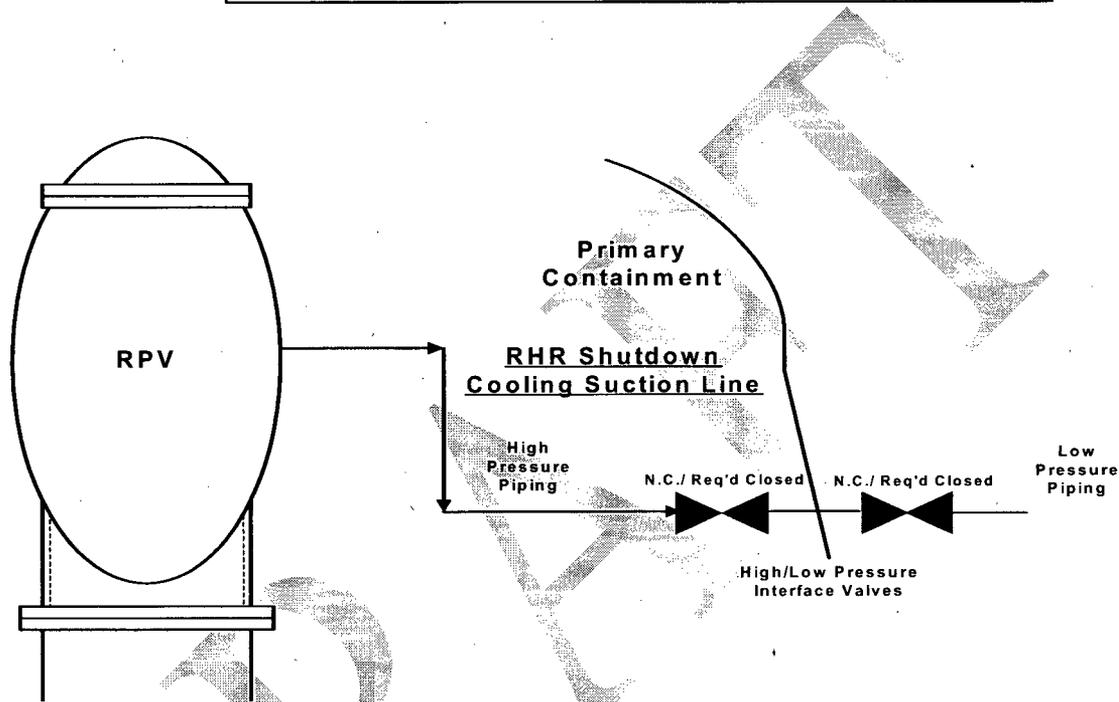
Sections III.G.2 and III.L.7 of Appendix R define the circuit failure modes as hot shorts, open circuits, and shorts to ground. For consideration of spurious actuations, all possible functional failure states must be evaluated, that is, the component could be energized or de-energized by one or more of the above failure modes. Therefore, valves could fail open or closed; pumps could fail running or not-running, electrical distribution breakers could fail open or closed. For three-phase AC circuits, the probability of getting a hot short on all three phases in the proper sequence to cause spurious operation of a motor is considered sufficiently low as to not require evaluation except for any cases involving Hi/Lo pressure interfaces. For ungrounded DC circuits, if it can be shown that only two hot shorts of the proper polarity without grounding could cause spurious operation, no further evaluation is necessary except for any cases involving Hi/Lo pressure interfaces.

The response to Question 5.3.1 establishes a basis for limiting the number of credible circuit failure modes that need to be postulated for non-high/low pressure interface components. At the same time it implies that further evaluation is required when considering circuit failures of high/low pressure interface components. Further evaluation is required for cases involving high/low pressure interfaces, specifically, the case of two hot shorts on an ungrounded DC circuit. The discussion involving the DC circuit implies that two hot shorts need not be postulated except for high/low pressure interface components.

High/low pressure interface valves are identified separately from other safe shutdown components because the cable fault analysis and the effects on safe shutdown due to spurious operation of the high/low interface valves are evaluated more stringently than the safe shutdown components. The potential for spuriously actuating redundant valves in any one high/low pressure interface as a result of a fire in a given fire area must also be postulated. This includes considering the potential for a fire to spuriously actuate both valves from a selective hot short on different cables for each valve.

C.5 FIRE AREA ASSESSMENT OF HIGH/LOW PRESSURE INTERFACES

Figure C-1
High/Low Pressure Interface Example



In this example, the postulated fire damage is evaluated for two cases. In the first case, Case (a), the fire is assumed to have the potential to cause the spurious opening of one of the two series normally closed high/low pressure interface valves. In the second case, Case (b), the fire is assumed to have the potential to cause the spurious opening of both series high/low pressure interface valves.

Case (a):

For this case, the spurious opening of either one of the two series high/low pressure interface valves can be justified on the basis that the other valve will remain closed and prevent an interfacing system LOCA.

Case (b):

For this case, the argument applied above would be unacceptable. Examples of acceptable alternatives would be to protect the control circuits for either valve in the fire

area, to reroute the spurious circuits or to de-power one of the valves to prevent spurious opening.

A mitigating action may be taken prior to the start of the fire event that precludes the condition from occurring, or a post-fire action may be taken that mitigates the effects of the condition prior to it reaching an unrecoverable condition relative to safe shutdown, if this can be shown to be feasible. When mitigating actions are taken, they must comply with the applicable regulations and licensing bases.

C.6 REFERENCES

- C.6.1 Branch Technical Position BTP RSB 5-1 Rev. 2, July 1981.
- C.6.2 Generic Letter 81-12, "Fire Protection Rule," February 20, 1981.
- C.6.3 Generic Letter 86-10 "Implementation of Fire Protection Requirements," April 24, 1986.
- C.6.4 IN 87-50 – Potential LOCA at High and Low Pressure Interfaces from Fire Damage, October 9, 1987.

APPENDIX D

ALTERNATIVE/DEDICATED SHUTDOWN REQUIREMENTS

D.1 PURPOSE

The purpose of this appendix is to provide the requirements for alternative and dedicated shutdown that are distinct and different from the requirements for redundant shutdown.

D.2 INTRODUCTION

The use of alternative/dedicated shutdown capability is required in those specific fire areas where protection of a redundant safe shutdown path from the effects of fire was not possible. Alternative/dedicated shutdown capability is generally specified for the control room. Other plant areas where alternative/dedicated shutdown capability may be required include the cable spreading room, electrical distribution room, relay room(s), or other plant areas where significant quantities of control cables are routed and redundant trains of safe shutdown equipment have not been separated in accordance with the requirements specified in Section III.G.2. of Appendix R. The areas where alternative or dedicated shutdown is credited are defined in the licensing basis documents for each plant. Use of the term alternative or dedicated shutdown is applied to the specific plant area(s) and not to the equipment or methodology (capability) employed to achieve safe shutdown. The alternative/dedicated shutdown capability may be different for each of the defined areas. Manual actions may be utilized for alternative/dedicated shutdown capability in accordance with NRC requirements and guidance.

Alternative/dedicated shutdown capability requires physical and electrical independence from the area of concern. This is usually accomplished with isolation/transfer switches, specific cable routing and protection, and remote shutdown panel(s). The alternative/dedicated safe shutdown system(s) must be able to be powered from the onsite power supplies, which must be physically and electrically independent from the area under consideration. The availability or loss of offsite power and loss of automatic initiation logic signals must be accounted for in the equipment and systems selected or specified. All activities comprising the alternative/dedicated shutdown capability are considered mitigating actions and need to be evaluated against regulatory acceptance criteria to ensure that the goals and criteria in Section III.L are met.

Appendix R Section III.G.3 requires that the equipment, cabling, and associated circuits required for alternative shutdown must be independent of the fire area being evaluated. Therefore, in the case of a control room fire, the safe shutdown systems and components may be similar to those used in other areas for redundant shutdown; however, they must be physically located outside the fire area and if required, the control of the components must be electrically isolated by transferring control to a remote shutdown control station(s). Examples of components and cables that must be physically and electrically independent of the control room for alternative or dedicated shutdown use include the

components that can be controlled from a remote shutdown panel and the cables that provide control from that panel once they are isolated from the control room circuit. GL 81-12 required that each Appendix R plant submit its modification plans for their alternative shutdown capability for prior staff review and approval. These submittals typically included details of the proposed isolation/transfer design.

This appendix describes those aspects of the methodology and guidance for alternative/dedicated shutdown that are different from the methodology and guidance applied for redundant post-fire safe shutdown in the body of this document. Section D.3 overviews the methodology as it relates to control room fires, since the control room is the fire area where alternative shutdown is predominantly used. Section D.4 describes the regulatory requirements for alternative and dedicated shutdown. Section D.5 itemizes the differences in shutdown methodology between alternative/dedicated shutdown and those supplied in the body of this document for redundant shutdown. Section D.6 recommends additional operator actions that should be considered for use on a plant-unique basis for fires requiring control room evacuation.

D.3 OVERVIEW

Since the majority of nuclear plants use the alternative/dedicated shutdown scheme exclusively for a control room fire, this overview addresses this fire location only. An exposure fire in the Control Room of an operating nuclear power plant would be a potentially serious event. The likelihood of a control room fire, however, is considered to be small. The worst-case expected fire for a control room would be one that is contained within a single section of a control panel. This is true because the control room is continuously manned, the introduction of combustible materials and ignition sources is strictly controlled, and the fire protection and separation features designed into the control room are focused on the prevention of such an event. The expected plant response to this type of event would be to immediately extinguish the fire and to determine the need to initiate alternative/dedicated shutdown. While the fire is being extinguished, assuming that the Control Room remains habitable, the remaining Control Room operators would continue to perform their duties as trained, responding to alarms and monitoring important plant parameters.

Despite this, the post-fire safe shutdown analysis for a control room fire must assume fire damage to all of the systems and equipment located within the Control Room fire area. Additionally, the analysis assumes that all automatic functions will be lost and a loss of offsite power will occur. Consequently, the operators will be forced to evacuate the control room and to safely shut down the unit from an emergency control station(s). The size and intensity of the exposure fire necessary to cause this damage are not determined, but are assumed to be capable of occurring regardless of the level of combustibles in the area, the ignition temperatures of these combustible materials, the lack of an ignition source, the presence of automatic or manual suppression and detection capability; and the continuous manning in the control room.

Generic Letter 86-10, Response to Question 5.3.10, states, "Per the criteria of Section III.L of Appendix R a loss of offsite power shall be assumed for a fire in any fire area concurrent with the following assumptions:

- a. *The safe shutdown capability should not be adversely affected by any one spurious actuation or signal resulting from a fire in any plant area; and*
- b. *The safe shutdown capability should not be adversely affected by a fire in any plant area which results in the loss of all automatic function (signals, logic) from the circuits located in the area in conjunction with one worst case spurious actuation or signal resulting from the fire; and*
- c. *The safe shutdown capability should not be adversely affected by a fire in any plant area which results in spurious actuation of the redundant valves in any one high-low pressure interface line.*

The analysis must consider the effects of each potential spurious operation and the mitigating action(s) that may be necessary for each. These conservative assumptions form the design basis for control room fire mitigation.

As with the post-fire safe shutdown analysis performed in areas where redundant safe shutdown paths are used, the analyst must be cautious not to improperly apply the conservative assumptions described above, for example, the assumption that unprotected circuits in a given fire area are damaged by the fire. This assumption is conservative only in terms of not being able to credit the systems and equipment associated with these circuits in support of post-fire safe shutdown. If the analyst, however, were to assume that these circuits were to be damaged by the fire when this provided an analytical advantage, this would be nonconservative. For example, assuming that fire damage results in a loss of offsite power may be nonconservative in terms of heat loads assumptions used in an analysis to determine the need for HVAC systems.

D.4 APPENDIX R REGULATORY REQUIREMENTS AND GUIDANCE

Appendix R Section III.G.3 provides the requirements for alternative or dedicated shutdown capability used to provide post-fire safe shutdown. Section III.G.3 states:

3. *Alternative or dedicated shutdown capability and its associated circuits,¹ independent of cables, systems or components in the areas, room or zone under consideration, shall be provided:*
 - a. *Where the protection of systems whose function is required for hot shutdown does not satisfy the requirement of paragraph G.2 of this section; or*
 - b. *Where redundant trains of systems required for hot shutdown located in the same fire area may be subject to damage from fire suppression activities or from the rupture or inadvertent operation of fire suppression systems.*

In addition, fire detection and a fixed fire suppression system shall be installed in the area, room, or zone under consideration.

III.G.3 Footnote 1 - Alternative shutdown capability is provided by rerouting, relocating or modification of existing systems; dedicated shutdown capability is provided by installing new structures and systems for the function of post-fire shutdown.

To satisfy the requirements of Section III.G.3 and use alternative or dedicated shutdown capability, the cables, systems or components comprising the alternative or dedicated shutdown capability must be independent of the area under consideration. Alternative/dedicated shutdown capability meeting the requirements of Section III.G.3 must satisfy the requirements of Section III.L. Section III.L.1 provides requirements on the shutdown functions required for the systems selected for alternative/dedicated shutdown. It also provides the minimum design criterion for the systems performing these functions.

L. Alternative and dedicated shutdown capability.

- 1. Alternative or dedicated shutdown capability provided for a specific fire area shall be able to (a) achieve and maintain subcritical reactivity conditions in the reactor; (b) maintain reactor coolant inventory; (c) achieve and maintain hot standby² conditions for a PWR (hot shutdown² for a BWR), (d) achieve cold shutdown conditions within 72 hours; and (e) maintain cold shutdown conditions thereafter. During the postfire shutdown, the reactor coolant system process variables shall be maintained within those predicted for a loss of normal a.c. power, and the fission product boundary integrity shall not be affected; i.e., there shall be no fuel clad damage, rupture of any primary coolant boundary, or rupture of the containment boundary.*

III.L.1 Footnote 2 - As defined in the Standard Technical Specifications.

III.G.3 Footnote 1 - Alternative shutdown capability is provided by rerouting, relocating or modification of existing systems; dedicated shutdown capability is provided by installing new structures and systems for the function of post-fire shutdown.

Section III.L.2 identifies the performance goals for the shutdown functions of alternative/dedicated shutdown systems as follows:

- 2. The performance goals for the shutdown functions shall be:
 - a. The reactivity control function shall be capable of achieving and maintaining cold shutdown reactivity conditions.*
 - b. The reactor coolant makeup function shall be capable of maintaining the reactor coolant level above the top of the core for BWRs and be within the level indication in the pressurizer for PWRs.**

- c. *The reactor heat removal function shall be capable of achieving and maintaining decay heat removal.*
- d. *The process monitoring function shall be capable of providing direct readings of the process variables necessary to perform and control the above functions.*
- e. *The supporting functions shall be capable of providing the process cooling, lubrication, etc., necessary to permit the operation of the equipment used for safe shutdown functions.*

When utilizing the alternative or dedicated shutdown capability, transients that cause deviations from the makeup function criteria (i.e., 2.b above) have been previously evaluated. A short-duration partial core uncover (approved for BWRs when using alternative or dedicated shutdown capability) and a short duration of RCS level below that of the level indication in the pressurizer for PWRs are two such transients. These transients do not lead to unrestorable conditions and thus have been deemed to be acceptable deviations from the performance goals²⁸. For Appendix R plants, these conditions may not meet the requirements of III.L and an exemption request may be needed.

Section III.L.7 also highlights the importance of considering associated non-safety circuits for alternative shutdown capability by stating the following:

"The safe shutdown equipment and systems for each fire area shall be known to be isolated from associated non-safety circuits in the fire area so that hot shorts, open circuits, or shorts to ground in the associated circuits will not prevent operation of the safe shutdown equipment."

Additional guidance on the topic of alternative/dedicated shutdown has been provided in the following documents:

- NRC Generic Letter 81-12
- NRC Information Notice 84-09
- NRC Generic Letter 86-10.

Furthermore, based on the guidance information in IN 85-09 as indicated below, the availability of redundant fusing should be considered when relying on transfer switches.

During a recent NRC fire protection inspection at the Wolf Creek facility, it was discovered that a fire in the control room could disable the operation of the plant's alternate shutdown system. Isolation transfer switches of certain hot shutdown systems

²⁸ NRC Letter December 12, 2000 (ML003776828) states, with respect to BWRs, "The staff reiterates its longstanding position that SRV/LPS is an appropriate means of satisfying Section III.G.3 of Appendix R (regardless of whether SRV/LPS can be considered to be a means of redundant hot shutdown capability)." Later the staff also concludes that "SRV/LPS meets the requirements of a redundant means of post-fire safe shutdown under Section III.G.2 of 10 CFR Part 50, Appendix R."

would have to be transferred to the alternate or isolated position before fire damage occurred to the control power circuits of several essential pumps and motor-operated valves at this facility. If the fire damage occurred before the switchover, fuses might blow at the motor control centers or local panels and require replacements to make the affected systems/components operable. This situation existed because the transfer scheme depended on the existing set of fuses in the affected circuit and did not include redundant fuses in all of the alternate shutdown system circuits. For most of the transfer switches, the situation would not cause a problem because the desired effect after isolation is the deenergization of power. In instances where the system/component has to be operable or where operation might be required to override a spurious actuation of a component (such as a motor-operated valve), replacement of fuses may have become necessary. In such cases, troubleshooting/repair would be required to achieve or maintain hot shutdown.

Additional guidance for selecting the process monitoring functions for alternative shutdown is provided in IN 84-09 as indicated in the following excerpt from GL 86-10.

1. Process Monitoring Instrumentation

Section III.L.2.d of Appendix R to 10 CFR Part 50 states that "the process monitoring function shall be capable of providing direct readings of the process variables necessary to perform and control" the reactivity control function. In I&E Information Notice 84-09, the staff provides a listing of instrumentation acceptable to and preferred by the staff to demonstrate compliance with this provision. While this guidance provides an acceptable method for compliance with the regulation, it does not exclude other alternative methods of compliance. Accordingly, a licensee may propose to the staff alternative instrumentation to comply with the regulation (e.g., boron concentration indication). While such a submittal is not an exemption request, it must be justified based on a technical evaluation.

For Appendix R Section III.G.3, the area/room/zone under consideration should be provided with a fixed suppression system and fire detection.

Additional guidance regarding the requirements for suppression and detection in rooms or fire zones relying on alternative/dedicated shutdown is provided in GL 86-10 Question 3.1.5.

3.1.5 Fire Zones

QUESTION

Appendix R, Section III.G.3 states "alternative or dedicated shutdown capability and its associated circuits, independent of cables, systems or components in the area room or zone under consideration...." What is the implied utilization of a room or zone concept under Section III.G. of Appendix R? The use of the phraseology "area, room or zone under consideration" is used again at the end of the Section III.G.3. Does the requirement for detection and fixed suppression indicate that the requirement can be limited to a fire zone rather than throughout

a fire area? Under what conditions and with what caveats can the fire zone concept be utilized in demonstrating conformance to Appendix R?

RESPONSE

Section III.G was written after NRC's multi-discipline review teams had visited all operating power plants. From these audits, the NRC recognized that it is not practical and may be impossible to subdivide some portions of an operating plant into fire areas. In addition, the NRC recognized that in some cases where fire areas are designated, it may not be possible to provide alternate shutdown capability independent of the fire area and, therefore, would have to be evaluated on the basis of fire zones within the fire area. The NRC also recognized that because some licensees had not yet performed a safe shutdown analysis, these analyses may identify new unique configurations.

To cover the large variation of possible configurations, the requirements of Section III.G were presented in three Parts:

Section III.G.1 requires one train of hot shutdown systems be free of fire damage and damage to cold shutdown systems be limited. [NRC has stated that 1) Section III.G.2 does not allow the use of operator manual actions without prior approval to demonstrate compliance with Section III.G.2 when redundant trains are located in the same fire area, and 2) despite Section III.G.1, compliance with Section III.G.2 needs to be demonstrated when redundant trains are located in the same fire area. Rulemaking currently in progress will impact this position. Repairs to, or manual operation of, equipment required for cold shutdown are allowed in accordance with current regulations and regulatory guidance.]

Section III.G.2 provides certain separation, suppression and detection requirements within fire areas; where such requirements are met, analysis is not necessary. [As clarified in Section 3.4.1.6 of this document (excepting emergency control stations), depending on a plant's licensing basis, exemption requests, deviation requests and GL 86-10, Fire Hazards Evaluations or Fire Protection Design Change Evaluations may be used to demonstrate equivalency to the separation requirements of Section III.G.2 as long the ability to achieve and maintain safe shutdown is not adversely affected.] [Note the current NRC position above on the use of unapproved operator manual actions]

Section III.G.3 requires alternative dedicated shutdown capability for configurations that do not satisfy the requirements of III.G.2 or where fire suppressants released as a result of fire fighting, rupture of the system or inadvertent operation of the system may damage redundant equipment. If alternate shutdown is provided on the basis of rooms or zones, the provision of fire detection and fixed suppression is only required in the room or zone under consideration.

Section III.G recognizes that the need for alternate or dedicated shutdown capability may have to be considered on the basis of a fire area, a room or a fire zone. The alternative or dedicated capability should be independent of the fire area where it is possible to do so (See Supplementary Information for the final rule Section III.G). When fire areas are not designated or where it is not possible to have the alternative or dedicated capability independent of the fire area, careful consideration must be given to the selection and location of the alternative or dedicated shutdown capability to assure that the performance requirement set forth in Section III.G.1 is met. Where alternate or dedicated shutdown is provided for a room or zone, the capability must be physically and electrically independent of that room or zone. The vulnerability of the equipment and personnel required at the location of the alternative or dedicated shutdown capability to the environments produced at that location as a result of the fire or fire suppressant's must be evaluated.

These environments may be due to the hot layer, smoke, drifting suppressants, common ventilation systems, common drain systems or flooding. In addition, other interactions between the locations may be possible in unique configurations.

If alternate shutdown is provided on the basis of rooms or zones, the provision of fire detection and fixed suppression is only required in the room or zone under consideration. Compliance with Section III.G.2 cannot be based on rooms or zones.

See also Sections #5 and #6 of the "Interpretations of Appendix R."

Additional guidance regarding alternative shutdown is found in GL 86-10 Enclosure 1 "Interpretations of Appendix R" and Enclosure 2 "Appendix R Questions and Answers" Section 5. Question 5.3.10 of GL 86-10 addresses the plant transients to be considered when designing the alternative or dedicated shutdown system:

5.3.10 Design Basis Plant Transients

QUESTION

What plant transients should be considered in the design of the alternative or dedicated shutdown systems?

RESPONSE

Per the criteria of Section III.L of Appendix R a loss of offsite power shall be assumed for a fire in any fire area concurrent with the following assumptions:

a. The safe shutdown capability should not be adversely affected by any one spurious actuation or signal resulting from a fire in any plant area; and

b. The safe shutdown capability should not be adversely affected by a fire in any plant area which results in the loss of all automatic function (signals, logic) from the circuits located in the area in conjunction with one worst case spurious actuation or signal resulting from the fire; and

c. The safe shutdown capability should not be adversely affected by a fire in any plant area which results in spurious actuation of the redundant valves in any one high-low pressure interface line.

This response defines a bounding design basis plant transient that should be considered to result during a fire that ultimately requires control room evacuation (this could be a control room fire or a fire in another area, depending upon the plant design). During such a fire, the operator would be expected to perform as trained. The operator would respond to any alarms, follow all plant procedures, and effectively and safely control the unit. The fire causing control room evacuation, however, could cause damage that affects the operator's ability to use all systems available for controlling the unit. In the unlikely event that control room evacuation is required, the response to question 5.3.10 provides a bounding plant transient that describes the expected worst-case conditions for such an event.

- The first condition that must be met is to be able to achieve and maintain safe shutdown in the event that offsite power is lost. This condition was specified as a part of the design basis because the potential for a loss of offsite power exists during a fire, since, in most plants, breaker control for the offsite power breakers is installed in the control room.
- The second condition that must be satisfied is that a single spurious operation may occur as a result of the fire and this spurious operation cannot adversely impact the safe shutdown capability. This condition was specified as a part of the fire design basis because there is some potential for a spurious operation to occur due to the high concentration of equipment controls within the control room. The specific worst-case single spurious operation, however, was not defined. The requirement for addressing a worst-case spurious signal is met by identifying any spurious operation that has the potential to adversely affect the safe shutdown capability and to evaluate the effects on the safe shutdown capability on a one-at-a-time basis.
- The third condition is that it should be assumed that all automatic functions capable of mitigating the effects of the postulated spurious operation are also defeated by the fire. This condition was prescribed in order to prevent crediting automatic functions for mitigating the effects of a worst-case single spurious signal when the controls for these automatic functions are also contained in the control room and other fire areas.
- The fourth condition is that protection must be provided to assure that the safe shutdown capability is not adversely affected by a fire that causes the spurious operation of two redundant valves in any high-low pressure interface line. Preventing the spurious operation of two redundant valves in a high-low pressure interface can

be important because the systems available may not be specifically designed to mitigate the effects of a LOCA.

Because of its specialized nature, the alternative/dedicated shutdown capability needs to be specifically directed by plant procedure(s). Other regulatory acceptance criteria must also be met.

D.5 METHODOLOGY DIFFERENCES APPLICABLE TO ALTERNATIVE / DEDICATED SHUTDOWN

The following are the differences between the "baseline" methodology provided in the body of this document and the requirements that must be applied to alternative/dedicated shutdown.

- The ability to achieve and maintain safe shutdown must be demonstrated for the condition of a loss of offsite power.
- Specific shutdown procedures must be developed for alternative/dedicated shutdown.
- The alternative/dedicated shutdown capability and its associated circuits must be physically and electrically independent of the cables, systems, and components in the area under consideration. Isolation transfer switches and redundant fusing unaffected by the fire or electrical and physical isolation and manual manipulation of equipment could be provided to ensure alternative or dedicated shutdown. Cold shutdown equipment can be repaired and operated to achieve cold shutdown within 72 hours. For the case of the alternative/dedicated shutdown area fire, potential spurious operations are assumed to occur as noted earlier in the discussion of GL 86-10 Question 5.3.10. Typically, alternative/dedicated circuit designs provide isolation/transfer switches, for safe shutdown equipment circuits, that when actuated will remove faults/spurious operations that may occur during the time of control room evacuation. Emergency control stations, such as remote shutdown panels, are typically provided with display instrumentation and other equipment/system status indications that alert the operators to spurious actions that may have occurred prior to the plant operators reaching the local stations and taking control. If the circuit can be isolated by the actuation of an isolation/transfer switch, the transfer switch should be provided²⁹. For those circuits in the affected fire area that are not provided with transfer switches, each identified potential and credible spurious operation must be identified to determine if mitigating actions are required. Similarly, for those circuits in the affected fire area prior to isolation/transfer that are provided with transfer switches, each identified potential and credible spurious operation must be identified, to assure that the isolation/transfer capability has provided the means to restore the component to its desired shutdown position. These mitigating actions cannot take credit for the loss of offsite power or loss of automatic actuation logic signals to the extent that this assumption would provide an analytical advantage. All mitigating

²⁹ See Generic Letter 81-12 Clarification, dated March 22, 1982.

actions need to be evaluated for acceptability using current NRC guidelines to ensure that safe shutdown can be achieved and maintained.

- Cold shutdown must be achievable within 72 hours.
- Areas where must have a fixed fire suppression system and fire detection installed.

D.6 ADDITIONAL OPERATOR ACTIONS RECOMMENDED FOR CONTROL ROOM EVACUATION

The primary goal for Control Room fires is to achieve safe shutdown. Guidance on actions to be taken is found in Generic Letter 86-10 Question 3.8.4. As a secondary consideration, in helping to minimize the impact of the effects of a fire on the potential property loss, additional operator actions could be useful if included in the plant procedures for control room evacuation. The following are examples of some beneficial actions. Licensees should identify actions that provide a positive benefit in terms of alternative post-fire safe shutdown and include these in the governing procedures.

The following actions should be considered for inclusion in the control room evacuation procedures as immediate operator actions to be performed prior to leaving the control room. These actions are in addition to performing the reactor scram/trip that is already endorsed for this event.

- a. Closing the Main Steam Isolation Valves.
- b. [BWR] Closing the Main Steam drain lines.
- c. [BWR] Tripping the feed pumps and closing the feed pump discharge valves.
- d. [PWR] Isolation of letdown.

This is done at the Auxiliary Shutdown Panel for some PWRs.

These actions could be a benefit in minimizing the potential for flooding of the main steam lines outside of primary containment (BWRs), minimizing the potential of an overcooling event (PWRs), and conserving RCS inventory (PWRs).

To prevent damage to equipment important to alternative post-fire safe shutdown at the emergency control station, the following actions should be considered for immediate operator actions in the procedures governing shutdown at the emergency control stations (some of these actions are performed by operators not at the auxiliary shutdown panel):

- (1) Upon arrival at the emergency control station, assure that the pumps (Service Water, Component Cooling Water, etc.) that provide cooling to the Emergency Diesel Generators are running. If the pumps are not running, start them immediately. [In the event of a loss of offsite power, the Emergency Diesel

Generators may receive a start signal. If the pumps providing cooling to the Emergency Diesel Generators are not running, then the Diesel Generators could be damaged. Performing this action as an immediate operator action upon arrival at the emergency control station will provide added assurance that the Diesel Generators will not be damaged.]

- (2) Upon arrival at the emergency control station, assure that an open flow path exists for any pumps that are running. If the pump is running, but not injecting, then assure that the pump minimum flow valve is open. If the pump minimum flow valve cannot be opened, trip the pump. Performing this as an immediate operator action upon arrival at the emergency control station will provide added assurance that these pumps will not be damaged.
- (3) [PWR] Upon arrival at the emergency control station, trip the Reactor Coolant Pump (RCP) to protect the RCP seals.

Licensees using such actions for alternative/dedicated shutdown must be able to demonstrate that these actions can be carried out according to appropriate regulatory acceptance criteria.

D.7 REFERENCES

- D.7.1 Generic Letter 81-12, "Fire Protection Rule," February 20, 1981.
- D.7.2 Generic Letter 86-10, "Implementation of Fire Protection Requirements," dated April 24, 1986.
- D.7.3 10 CFR 50 Appendix R, Fire Protection for Operating Nuclear Plants.
- D.7.4 IN 84-09 – Lessons Learned from NRC Inspections of Fire Protection Safe Shutdown Systems (10 CFR 50 Appendix R), Revision 1, March 7, 1984.
- D.7.5 IN 85-09 - Isolation Transfer Switches and Post-Fire Safe Shutdown Capability, January 31, 1985,

APPENDIX E

ACCEPTANCE CRITERIA

OPERATOR MANUAL ACTIONS AND REPAIRS

I. PURPOSE

This appendix provides guidance regarding the use of operator manual actions and repairs to equipment required for post-fire safe shutdown.

II. INTRODUCTION

Operator manual actions may involve manual control, local control or manual operation of equipment. Operator manual actions on equipment for the purpose of performing its required safe shutdown function are allowed based on the criteria provided in this appendix in Section VII. Repairs may be performed to equipment required for cold shutdown. This appendix provides the criteria to assure that the reliance on operator manual actions or repairs is appropriate. These criteria are intended to assure that the actions specified are capable of being performed, and that reliance on them is balanced within the overall safe shutdown strategy for a given fire area.

III. RELIANCE ON OPERATOR MANUAL ACTIONS

Automatic control functions are a design feature provided to mitigate or limit the consequences of one or more design basis accidents. NRC Generic letter 86-10 Section 5.3.10 suggests that post-fire safe shutdown be able to be accomplished without reliance on these automatic functions. Therefore, automatic control functions are not required for post-fire safe shutdown. As a result, manual operation of the systems available for mitigating the effects of plant fires is required. This Appendix provides the criteria for determining when an operator manual action is allowed by NRC and when NRC approval for the use of an operator manual action in support of post-fire safe shutdown is required.

Specific plant protective functions, due to the nature of their design in assuring safe and reliable plant operation, require special consideration for a fire event. The RPS Scram function is one such system. Due to the required design features of RPS Scram System, automatic or manual Reactor Scram circuitry cannot be fully protected from the effects of fire-induced circuit failures. Due to the importance of this system to reactor safe shutdown for multiple design conditions, re-design of the RPS Scram circuitry is not feasible. To assure the Reactor is scrammed for all fire conditions, it is recommended that each licensee assure that the Emergency Operating Procedure (EOP) action to implement the requirements of EO-113 is linked to their post-fire safe shutdown procedures. This action is considered to be acceptable, feasible and reliable for all fire

conditions, i.e. III.G.1/III.G.2 and/or III.G3./III.L. [Reference BWROG Paper on NRC IN 2007-07.]

IV. DIFFERENTIATING BETWEEN OPERATOR MANUAL ACTIONS AND REPAIRS

The fundamental difference between operator manual actions and repairs is definitional. Both are subject to timing limitations, feasibility, and resource constraints. The NRC has placed additional limitations on the use of repairs, such that they may only be used to achieve and maintain cold shutdown conditions. This distinction provides the opportunity for licensees to maintain hot shutdown for an extended period of time, if necessary, while repairs are performed to equipment that is required to either transition to, or maintain cold shutdown.

From an operational perspective, there is no meaningful distinction whether an action is defined as an operator manual action or a repair, since the same considerations apply.

V. DEFINITIONS

This appendix on operator manual actions relies upon definitions contained in Section 6. For the definition of terms used in this appendix, refer to Section 6, Definitions.

VI. CRITERIA

To credit the use of operator manual actions or repairs to achieve post-fire safe shutdown, certain criteria must be met. The first criteria for operator manual actions is that the operator manual action must be allowed. Section VII of this Appendix provides the criteria for determining whether an operator manual action is allowed. For those actions that are allowed, the remaining sections of this Appendix apply in determining whether the specific allowed action is feasible. To credit an operator manual action not allowed based on the criteria in Section VII, NRC approval through an exemption request or a license amendment is required. In processing an exemption request and/or license amendment, the licensee submitting the exemption request or amendment should consider the requirements of NUREG 1852. NRC has stated that exemption requests and license amendments for operator manual actions will be evaluated for feasibility and reliability against the criteria contained in NUREG 1852.

Due to the similarity between operator manual actions and repairs from the operational perspective, most of these criteria in this appendix apply to both. There are, however, a small number of additional criteria applied only to repairs. These additional criteria for repairs only are identified as such below.

Criteria Applicable to Both Operator Manual Actions and Repairs

NOTE: The generic term "actions" is used below, in order to refer to operator manual actions and Repairs collectively, without creating cumbersome language. If the specific term

Operator Manual Action or Repair is used below, it is used intentionally to show some specific distinction.

- There shall be sufficient time to travel to each action location and perform the action. Actions should be verified and validated by plant walkdowns using the current procedure. The action must be capable of being identified and performed in the time required to support the associated shutdown function(s) such that an unrecoverable condition does not occur. Previous action locations should be considered when sequential actions are required.
- Fire tests indicate that spurious actuations do not typically occur for 30 minutes or more, especially for thermoset cable, allowing for additional action time. For example, actions to lock out charging pumps prior to pump start or close PORV block valves prior to PORV opening may be considered feasible. In the later case, closing the block valve may not prevent the re-opening of the block valve due to spurious operation.
- There shall be a sufficient number of plant staff available to perform all of the required actions in the times required, based on the minimum shift staffing. The use of personnel to perform actions should not interfere with any collateral fire brigade or control room duties they may need to perform as a result of the fire. Administrative controls shall exist to ensure that the personnel necessary to perform actions are available when required, and that unexpected absences are promptly corrected. If staff augmentation consistent with the licensee's Emergency Plan Implementing Procedures is credited, then the licensee must demonstrate that un-recoverable conditions would not occur in the time period before staff augmentation is achieved.
- The action location shall be accessible. In evaluating actions and the route through the plant for performing any actions, consideration should be given to the potential effects of temperature, humidity, radiation levels, smoke, and toxic gases. Actions required in a fire area experiencing a fire, or that require travel through a fire area experiencing a fire, may be credited if it is demonstrated that these actions are not required until the fire has been sufficiently extinguished to allow completion of necessary actions in the fire area. In addition, if the action required is to be performed in the fire area experiencing the fire, it must be assured that fire damage within the fire area does not prevent completion of the action. NOTE: NUREG-0737 II.B.2 addresses dose limitations for operators performing emergency response actions. Specifies that GDC 19 applies to operator actions post accident, i.e., 5 rem whole body (or it's equivalent to any part of the body) for the duration of the accident.
- The action locations and the access and egress path for the actions shall be lit with 8-hour battery-backed emergency lighting. Tasks that are not required until after 8 hours do not require emergency lights as there is time to establish temporary lighting. The path to and from actions required at remote buildings (such as pump

house structures) does not require outdoor battery backed lights, if other lighting provisions are available (portable lights, security lighting, etc.).

- There should be indication, which is unaffected by the postulated fire, that confirms that an action is necessary and that the action, once completed, has achieved its objective. This indication is not required to be a direct reading instrument and may be a system change (level, pressure, flow, amps, temperature, etc.). Additional instrumentation may be needed to properly assess spurious operation, however it may not be necessary to make a diagnosis of the specific spurious operation that occurred, if symptom-based plant procedures provide the appropriate guidance to respond to the situation. If pre-emptive actions will be taken to preclude spurious actuations, then event-based procedures should be provided for the situation.
- Administrative controls shall be provided to ensure that any tools, equipment or keys required for the action shall be functional, available, and accessible. This includes consideration of self-contained breathing apparatus (SCBA) and personnel protective equipment, if required. This also includes the availability of ladders or special equipment, if these items are required for access.
- There shall be provisions for communications to allow coordination of actions with the main control room or the alternative shutdown facility, if required. The nature of the action, and the need for coordination with other related actions or the control room should be considered when determining what type of communication is required.
- Guidance (e.g., procedures, pre-fire plan, etc.) should be provided to alert the operator as to when actions may be required in response to potential fire damage. This guidance shall be provided in locations that will be accessible during and after the fire. The guidance may be prescriptive or symptomatic. Specific event-based procedures are required for activities not addressed in existing operating procedures (normal, abnormal, emergency) for actions and repairs as a result of fire-induced failures that cannot be readily diagnosed using fire protected information to the operator. The "skill of the craft" should be considered when determining the level of procedural guidance to provide. Typically, plant operators should be capable of performing actions without detailed instructions. Detailed instructions should be readily available, if required. Guidance should likewise be provided to the operator as to when to perform repairs in response to potential fire damage. The guidance shall provide the level of detail required to enable plant personnel to perform the task. Personnel shall be trained and qualified, as appropriate, to perform the specified actions, in accordance with INPO's Systematic Approach to Training.
- The complexity and number of operator manual actions required for safe shutdown shall be limited, such that their successful accomplishment under realistically severe conditions is ensured for a given fire scenario.

Additional Criteria Specific to Repairs

- Repairs may only be used to achieve and maintain cold shutdown (not hot shutdown).
- Hot shutdown must be capable of being maintained for the time required to perform any necessary repairs to equipment or systems needed to transition to and/or maintain cold shutdown.
- Additional non-operating personnel (e.g. maintenance, instrument and control technicians, electricians) may be relied upon to perform repairs, provided their availability is consistent with plant's Emergency Plan Implementing Procedures.

Other Types of Actions

When performing the post-fire safe shutdown analysis, additional actions that are not credited in the post-fire safe shutdown analysis may be identified that have a positive benefit to the safe shutdown scenario such as minimizing the shutdown transient or reducing commercial property damage. Since these actions are not specifically required by the regulations or the safe shutdown analysis, it is not necessary to provide 8-hour emergency lighting or communication for these actions. It is also not required to specifically address the required timing for these actions. Similarly, operator manual actions specified as precautionary or confirmatory backup actions (prudent, but unnecessary or redundant) for a primary mitigating technique that are not credited in the post-fire safe shutdown analysis do not require 8-hour emergency lights, communications or timing considerations.

VII. Process for Assessing Whether an Operator Manual Action is Allowed Under the Current Regulations

Background

In 2001, industry inspection activity led to regulatory interest in post-fire operator manual actions. This led to a number of developments, including:

Proposed rulemaking

Withdrawal of proposed rulemaking

Plans for resolution of the issue and associated enforcement discretion

Clarification on the scope of allowed/approved operator manual actions

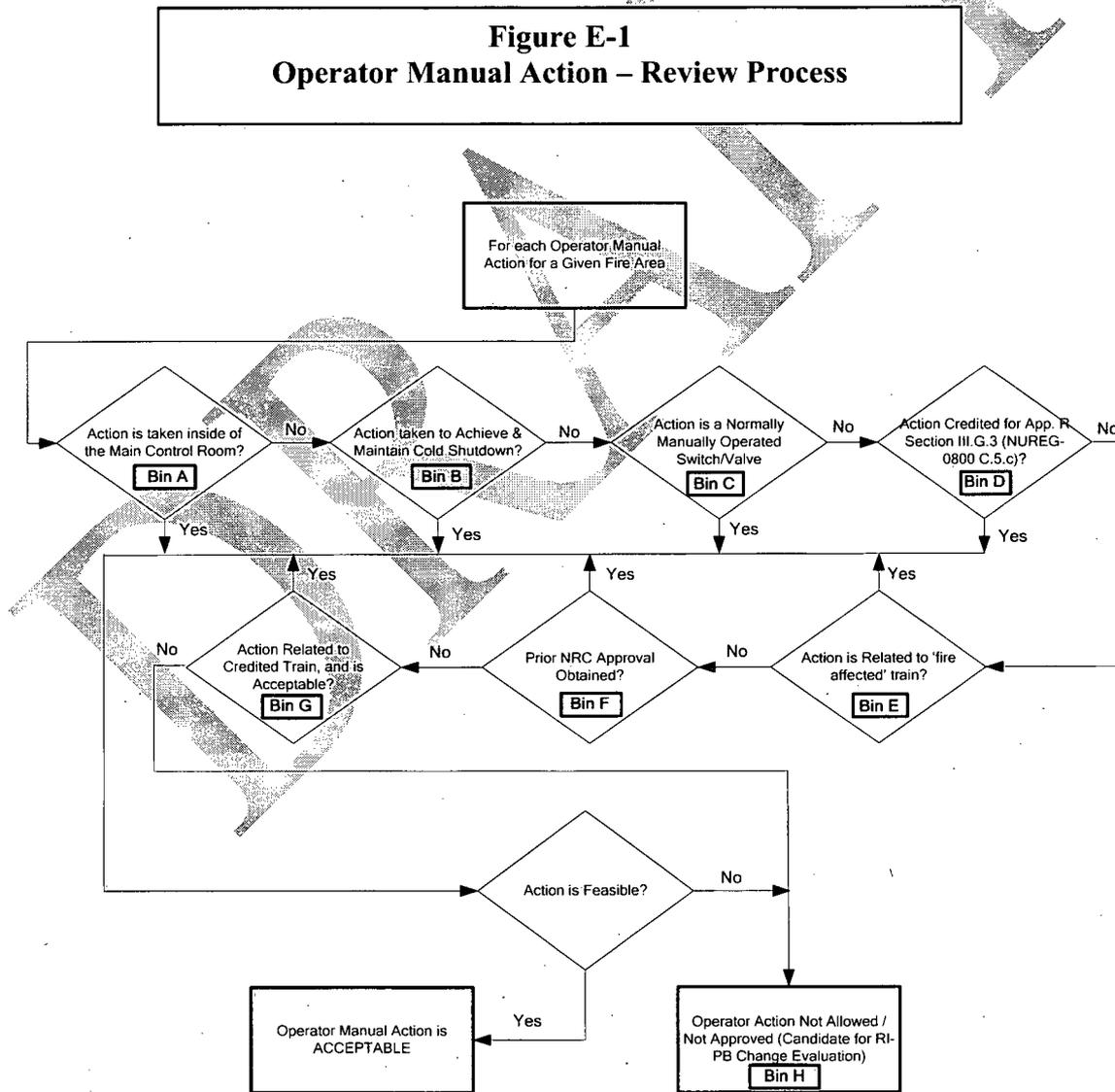
NUREG-1852, which provides feasibility and reliability guidance for exemptions

A March 2006 NRC public meeting, related correspondence, and subsequent RIS 2006-10 provided information regarding types of operator manual actions that would be considered allowable under a licensee's fire protection licensing basis.

A Frequently Asked Question (FAQ) 06-0012 was developed for plant's transitioning to a new fire protection licensing basis based in accordance with 10 CFR 50.48(c) (NFPA 805). FAQ 06-0012 was developed in order to define which operator manual actions were allowed/approved under a plant's current (pre-transition) fire protection licensing basis, which would be either 10 CFR 50, Appendix R or in accordance with the plant-specific fire protection license condition. Although FAQ 06-0012 was developed for NFPA 805 transition, the process is directly applicable to licensees that are not transitioning to NFPA 805.

Process for Evaluation of Operator Manual Actions

Figure E-1 depicts this general process for determining whether a operator manual action is allowed under the current fire protection licensing basis. The 'bin' identifiers are for ease of reference.



Operator manual actions that are allowed and/or have been previously reviewed and approved by the NRC (as documented in an approved exemption/deviation/safety evaluation report) meet current fire protection regulatory requirements. Examples of allowed operator manual actions include:

- Operator manual operation from the control room or emergency control station(s)
[Bin A]
- Repairs or operator manual actions credited either for transitioning to or maintaining cold shutdown equipment [Bin B]
- Manual operation of normally operated manual switches and valves where separation/protection is provided for redundant safe-shutdown trains in accordance with Section III.G.1 or III.G.2 of 10 CFR 50, Appendix R (or applicable sections of NUREG-0800) [Bin C]
- NRC Letter to NEI dated May 16, 2002 states: "With proper analysis, manual actions are allowed for fire safe shutdown activities under the following circumstances: manual operation of normally operated manual switches and valves"
- Operator manual actions credited for compliance with Section III.G.3 of 10 CFR 50, Appendix R (or Section C.5.c of NUREG-0800). [Bin D]
- NRC Letter to NEI dated May 16, 2002 states: "With proper analysis, manual actions are allowed for fire safe shutdown activities under the following circumstances: manual operation of equipment used to meet the requirements of Section III.G.3 for Alternative or Dedicated Shutdown of Appendix R to 10 CFR Part 50, where meeting performance criteria of Section III.L is required"
- RIS 2006-10 states: "Paragraph III.G.2 allows the licensee to use the alternative shutdown method described in paragraph III.G.3 of Appendix R if the licensee cannot meet the requirements of paragraph III.G.2."
- Operation of fire affected equipment for fire areas that meet the separation requirements of Section III.G.1 of 10 CFR 50, Appendix R (or applicable sections of NUREG-0800). See Figure E-2. [Bin E]
- NRC Letter to NEI dated May 16, 2002 states: "With proper analysis, manual actions are allowed for fire safe shutdown activities under the following circumstances: operation of equipment for which cables are located in fire areas that meet Section III.G.1 of Appendix R to 10 CFR Part 50, by having redundant cables and equipment in a completely different fire area"
- Operation of fire affected equipment for fire areas that meet the protection requirements of Section III.G.2 of 10 CFR 50, Appendix R (or applicable sections of NUREG-0800) for redundant trains. See Figure E-3. [Bin E]
- RIS 2006-10 states: "As discussed during a March 1, 2006, public meeting, if one of the redundant trains in the same fire area is free of fire damage by one of the specified means in paragraph III.G.2, then the use of operator manual actions, or other means necessary, to mitigate fire-induced operation or maloperation to the second train may be considered in accordance with the licensee's fire protection program and license condition since paragraph III.G.2 has been satisfied."

Operator manual actions to address spurious operations that affect the credited safe shutdown success path may or may not be allowed, depending upon the affect of the fire on the safe shutdown components. [Bin G]

A special case of "fire affected train" exists where two redundant trains have components/cables in a given fire area, and both trains take suction from a common tank. In this case, a manual action would be allowed to secure the fire affected train, since the credited train is protected (meets III.G.2 requirements) even though the manual action would need to be accomplished before the common tank level decreased to the point where operation of the credited train would be affected. This is acceptable since the common point in the system is the tank, which is still free of fire damage (Figure E-4). This example was discussed in the June 9, 2006 public meeting. (ML061980016)

An example where operator manual action to address spurious actuations that affect the credited safe shutdown success path would not be allowed is the case where the credited function is to inject water to one of the Steam Generators (reactor) and a spurious actuation causes a diversion from the credited flow path. Even though the minimum required injection flow can be maintained and the operator manual action can be accomplished prior to the function being disabled, the operator manual action is not allowed since the credited train is not free of fire damage (the diversion of flow must be terminated at some point or the credited safe shutdown path will not be successful). (Figure E-5). An example of this configuration is BWR example 3 of the June 9, 2006 public meeting (ML061980016). This clarification of the 'credited train not being free of fire damage' was provided by the NRC on September 20, 2007. (ML072820168)

In addition to allowed operator manual actions some manual actions may have been previously reviewed and approved by the NRC [Bin F] (as documented in an approved exemptions/deviations/safety evaluation reports).

In some instances the NRC may have reviewed and approved [Bin F] an operator manual action in an SER without granting an exemption/deviation request.

- RIS 2006-10 states: "For pre-1979 licensees, a staff decision in a safety evaluation report (SER) that approves the use of operator manual actions, in lieu of one of the means specified in paragraph III.G.2, does not eliminate the need for an exemption. Pre-1979 licensees who have SERs, but not a corresponding exemption, which approve manual actions should request an exemption under 10 CFR Part 50.12, citing the special circumstances of section 50.12(a)(2)(ii), citing the SER as the safety basis, and confirming that the safety basis established in the SER remains valid. The staff expects to grant the exemption on these bases without further review."

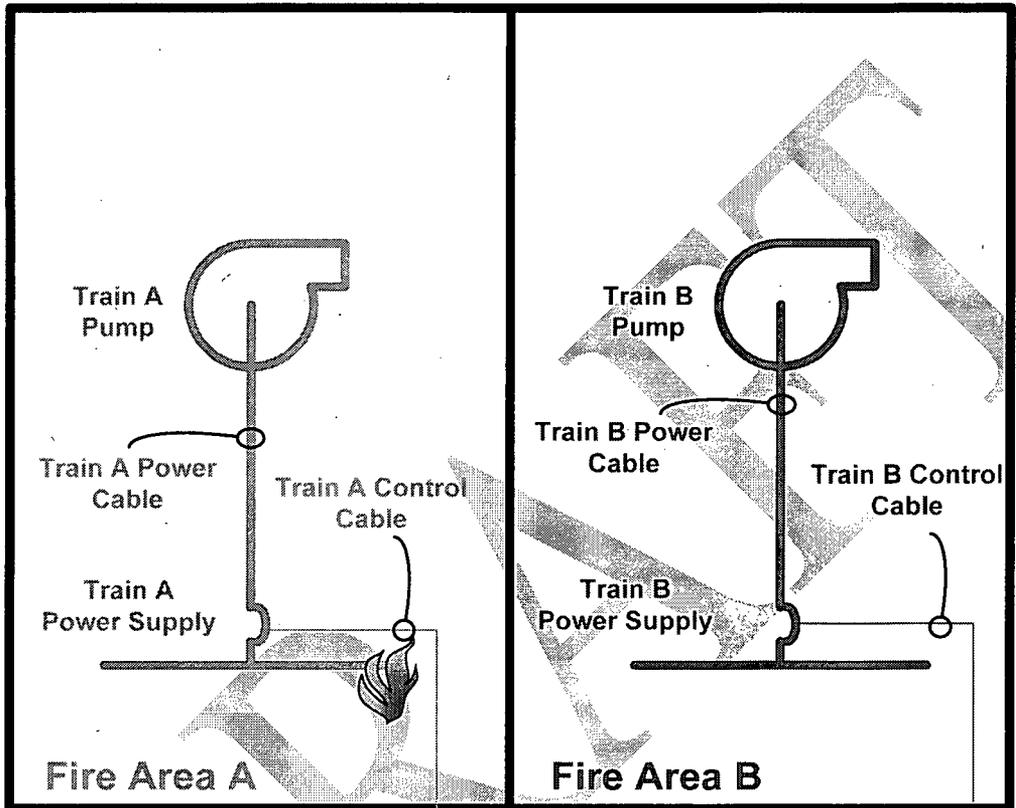
Pre-1979 licensees who have SERs, but not a corresponding exemption, which approves operator manual actions, should verify that the basis for acceptability in the SER is still valid. If the basis for acceptability is still valid, then no additional regulatory action is required.

- RIS 2006-10 states: "Since plants licensed to operate on or after January 1, 1979 (post-1979 licensees), are not required to meet the requirements of paragraph III.G.2, a staff decision in an SER that approves the use of manual operator actions does not require exemption under 10 CFR 50.12. Post-1979 licensees may be requested to demonstrate, as part of the NRC Reactor Oversight Process, that the use of an operator manual action would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire consistent with their license."

Operator manual actions that are not allowed or have not been previously reviewed and approved by the NRC should be addressed via the appropriate regulatory process, if intended to be relied upon as a long term strategy (e.g., exemption request, license amendment request, etc.). Examples of operator manual actions that are not allowed are provided in summary of the June 9, 2006 Public Meeting (ML061950327, ML061980016)

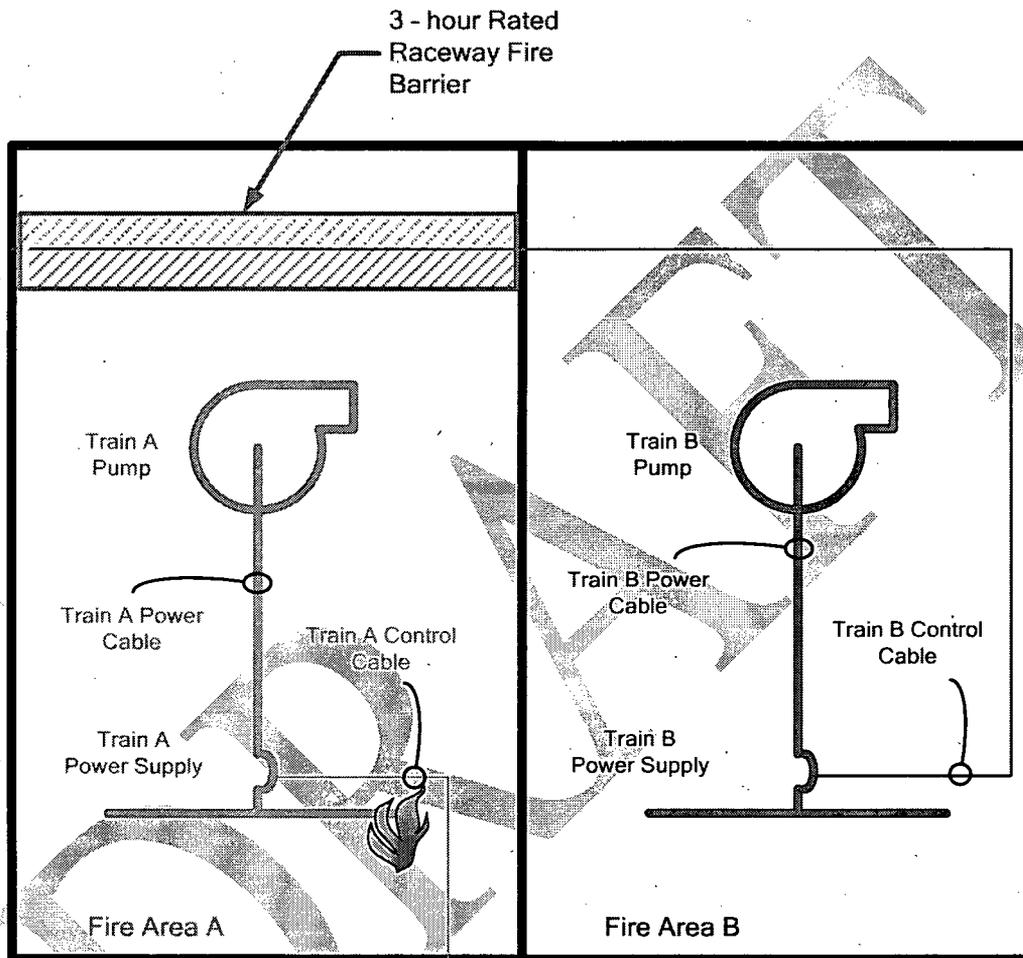
DRAFT

Figure E-2
Allowed Operator Manual Action in Fire Area Meeting
10 CFR 50, Appendix R,



Fire Area A and B meet the separation criteria of 10 CFR 50 Appendix R Section III.G.1 A postulated fire in Fire Area A could result in the spurious starting of the Train A pump, which can be mitigated by an operator manual action to de-energize the Train A Power Supply to stop Pump A.

Figure E-3
Allowed Operator Manual Action in Fire Area Meeting
10 CFR 50, Appendix R,



Fire Area B meets the separation criteria of 10 CFR 50 Appendix R Section III.G.2.a. A postulated fire in Fire Area A could result in the spurious starting of the non-credited Train A pump, which can be mitigated by an operator manual action to de-energize the Train A Power Supply to stop Pump A. This is functionally equivalent to Case in Figure E-2.

Figure E-4
Allowed Operator Manual Action – In Credited Success
Path – Common Tank Suction

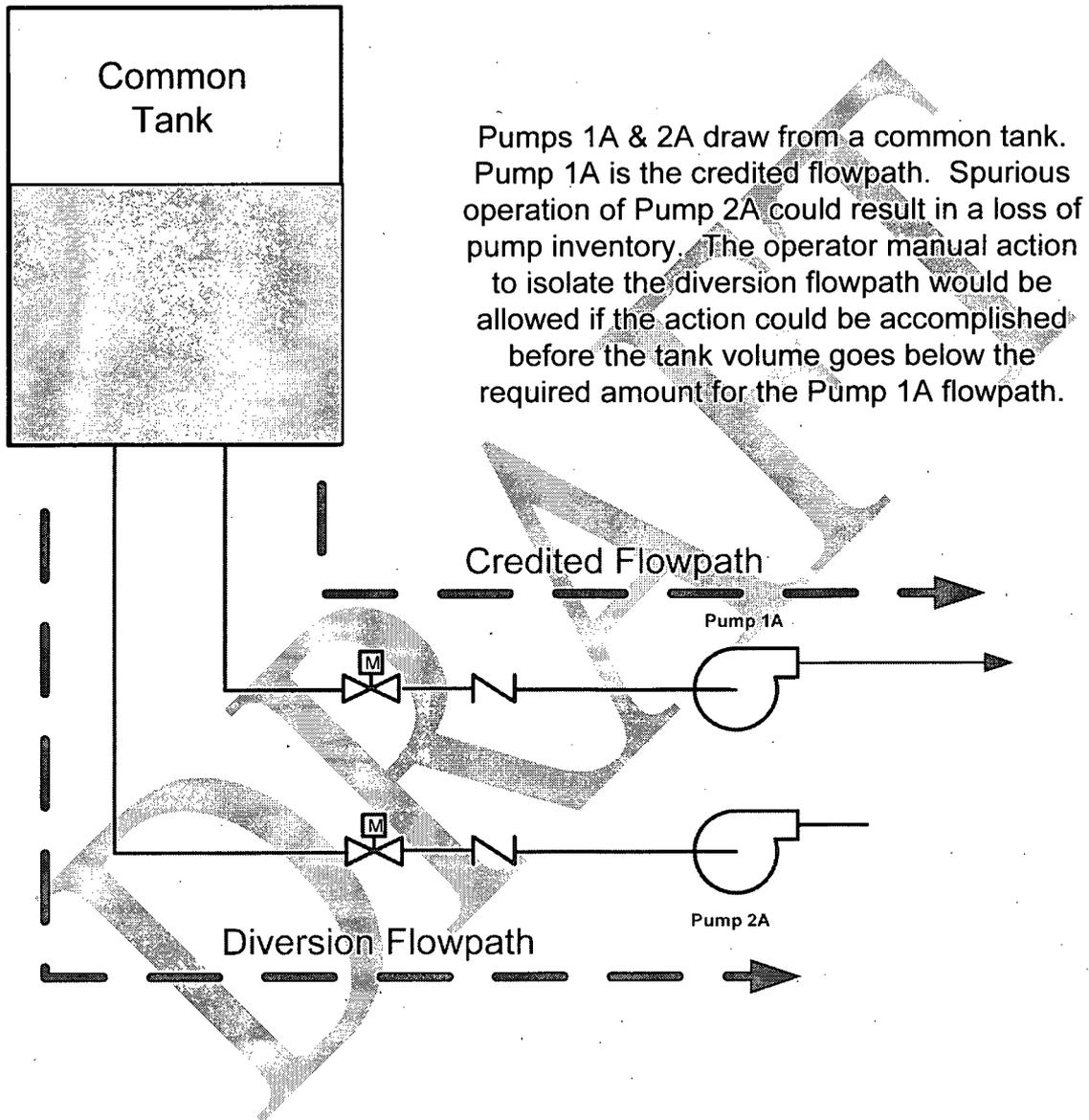
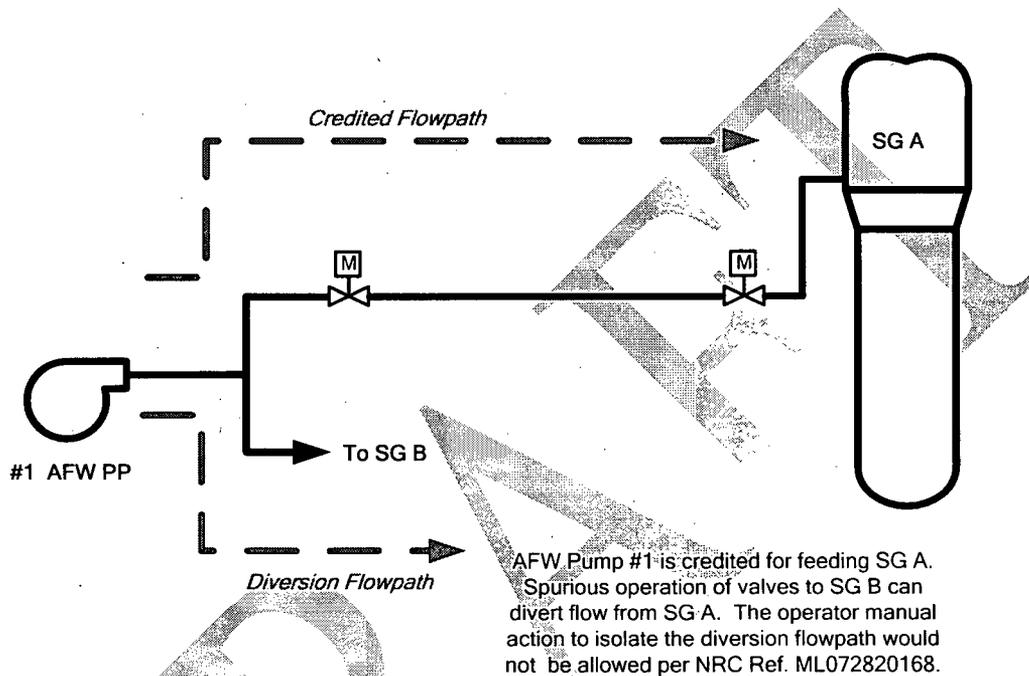


Figure E-5
Operator Manual Action – In Credited Success Path –
Auxiliary Feedwater Flow Diversion [not allowed per
NRC Ref. ML072820168]



VIII. REFERENCES

10 CFR 50 Appendix R Fire Protection for Operating Nuclear Power Plants

Draft NRC Response to 03-29-06 EPM letter, May 25, 2006 (ML061440237)

Draft NRC Response to 05-03-06 NEI letter, May 25, 2006 (ML061440251)

NEI 04-02 Frequently Asked Question 06-0012, Determining Manual Actions that Require a Change Evaluation during Transition, Revision 5, November 26, 2007 (ML073320028)

NRC Inspection Procedure 71111.05, March 18, 2005

NRC letter to NEI, Use of Manual Actions to Achieve Safe Shutdown for Fire Events, dated May 16, 2002 (ML021410026)

NRC Meeting Summary of 06-09-06 OMA Meeting, July 19, 2006 (ML061950327)

NRC Revision to Draft Response to EPM March 2006 letter, July 19, 2006 (ML061980016)

NEI 00-01 Revision 2 - Draft
December 2007

NRC Revision to Draft Response to NEI May 2006 letter, July 19, 2006 (ML061980035)

NUREG-1778, Knowledge Base for Post-Fire Safe-Shutdown Analysis, January 2004

Public Meeting Notice 20060609 on Manual Action Clarifications, May 26, 2006
(ML061390156)

RIS 2006-10 Regulatory Expectations with Appendix R Paragraph III.G.2 Operator Manual
Actions, June 30, 2006 (ML061650389)

SECY-03-0100, Rulemaking Plan on Post-Fire Operator Manual Actions, June 17, 2003

DRAFT

APPENDIX F

SUPPLEMENTAL SELECTION GUIDANCE (DISCRETIONARY)

F-1 INTRODUCTION

This appendix is to be used to supplement the information in Section 4 in support of the plant specific review of the Generic List of MSO in Appendix G to supplement the list of MSOs to be reviewed on a Plant Unique basis.

F-2 P&ID OR LOGIC DIAGRAM REVIEW

The first step is to select target components/combinations that could impact safe shutdown. This first step limits consideration to combinations of multiple spurious actuation evaluations whose maloperation could result in loss of a key safety function, or immediate, direct, and unrecoverable consequences comparable to high/low pressure interface failures. These consequences are noted hereafter as "unacceptable consequences." Potential circuit failures affecting these safe shutdown target components may have been considered in previous circuit analyses, but perhaps not for IN 92-18 or multiple spurious actuation concerns.

A system engineer can identify component combinations that can result in a loss of system safety function or immediate and unrecoverable consequences. Then, an electrical or safe shutdown engineer can identify areas where these component combinations have power, control, or instrument cables routed in the same fire area.

The review for component combinations can be performed with P&IDs or safe shutdown logic diagrams (if available) or both. The review should focus in on "pinch points" where the system function or safe shutdown (SSD) function would be failed. Failure of the entire SSD function is not necessary for identification of component combinations but would be a limiting case assuming all identified components can fail with the same fire. Component combinations that do not fail the entire SSD function can be as important as combinations failing the entire function, especially if there is only a single component or manual/operator action remaining for the SSD function, or if the remaining SSD equipment is potentially unreliable. Some internal events PRA input may be helpful for determining potentially unreliable equipment or manual/operator actions.

The results of the P&ID or logic diagram review would be a list of potentially important component combinations to be treated with the NEI 00-01 methodology. Since the internal events PRA scope and fire protection SSD scope are different, the SSD review may provide potential combinations that have not been included in the internal events PRA. Also, it is possible for this review of the P&ID to identify component

combinations not identified by SSD analysis (because it requires multiple spurious operations) or internal events PRA (because of a high level of redundancy). The final list of identified component combinations should be combined with any internal events PRA combinations (from the PRA review below) for a final list for analysis.

F.3 PRA REVIEW

The internal events PRA can be used to determine potentially important component combinations through either cutset review or through model reanalysis. These are both described below. Note that a PRA review may identify combinations which include equipment not included in the Fire Protection Safe Shutdown list. The important components identified in the pilot applications were already in the Safe Shutdown Equipment List, but the internal events PRA scope includes additional equipment that is not in this list.

F.3.1 Cutset or Sequence Review

The plant analyst may review cutsets or sequence results (in this discussion, this is simplified to "cutsets") with high contributions to core damage frequency, including common cause failures that include combinations with unacceptable consequences as noted above. These cutsets will generally contain few terms, have a significant contribution to core damage frequency, and include one or more basic events that can be affected by fire, either through direct damage or through spurious operation. Cutsets reviewed should include cutsets sorted by probability, and cutsets sorted by order (from least number of events in the cutset to most). Review of the cutsets would identify combinations where one or more components may spuriously operate, and whose spurious operation may be significant. The pilot project showed the spurious operation components are typically not in the top cutsets, since random (non fire-induced) spurious operation is typically a low probability event. It may be helpful to manipulate the cutsets using a cutset editor by setting the basic event probabilities associated with spurious operation events to 1.0, and re-sorting the cutsets³⁰. For example, by setting all of the motor-operated valve (MOV) spurious operation events to 1.0 and re-sorting, the top cutsets may now include potentially important component combinations for MOV cables.

Generally, the significance of each combination cannot be determined from a cutset review. However, the relative significance of one combination versus another can be performed when the cutsets include similar equipment. For example, when two similar cutsets, one with two spurious operations required and one with the same two and one

³⁰ If the licensee has a full internal events PRA model, re-running with spurious failures set to a high screening value (>0.1) could recover cutsets truncated in the internal events PRA that could contribute non-negligibly to the core damage frequency due to fire.

additional spurious operation required are compared, the latter combination is probably less important. This type of comparison would require review of the other events in the cutsets, and the fire characteristics for the event causing equipment damage.

One additional consideration is that the cutset review does not need to include review of cutsets for initiating events that cannot be fire induced. For example, cutsets for steam generator tube rupture or large LOCA need not be reviewed. Typically, the review can be performed on turbine/reactor trip cutsets, loss of offsite power cutsets, and induced small LOCA cutsets. Similarly, cutsets requiring failure of components in both redundant trains can be dismissed as long as it can be assured that one redundant train's component is protected in each fire area. A review of the plant's fire Individual plant Examination of External Events (IPEEE) can determine what initiating events can result from a fire.

F.3.2 PRA Model Manipulation

If a logic model of the plant core damage sequences including all possible fire events is available, this model can be exercised/manipulated to identify component combinations of interest to risk significance evaluation described in Section 5 of this document.

The level and amount of model manipulation can range from a single re-resolution of the model, to many re-resolutions following modeling changes. The analysis discussed below is based on the limited analysis used in support of the pilot application of NEI-00-01, with discussion of additional runs considered during the pilot.

A basic analysis that can provide significant results is solution of the internal events PRA model with all basic events set to 1.0 (True) that can potentially spuriously operate following a major fire. The McGuire pilot performed this analysis by also setting the transient and loss of offsite power initiating events to 1.0. The types of components and PRA basic events that should be set to 1.0 in the model include:

- MOV spuriously open or close
- AOV spuriously open or close
- PORV spuriously open or close
- Spurious actuation of automatic actuation signals

The cutsets or sequence results can be reviewed to identify component combinations that are potentially significant. Review of the results will show patterns of cutsets that can be grouped or combined. For example, a cutset with a PORV spuriously operating and charging injection failures could repeat hundreds of times with both PORVs combined with the multiple combinations failing injection and the random failures not set to 1.0 in the model. These hundreds of cutsets can be grouped into limiting combinations based on order (less spurious operations leading to core damage) and/or likelihood (less random failures leading to core damage). Initial review of the cutsets should also look for other component basic events that could occur due to spurious operation following a fire. If

additional basic events are identified, additional model solutions may be necessary prior to selection of the component combinations to be analyzed.

If the PRA model includes some fire PRA sequences, additional runs with the fire PRA initiating events set to 1.0 should be performed. In this case, the PRA results would identify component combinations important for particular fire areas (or fire areas with similar characteristics).

If the PRA model does not include any fire PRA sequences, model manipulation can be performed to simulate fire PRA results. For example, in the McGuire pilot analysis, additional internal events PRA runs were performed where the 4160 VAC switchgear was failed. This included two PRA runs, one with A train 4160 VAC failed, and one with B train failed. These runs simulated a switchgear fire, but also provided representative runs important if opposite train components were located in the same area. For example, cutsets were identified where A train cooling water failed due to the A train 4160 VAC failure, and B train cooling water failed due to spurious operation. This sequence could be potentially important if the cables causing the B train failure were located in an A train fire area. The B train failure (in this example) could be as a result of a diversion due to an A train valve spuriously opening.

Additional PRA runs can be performed based on the IPEEE results. The IPEEE can provide a list of important fire areas, and the equipment that potentially fails due to a fire in these areas. By setting the component basic events to 1.0 for a selected fire area, and also setting our list of spurious operation components to 1.0, a list of potentially important component combinations can be developed for the selected fire areas. This type of analysis was not performed for the pilots, other than the fire sequences already included in the PRA models.

F.3.3 Analysis of the New PRA Sequences

Some important fire-induced accident sequences of interest involving spurious operation may have been screened from the internal events and Fire PRAs. New scenarios or accident sequences not previously considered may result from Fire-Induced damage or as a result of operator actions taken in response of a fire. For example, manual action to close a PORV or PORV block valve in response to spurious operation concerns would result in the Pressurizer Safety Valve (PSV) being challenged following a pressure increase. Spurious injection could also challenge the PSV, and if water relief were to occur, it is likely the PSV would stick open. A stuck open PSV is generally considered a low probability event in an internal events PRA, but may show up as significant in a Fire PRA. Scenarios involving Steam Generator overfeed may not be considered important for an internal events PRA, but may be important for sequences involving control room evacuation where a turbine driven pump is the credited safe shutdown equipment.

Performing a Fire PRA update in order to develop possible multiple spurious combinations would not be an efficient method for developing a complete list of combinations. However, if a Fire PRA were being updated, either the scenario

development process or PSA cutset results could provide insight to developing a complete list. The scenario development, including the development of new event trees or accident sequences, could provide a useful input to the SSA analyst.

NUREG/CR-6850 (EPRI TR-1011989) methods for consideration for MSOs includes the following additions to the PRA in step 2.5.1:

- *Sequence Considerations that were screened out of the Internal Events PRA may become relevant to the Fire PRA and need to be implemented in the Fire PRA model. For example, spurious safety injection is often screened out from the Internal Events PRA and yet may be important for fires that could cause both the spurious injection and damage to one or more pressurizer PRA such that the pressurizer SRVs are challenged. These SRVs could subsequently stick-open causing a complicating LOCA accident sequence. A review should be conducted for such scenarios originally eliminated from the Internal Events PRA to determine if the analysis needs to add components to the Fire PRA Component List as well as model those components (and failure modes) in new sequences in the Fire PRA Model.*
- *Particularly when considering the possible effects of spurious operation, new accident sequences and associated components of interest may be identified that should be addressed in the Fire PRA and go beyond considerations in the Internal Events PRA. Typically, these new sequences arise as a result of spurious events that:*
 - *Cause a LOCA: e.g., PORV opening, reactor cooling pump seal failure,*
 - *Adversely affect plant pressure control: e.g., vessel or steam generator overfill that if unmitigated could subsequently fail credited safe shutdown equipment such as a turbine-driven feedwater or auxiliary feedwater pumps, or*
 - *Introduce other "new" scenarios that may not be addressed in the Internal Events PRA.*

These fundamental steps for performing a baseline PRA review (for possible scope increases) can also be performed in support of a review for new MSO scenarios. Additional guidance is given in NUREG/CR-6850 in the following sections:

- Fire-induced initiating events, including those not modeled in the Level 1 PRA (2.5.3)
- Equipment with the potential for spurious actuation for failing Safe Shutdown Equipment (2.5.4), including new accident sequences not previously modeled.
- Additional Mitigating, Instrumentation and Diagnostic equipment important to Human Response (2.5.5).

One of the key areas of screened sequences from the internal events PRA is the modeling of Interfacing Systems LOCA (ISLOCA) accident sequences. The internal events screening criteria for ISLOCA pathways would screen flow paths with 3 normally closed MOVs due to the low random failure rate of an MOV to remain closed. However, the fire-induced failure rate of an MOV spurious operation is significantly higher, and the screened scenario may need to be considered in the plant specific MSO list, given the scenario is possible (if one or more of the MOVs have power removed, then the cable criteria considerations in Appendix H would indicate the MSO is not likely).

In reviewing the Internal Events PRA for screened (or even combined) initiating events, the following should be considered:

- 1) The Initiating Event is more likely than the internal events PRA estimate (i.e., pressurizer heaters fail on).
- 2) The resulting Consequences can be worse (i.e., loss of HVAC coincident with a fire).
- 3) The Fire introduces new accident sequences not considered in the Internal Events PRA (i.e., spurious injection with PORVs closed, result in water relieve from the SRVs).

During the review of the PRA scope for possible new MSOs, the plant and operator response to a fire should be understood. In particular, if the plant procedures direct the operator to turn off power to a train of SSE, isolate a train or function, or otherwise disable equipment, then this should be accounted for in the review. In this regard;

- Credit for plant procedures to mitigate an MSO should not be used during the MSO scenario identification step, but should be used in the disposition of the MSO in the SSA.
- Negative effects of plant procedures (operator actions) should be considered when determining if a new MSO scenario should be considered.

These assumptions for the PRA input to the MSO list are conservative, but will result in a more complete list of MSOs for consideration.

The output of the above review can be used as either an input to a Fire PRA, or as consideration for additional MSOs to be identified by the Expert Panel. See the information below for additional information on this topic.

F.4 EXPERT PANEL REVIEW

F.4.1 Expert Panel Review

The expert panel process described herein supplements the information provided in Section 4.

The team for an expert panel review includes operations, engineering, electrical, PRA, and others. This process involves four phases:

- Phase 1: Preparation, including an initial list of potential accident sequences
- Phase 2: Training of the expert panel on Safe Shutdown Analysis and Multiple Spurious Operation
- Phase 3: Performance of the Expert Panel Review
- Phase 4: SSA review of the Expert Panel Results

The preparation would involve developing a list of scenarios to consider for review, including input from the PRA as described above, and the potential list of scenarios from NEI-04-06, if performed. Training will be required for participants not familiar with both the SSA process and issues related to multiple spurious. The scope of the original SSA should also be discussed. The Expert Panel Review involves group what-if discussions of both general and specific scenarios that may occur. Documentation of both issues and non-issues, and the reason they were either, was important. For example, if a possible scenario was considered not possible due to power being removed from a valve, then this is documented. This documentation can be carried over into the SSA. The expert panel process also involves a P&ID review of each system credited in the SSA, including discussions of how the flow path would change for each type of Fire Area (redundant and alternate shutdown).

The expert panel process can be run in a number of ways. A typical expert panel process involves a structured team review of systems and functions using a P&ID review. The P&ID review progresses through each P&ID by having the group review each possible flow path and consider the possibility and effect of a fire-induced MSO for that flow path. This consideration includes:

- a) Consideration of an MSO resulting in failure of the primary flow path or function.
- b) Consideration of an MSO that combines the failure of the flow path being considered in combination with other possible spurious operation to fail the primary flow path or function.

The first example would occur if two or more valves spuriously open, resulting in a diversion and failure of the credited train. The second example could occur given spurious closure of an RCP seal-cooling valve, and a simultaneous spurious closure of a seal injection valve, resulting in a possible RCP seal LOCA.

The expert panel review can also be performed using a review of flow diagrams, PRA events trees, Safe Shutdown Logic Diagrams, or similar logic structure. The general process for review of each is similar, although the methods for discussion may differ, given the variation in the information being presented to the expert panel.

Key to the expert panel process is the diverse review of Safe Shutdown Functions. This diverse review is performed by an expert panel comprised of experienced personnel in the major aspects of plant operation and fire safe shutdown. The expert panel should include the following expertise:

- Fire Protection
- Fire Safe Shutdown Analysis: This expert should be familiar with the SSA input to the expert panel and with the SSA documentation for existing spurious operations.
- PRA: This expert should be familiar with the PRA input to the expert panel.
- Operations
- System Engineering
- Electrical Circuits

Additional experts may be needed, depending on the system interactions that are discussed. For example, water relief from a safety valve may require expertise in relief valve. Additionally, a single individual may provide expertise in multiple areas, such as Fire Protection and Fire Safe Shutdown Analysis.

The expert panel will review and discuss one Safe Shutdown Function at a time. For that Safe Shutdown Function, the panel will identify possible failure mechanisms that can result from spurious operation or a combination of spurious operation and direct fire damage. Using various tools, identify "Choke Points" that could defeat safe shutdown through the previously identified failure mechanisms:

- Flow Diagrams
- Safe Shutdown Logic Diagrams
- PRA Event Trees
- PRA Results or Sensitivity Analysis

The panel will build these "Choke Points" into fire scenarios to be investigated. The scenario descriptions that results should include the identification of specific components whose failure or spurious operation would result in a loss of a safe shutdown function or lead to core damage.

Training is performed prior to the beginning of the expert panel. This training should include:

- a. Purpose and scope of the SSA
- b. PRA overview and results
- c. Overview training on the MSO issue, including
 - i. Appendix G to this document

- ii. Background on Fire-Induced Multiple Spurious
- iii. Types of circuit failures that can occur, including shorts to ground that can cause spurious component operation.
- iv. Results of the Fire Testing (EPRI/NEI Testing), including:
 1. Likelihood of various spurious operation probabilities.
 2. Timing including the likelihood that failures will occur close in time, and issues affecting time to damage.
 3. Duration

The Expert Panel will then systematically review the systems (P&IDs, etc) affecting safe shutdown and the core, for the following Safe Shutdown Functions:

- Reactivity Control
- Decay Heat Removal
- Reactor Coolant
 - Inventory Control
 - Pressure Control
- Process Monitoring
- Support Functions

Safe Shutdown Failure Mechanisms to be considered are discussed in Appendix B. These mechanisms are supplemented with input from:

- The PRA Results and sensitivity
- Additional scenarios as previously identified in the corrective action program, inspections, or other identification methods (i.e., previously identified issues).

The expert panel should make a conservative determination of the impact and likelihood of the scenario. This determination should be documented for each scenario, with specific information on each scenario being provided. Where needed, the expert panel should identify where additional information is needed to justify a disposition. For example, if a diversion flow path is considered too small to affect flow in a main flow path but some additional calculations are needed to justify the opinion, then the additional calculations should be noted. These open items should be closed prior to completion of the expert panel report.

The expert panel will likely have to meet several times to initially disposition all possible systems and flow paths potentially affecting plant safe shutdown. Additional follow-up meetings may be needed, if open items are found to not support the initial disposition of the expert panel. If, for example, the small diversion flow path discussed above does result in a significant diversion where the main flow path does not provide sufficient flow to fulfill its function, the expert panel would need to meet again on this issue.

A report of the expert panel findings should be developed. This report should be treated as a living calculation, and updated if any new information is developed or if any additional multiple

spurious scenarios require disposition. The expert panel report should identify a list of scenarios that need to be addressed by the safe shutdown analysis.

One of the lessons learned from the initial expert panels performed was that all scenarios considered, including those considered low likelihood or scenarios that would not go to core damage, should be documented. Additionally, the reason the scenario was not added to the plant specific MSO list should be documented in the report. Any supporting or supplemental analysis should be either added to the report or referenced.

F.5 SELECTION OF POTENTIALLY IMPORTANT COMPONENT COMBINATIONS

Based on the results, performance of some or all of the types of analysis discussed above will provide hundreds of thousands of possible component combinations for review. Analysis of all these combinations is not possible. The PRA output provides the largest number of possible combinations. These combinations can be screened in the expert panel or self assessment process to reduce the scenarios to those that can actually occur and those of potential significance. The final selection of component combinations for analysis needs to account for various factors affecting the final expected risk for the combinations, including:

- Expected spurious operation probability, including the combined frequency for multiple components. For example, it can easily be shown that three or more spurious operations for armored cable (with fused armor) components would most likely be unimportant, since the probability of spurious operation alone is on the order of $1E-06$.
- Conditional core damage probability listed in the cutsets
- Additional factors not in the cutsets affecting the core damage probability, including both positive factors where additional equipment may be available and negative factors such as human actions that may be less reliable following a fire
- Expected fire frequencies (i.e., combinations in high fire frequency areas may be more important than those in low fire frequency areas).

These and other factors should be used by the analysts in determining the potentially important component combinations for review, and the number of combinations that need to be evaluated for risk significance. Combining the PRA-identified combinations with the P&ID or logic diagram review should provide a comprehensive list of potentially important component combinations that should be added to the Generic List of MSOs from Appendix G.

Appendix G

Generic List of MSOs

The attached tables provide examples of BWR and PWR MSO scenarios to be included in the generic MSO lists. Presently, these lists are in development and trial, and when published, should provide a comprehensive list of MSOs for consideration for each reactor type.

DRAFT

ABD