# NEI 00-01

# GUIDANCE FOR POST-FIRE SAFE SHUTDOWN ANALYSIS

***Prepared by:***

***NEI Circuit Failure Issues Task Force***

***October, 2002***

## FIGURES

## TABLES



## ATTACHMENTS



## APPENDICES

# GUIDANCE FOR POST-FIRE SAFE SHUTDOWN 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. 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), and to address emerging safe shutdown issues from a risk-informed standpoint.

From the standpoint of deterministic safe shutdown analysis, Generic Letter 86-10 (Reference 6.1.10) attempted to provide 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 foregoing 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) and the industry response (Reference 6.4.31), it became evident that industry and NRC staff interpretations differ significantly on at least some aspects of the post-fire safe shutdown analysis requirements. The Boiling Water Reactor Owners Group (BWROG) developed a comprehensive document for BWRs to codify generally accepted deterministic safe shutdown analysis practices based on existing regulatory requirements and guidance.

The differences between the regulator and the industry led industry to propose a risk-informed method for resolving these differences. The risk methods included in this document provide a means of addressing and resolving these differences on a plant-specific basis. These methods are based on generally accepted principles of fire PRA.

### 1.1 PURPOSE

The purpose of this document is to provide a consistent process for performing a fire safe shutdown analysis and to provide a method for addressing identified issues both within and beyond a utility's licensing basis.

This document provides both deterministic and risk methods for addressing potential fire-induced circuit failure issues, either within or beyond the existing plant licensing basis. The deterministic method, derived from NRC regulation, guidance, and long-held

industry interpretations of the foregoing (incorporated into plant licensing bases) is provided for analyzing and resolving circuit failure issues. Risk-informed methods are provided to determine the risk significance of identified issues. This approach is in concert with the principle that risk-significant failures, or combinations thereof, should be addressed, and non-significant ones need not be.

The methods in this document do not require the systematic re-evaluation of a plant's post-fire safe shutdown analysis, nor do they take precedence over specific requirements accepted by the NRC in a plant's post-fire safe shutdown analysis. The deterministic methods in this document clarify industry-accepted methods based on approved licensing bases. This provides a baseline in the event that differences of opinion arise related to the interpretation of the current regulatory requirements that are not specifically described and accepted within a plant's current licensing basis. In addition, this document provides criteria for assessing the risk significance of those issues that are not included in current safe shutdown analyses, but that may be a concern because of potential risk significance. Some specific issues of concern are multiple spurious signals/operations and MOV damage as described in NRC Information Notice (IN) 92-18.

This guidance in this document reflects the position that licensee should address potential risk-significant issues regardless of whether they involve compliance with the licensing basis. This is illustrated below.

### 1.1.1 Issues Within the Licensing Basis

The plant's post-fire safe shutdown analysis is a part of the plant licensing basis. 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 manual operator actions required to support achieving either hot or cold shutdown are identified and can be implemented within the time required.

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.

However, there are interpretive differences over regulatory guidance concerning certain circuit analysis assumptions in plant post-fire safe shutdown analyses. One such difference is whether to consider the effects of fire-induced spurious actuations and subsequent effects one at a time, as reflected in Section 3 but questioned by NRC. The NRC views are not typically reflected in the plant licensing basis.

NEI 00-01 can be used to support exemptions or deviations in areas where the plant configuration clearly does not meet its own long-standing licensing basis. Section 4 provides probabilistic methods for identifying and assessing the risk significance of potential circuit failures. The risk significance screening will determine whether additional action to address these potential failures is warranted.

An example will illustrate the use of NEI 00-01 for issues clearly within the licensing basis. In this example, a licensee discovers an oversight in the implementation of its own licensing basis, and has failed to postulate a spurious actuation where one should have been postulated. The licensee can determine the significance of the issue using the methods of NEI 00-01. The licensee would place the issue in the plant Corrective Action Program (CAP) if it is significant according to the NEI 00-01 criteria, or request an exemption or deviation, or change the fire protection plan, if it is not. Normal reporting guidelines would be followed.

### 1.1.2 Issues Beyond the Plant Licensing Basis

The deterministic and probabilistic methods outlined in Sections 3 and 4 can also be used to determine the safety significance of identified issues such as multiple spurious signals/operations, and the potential for fire-induced circuit failure modes described in NRC IN 92-18 (Reference 6.3.37). As noted above, these issues are considered to be outside the licensing basis of many plants. If the user determines that additional measures are needed to prevent or mitigate the consequences of the spurious signals/operations, these methods can also be used to ensure the cost-effectiveness of these measures.

Exemption or deviations should not be required where there has been a legitimate and long-standing difference in interpreting the regulations. In these cases, a safety significance determination is useful in determining the action to be followed by the licensee without having to directly address the interpretive differences.

As an example, a licensee may have a longstanding licensing basis reflecting the postulation of any and all spurious actuations, one at a time. NRC inspectors several years ago informed the licensee that they should have considered a particular combination of two simultaneous spurious actuations in a particular fire area to maintain one train free of fire damage. As in the example of Section 1.1.1, the licensee would perform a risk significance analysis using the methods in NEI 00-01. If the licensee finds the combination to be risk significant, they should place the issue resolution in the CAP. If the licensee finds the combination to not be risk significant, however, no exemption request is required. The licensee would update its fire protection plan. The licensee remains in compliance with his own licensing basis and there is no significant safety benefit to be gained in pursuing traditional "fixes"; therefore, the health and safety of the public is preserved.

## 1.2 BACKGROUND

Reviewing past fire events can substantiate the uncertainty associated with the behavior of actual plant fires. On March 22, 1975, the Brown's 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 Brown's 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 APCSB 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 APCSB 9.5-1 or Appendix A to BTP APCSB 9.5-1. The staff reviewed the fire protection programs for compliance with the guidance.

The guidance in BTP APCSB 9.5-1 and Appendix A to BTP APCSB 9.5-1, however, did not provide specific information for determining those SSCs important to post-fire safe shutdown. To address this issue 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.

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 APCSB 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 committed to meet the guidelines of Section 9.5-1, "Fire Protection Program," of NUREG-0800, "Standard Review Plan" (SRP), which incorporated the guidance of Appendix A to BTP APCSB 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 APCSB 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 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 Brown's Ferry. Appendix R is a deterministic

approach, and it has been only recently that plants have begun to determine the risk implications of Appendix R.

The regulations, however, did not provide sufficient detail to establish clear and uniform criteria for performing post-fire safe shutdown analysis. To address this issue, the NRC Staff has issued numerous guidance documents in the form of Generic Letters and Information Notices. These documents provide insights as to the NRC staff's interpretation of the regulations and their views on acceptable methods for complying with the regulations. This document provides 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 Brown's Ferry fire resulted in damage to plant equipment important to safe shutdown. Although safe shutdown of the Brown's 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 Brown's 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 Brown's Ferry fire, solidify this conclusion regarding plant safety.

### 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 risk significance methodology evaluates the risk significance of potential failures or combinations of failures. [Note: The term "component combination" will be used throughout this report to denote one or more fire-induced component failures due to spurious actuations.] The methodology for performing the

probabilistic analysis in combination with the deterministic post-fire safe shutdown analysis is depicted in Figure 1-1.

### 1.3.2 Deterministic Method

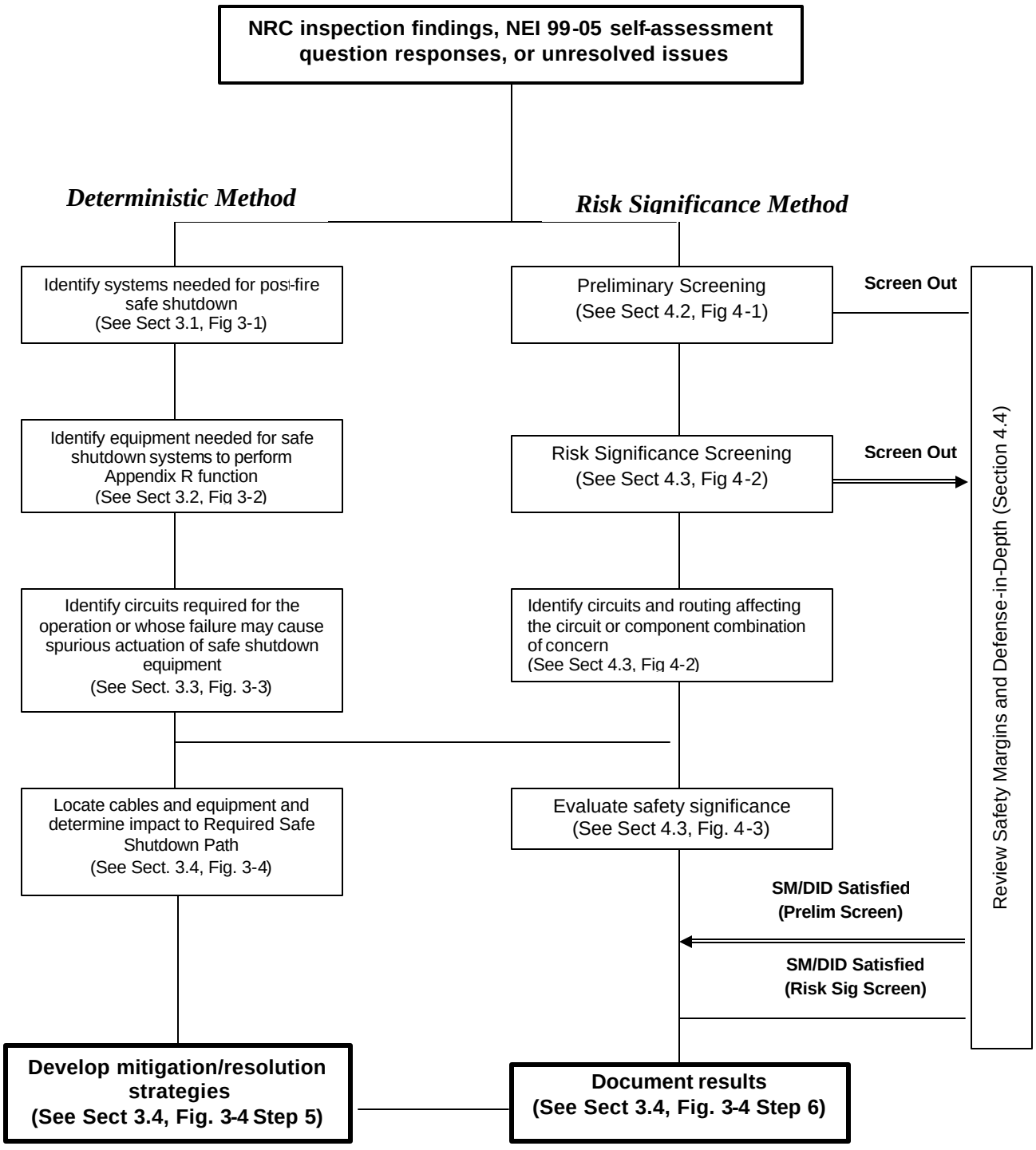
When using the deterministic methodology to address the current regulatory requirements, a basic assumption of the methodology is that there will be fire damage to systems and equipment located within a common fire area. The size and intensity of the fire required to cause this system and equipment damage is 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 shutdown in the event of a single fire in any plant fire area.

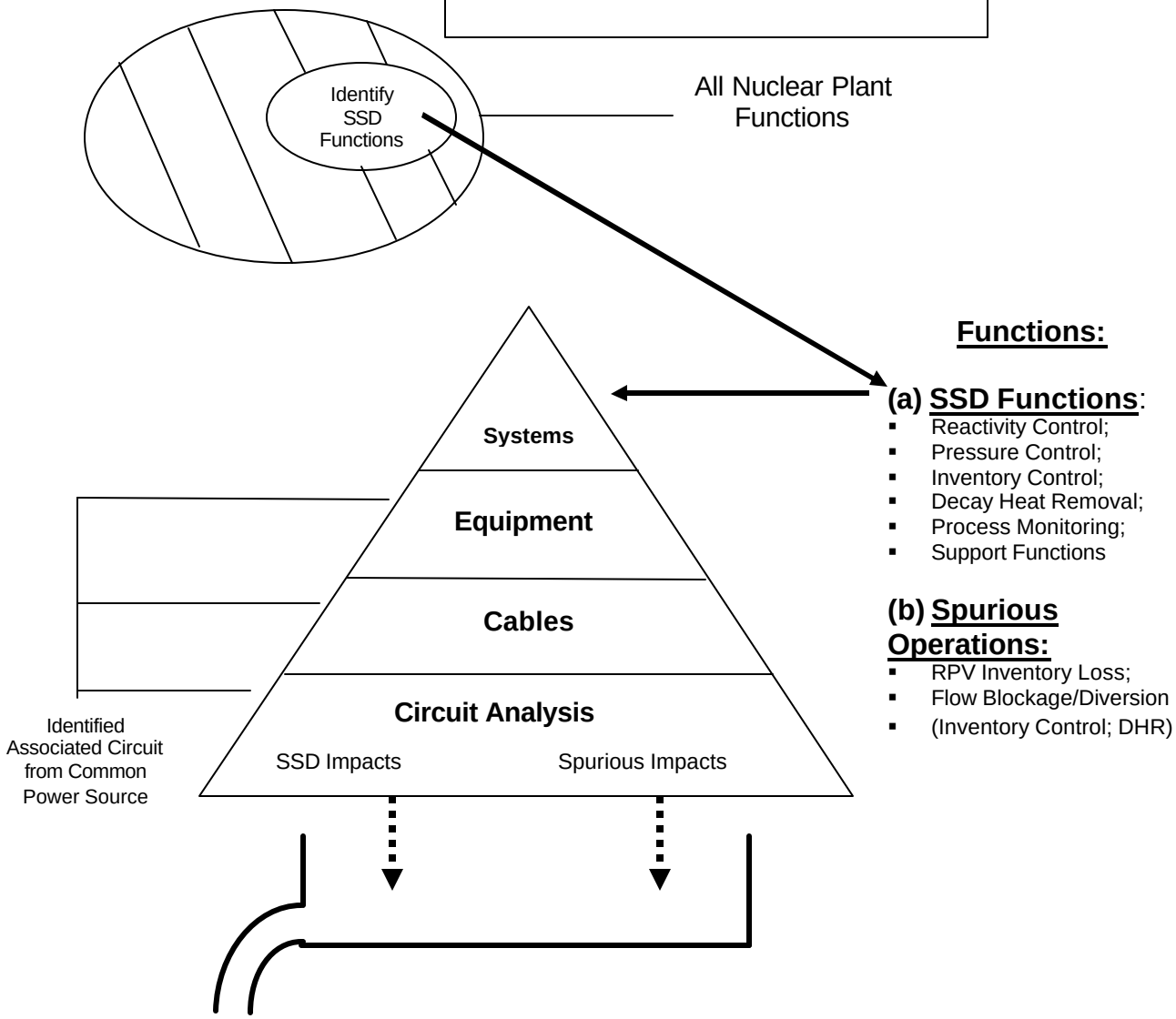
In performing a deterministic post-fire safe shutdown analysis, the analyst must be cautious not to improperly apply the conservative assumptions described above. For example, one cannot rule out fire damage to unprotected circuits in a given fire area. This assumption is conservative only in terms of 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 1-2. The specific steps are summarized in Sections 1.3.2.1 through 1.3.2.6, and discussed in depth in Section 3.

**Figure 1-1**
**NEI 00-01 Process Flow Chart**



## Figure 1-2
## Deterministic Post-fire
## Safe Shutdown Overview



#### 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 function[1].

[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.

#### 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 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

[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.

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 or flow diversion (inventory makeup capability) 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 "Hi/Lo Pressure Interfaces." Refer to Appendix C for the special requirements associated with Hi/Lo 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 be open in the fire area in which a required cable is routed).

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 circuit[2] (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.

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

### 1.3.3 Risk Significance Methods

The risk significance methods begin with the preliminary screening process described in Section 4. In doing this, the analyst first identifies potential component combinations using Section 4.1, based on known inspection or self-assessment issues. He determines whether these component combinations should be addressed. These items may need to be addressed if they are clearly within the plant licensing basis, or if they are not within the plant's licensing basis but potentially have high risk significance.

The analyst uses the screening method in Section 4.2 to perform an initial risk significance assessment and documents those potential component combinations screened out at this step. Section 4.2 is a relatively conservative process for applying a qualitative probabilistic screen. The assumptions used in the process are less conservative than those of the deterministic safe shutdown analysis process that follows it.

For failures screened out after applying Section 4.2, the analyst determines whether a successful screening out of the component combination could be supported by safety margins (SM) and defense-in-depth (DID) considerations. This process is described in Section 4.4.1. For component combinations not screened out, the deterministic safe shutdown analysis in Section 3 is performed to the extent needed to carry out the more detailed probabilistic screening analysis method described in Section 4.3. This "extent needed" includes the steps through

[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.

identifying cables and locations. If information for the component combination is already available, the appropriate steps can be skipped.

Once the deterministic analysis has progressed to the point where cables and locations for the component combination are identified, the probabilistic screening analysis in Section 4.3 can begin. Each step in the screening process is performed to determine the risk significance of a component combination under consideration. If a component combination can be screened out based on core damage frequency (CDF) and Large Early Release Frequency (LERF), additional reviews of SM/DID and uncertainty analysis are performed prior to screening. These additional reviews are described in Sections 4.3.4 and 4.4.

# 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 REGULATORYREQUIREMENTS

10CFR50 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. 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.*

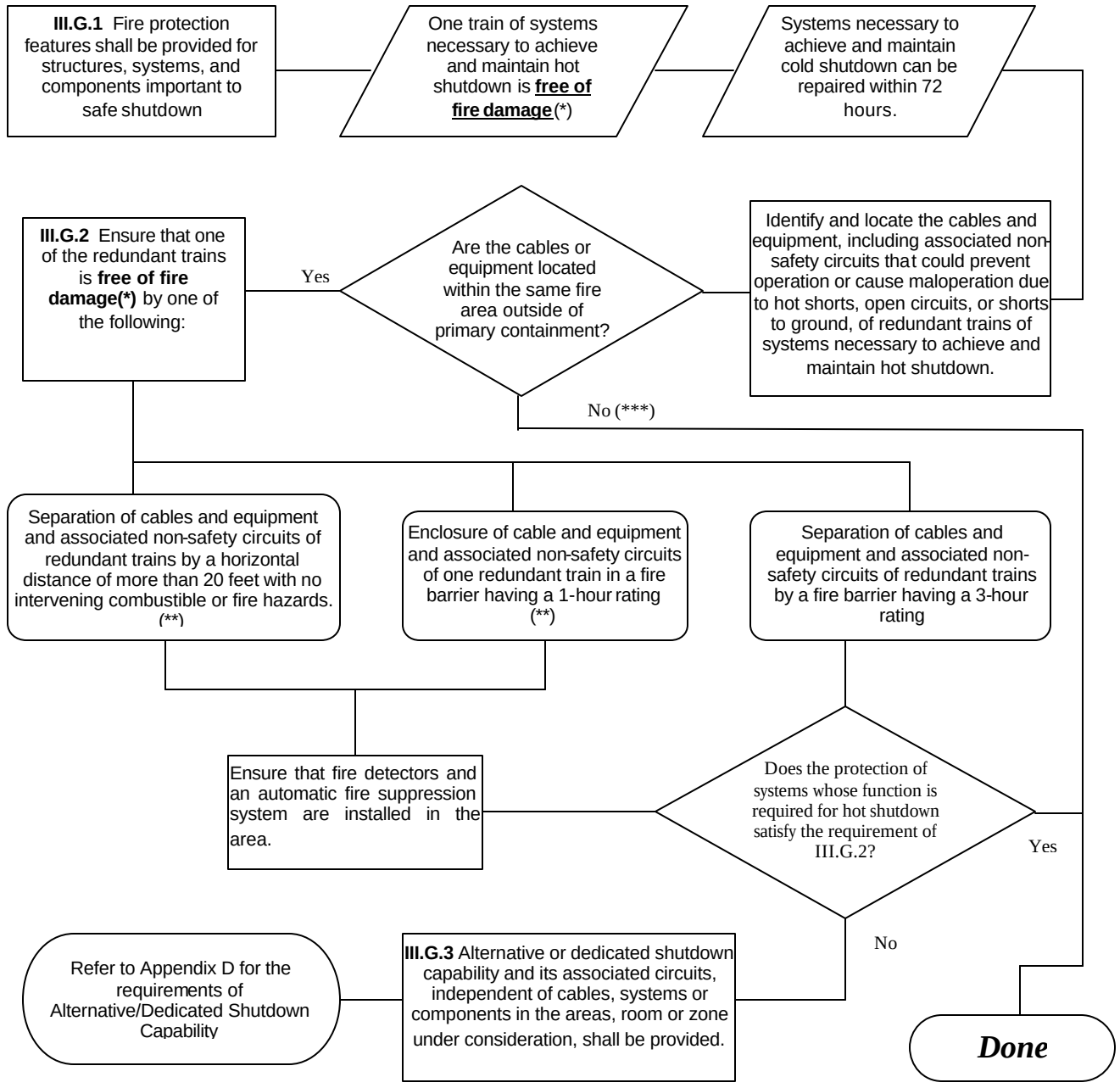
*1. Fire protection features shall be provided for structures, systems, and components important to safe shutdown. These features shall be capable of limiting fire damage so that:*

*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.*

In Section III.G there are no functional requirements specifically itemized for the structures, systems or components. The only performance goal identified is the requirement to initially achieve and maintain hot shutdown and to subsequently achieve cold shutdown once any required repairs have been completed. This performance goal can be further defined as follows: "To assure that a single fire in any plant fire area will

# 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. It may perform this function automatically, by remote control, or by manual operations*

*(**) 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 for separation, detection/suppression, or radiant energy shields as specified in Appendix R Section III.G.2 (d), (e), or (f)*

not result in any fuel cladding damage, rupture of the primary coolant boundary or rupture of the primary containment."

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. The term free of fire damage allows the operator to perform a manual action on safe shutdown equipment to accomplish its required safe shutdown function, in the event the remote/automatic function of the equipment is impacted. Section III.G.1.b allows for repairs to be performed on safe shutdown equipment used for achieving and maintaining cold shutdown. Appendix E to this document provides guidance on the use of manual operator actions and the performance of repairs. Section III.G.1 presumes that some pre-existing fire protection features have been provided, such as barriers (previously approved by the NRC under Appendix A to BTP APCSB 9.5-1). Section III.G.2 provides additional separation options that may be utilized, in the event that III.G.1 criteria have not already been met.

*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.*

Therefore, in order to comply with the regulatory requirements in Section III.G.1 and 2, it is necessary to: (1) maintain those barriers previously reviewed and approved by the NRC under Appendix A to APCSB 9.5-1 that provide separation essential for safe shutdown; (2) where redundant trains of systems necessary to achieve hot shutdown are located in the same fire area and manual operation of the required components is not achievable, 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; and (3) assure that any repairs required to equipment necessary to achieve and maintain cold shutdown can be made within 72 hours.

Section III.G.2, however, also makes provisions for the actions required in the event that none of the options described above can be used and the fire protection features are not adequate to assure that one of the hot shutdown redundant trains can be demonstrated to be free of fire damage. In these cases, Section III.G.2 invokes the requirements of Section III.G.3. Section III.G.3 requires that "Alternative" or "Dedicated" shutdown capability be provided which is independent of the area being evaluated. Refer to Appendix D to this document for the additional requirements applicable to "Alternative" and "Dedicated" shutdown capability.

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 50.59 process) may be used (when issued) to justify configurations that meet the underlying goals of Appendix Rbut not certain specific requirements.

## 2.2 REGULATORYGUIDANCE ON ASSOCIATED CIRCUITS

2.2.1 In addition to ensuring 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 insure that the safe shutdown system functions are not defeated. The analysis requires that consideration be given to cable failures that may cause spurious actuations 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. These types of circuits are collectively referred to as Associated Circuits.

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

*"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…"*

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.

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.*

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.*

## 2.3 REGULATORYINTERPRETATION 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 it's 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

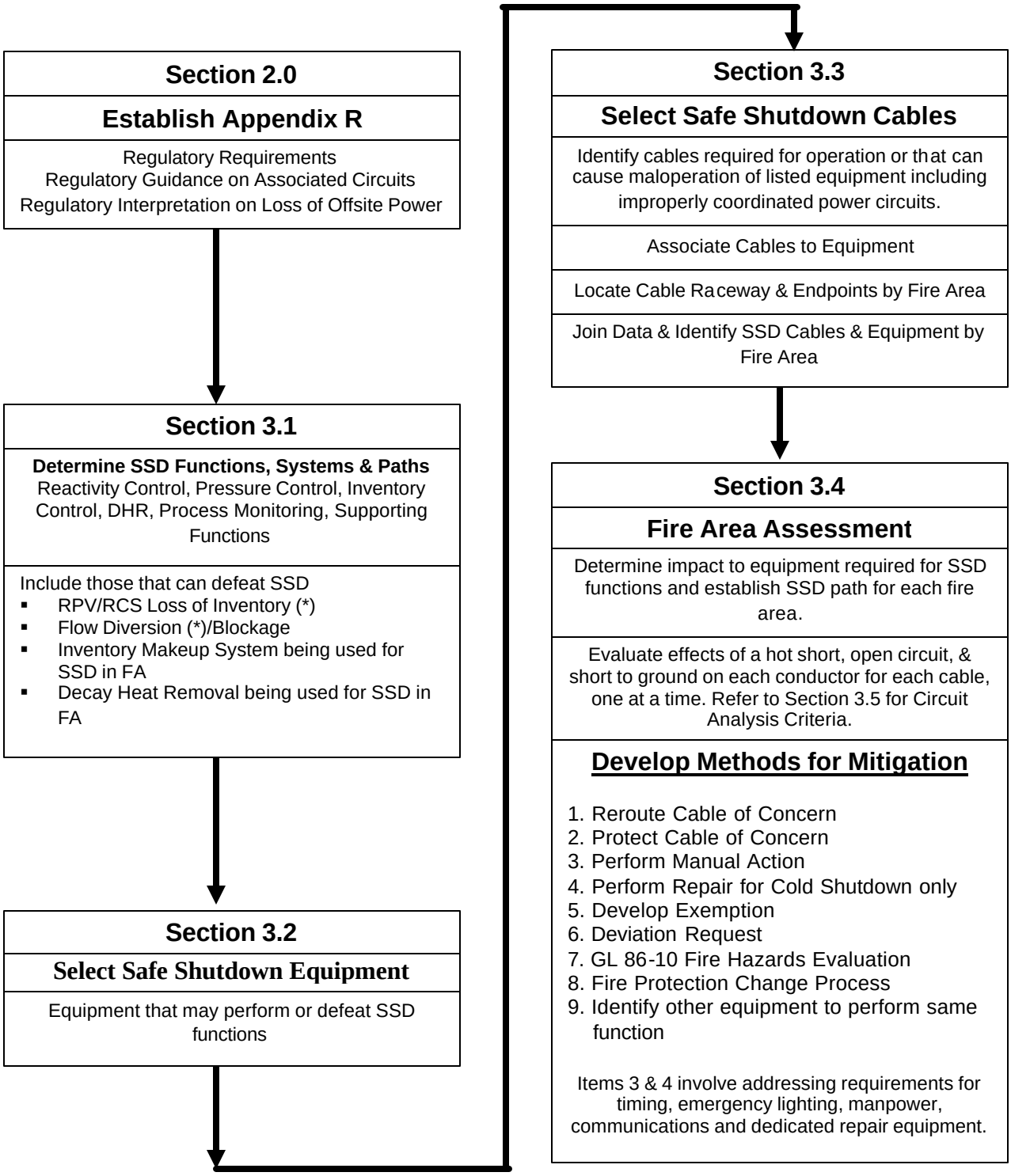
This section discusses a generic deterministic methodology and criteria that licensees can use to perform a post-fire safe shutdown analysis to meet regulatory requirements. This methodology is indicated in Figure 3-1. The methodology described in this section is one acceptable method of performing a post-fire safe shutdown analysis, but it is not the only method. Regardless of the method selected by an individual licensee, the criteria and assumptions provided in this guidance document will 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 of the defense-in-depth fire protection program and their operability must be fully considered, these items are not governed by the protection/separation requirements of Appendix R Section III.G.2. Therefore, this guidance document does not address them or their associated cables.

## 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. "Free of fire damage" allows for the use of manual operator actions to complete the required safe shutdown functions. 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. In conjunction with allowing the use of manual operator actions and repairs in support of post-fire safe shutdown, the NRC has also provided regulatory guidance related to these two aspects of safe shutdown. Refer to Appendix E to this document for the requirements associated with using manual operator actions and repairs to support post-fire safe shutdown.

## 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 safely shutting down the reactor. 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 protecting the fuel, the reactor pressure vessel and the primary containment. If these functions are preserved, then the units will be safe and 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. Spurious operations/actuations 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 make-up 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 protect the fuel and prevent damage to the reactor pressure vessel or the primary containment.

### 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 1960's and 1970's, that can be used to achieve and maintain safe shutdown per Section III.G.1 of 10CFR 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 10CFR50 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 make up/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. Any systems that are capable of achieving natural circulation are considered to be acceptable for achieving redundant safe shutdown.

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 manual actions, 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, LCOs etc. in progress. The unit(s) are assumed to be operating at full power under normal conditions and normal lineups.

3.1.1.6 No FSAR 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 Alternate 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 Safe shutdown systems 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 within this 72-hour period need not be included in the post-fire safe shutdown analysis.

3.1.1.10 Manual initiation of systems required to achieve and maintain safe shutdown is acceptable; automatic initiation of systems selected for safe shutdown is not required but may be included as an option.

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 (CRD) 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.

**[PWR] Makeup/Charging**

There must be a method for ensuring that adequate shutdown margin is maintained by ensuring borated 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)**

The SRVs are 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 ADS is not a required function.

**[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. In some cases PORVs may be used to relieve pressure.

### 3.1.2.3 Inventory Control

[BWR] Systems selected for the inventory control function should be capable of supplying sufficient reactor coolant, such that no fuel cladding damage occurs through boil-off. 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 within the indication of the pressurizer. Temporary fluctuations outside this range are permissible with the stipulation that level can be restored and unrestorable conditions do not occur. Typically, the same components providing inventory control are capable of providing pressure control.

### 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 NPSH requirements of any SSD 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 RCPs 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 (10CFR50 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).

<u>BWR</u>

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

<u>PWR</u>

- Reactor coolant temperature (Hot leg / Cold leg)
- Pressurizer pressure and level

- Neutron flux monitoring (source range)
- Level indication for various tanks
- 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 Buses either directly from the buses 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 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 125 VDC 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 RCIC and/or HPCI 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.

### 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:

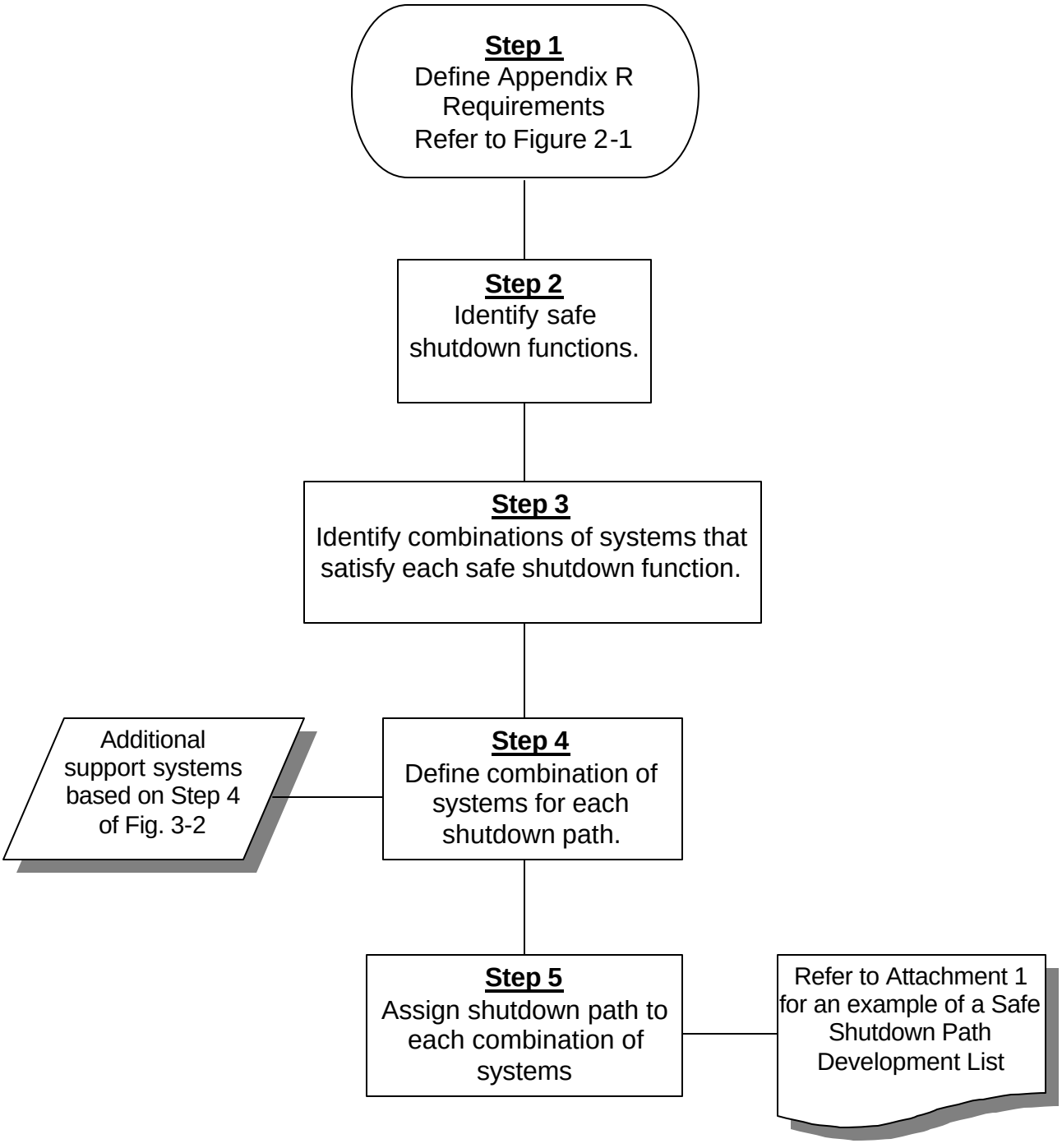
#### 3.1.3.1 Identify safe shutdown functions

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"

**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 that could impact the required safe shutdown path.

#### 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 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, associate 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 are not included in this assumption). Fire damage to a manual valve is not postulated to affect 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 that 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 up-scale, mid-scale, or down-scale 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 and impact the performance of equipment on a required safe shutdown path during the equipment selection phase.

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 to this document 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) are 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 within the safe shutdown system that could spuriously operate and impact the operation of that safe shutdown system. Assign the safe shutdown path for the affected system to this valve. During the

cable selection phase, identify additional equipment (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 Safe Shutdown Equipment List (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.

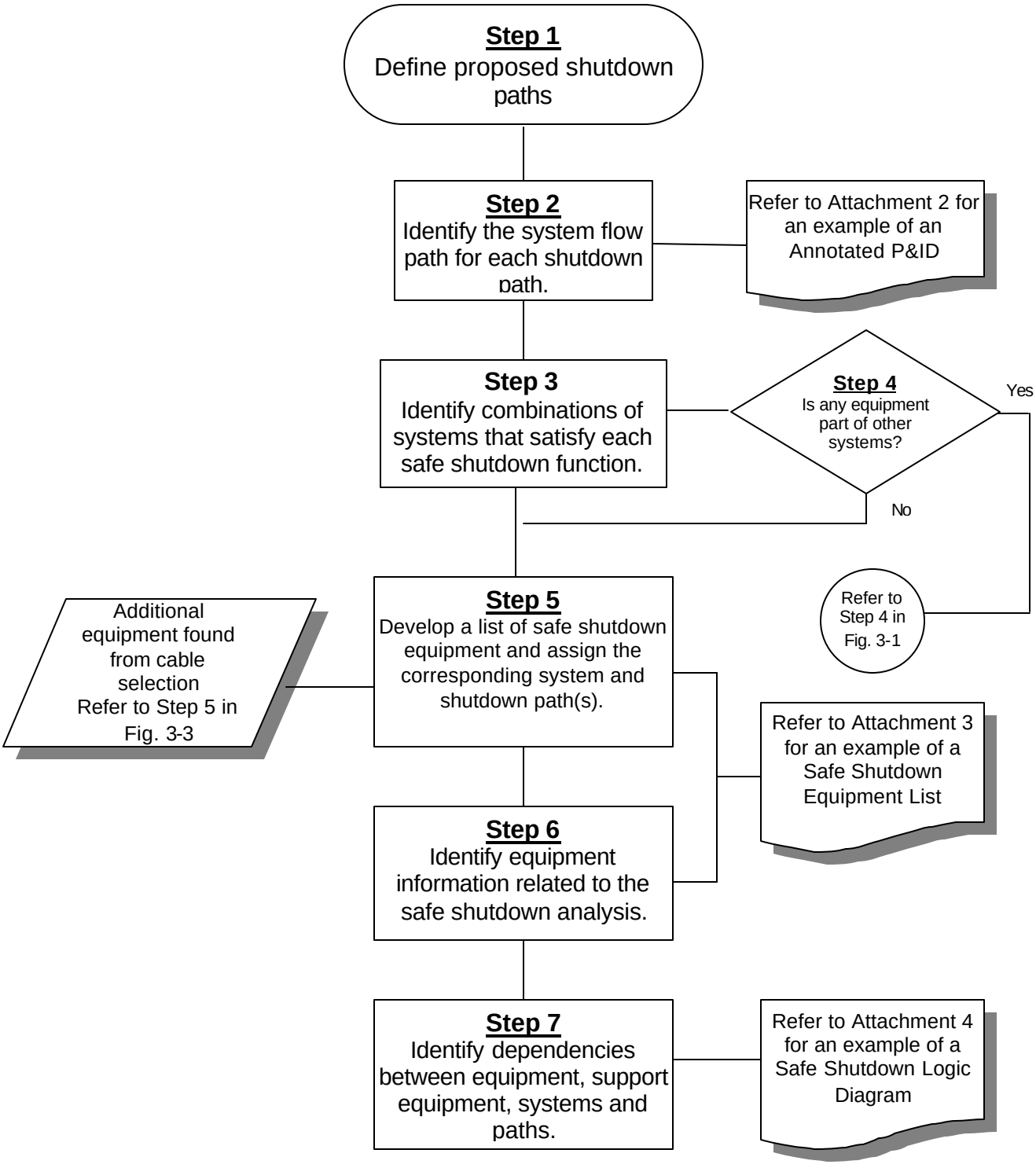
#### 3.2.2.4 Identify equipment information required for the safe shutdown analysis

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, Hi/Lo 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 to this document 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 to 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 is 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 effect. Through this cable-to-equipment relationship, cables become associated with the safe shutdown path assigned to the equipment affected by the cable.

### 3.3.1 Criteria/Assumptions

In order to identify an impact to safe shutdown equipment based on cable routing, the equipment must have cables associated with it. 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. Consider reviewing additional schematic diagrams to identify additional cables for interlocked circuits that also need to be considered for their impact to 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 of a single cable could impact more than one piece of safe shutdown equipment, associate the cable with each piece of safe shutdown equipment.

3.3.1.3 Electrical devices such as relays, switches and SRUs (signal resistor units) are considered to be acceptable isolation devices. In the case of

instrument loops, 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.

3.3.1.4 Screen out cables for circuits that do not impact the safe shutdown function of a component (e.g., 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.

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 not required to support safe shutdown. Each system can be controlled manually by operator actuation. However, if not protected from the effects of fire, the fire-induced failure of automatic initiation logic circuits must not 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 associated with the pump. Similarly, the power feed from the load center to an MCC is associated with the MCC. However, for cases where sufficient branch-circuit coordination is not provided, the same cables discussed above would also be associated with the power supply. For example, the power feed to the pump discussed above would also be associated with 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 associated with 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 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 hot shutdown. The three types of associated circuits were identified in Generic Letter 81-12 and they are as follows:

- Spurious Actuations
- Common Power Source
- Common Enclosure

**Cables Whose Failure May Cause Spurious Actuations**

Safe shutdown system spurious actuation concerns can result from fire damage to a cable whose failure could cause the spurious actuation/operation of safe shutdown equipment. 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.

**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) 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

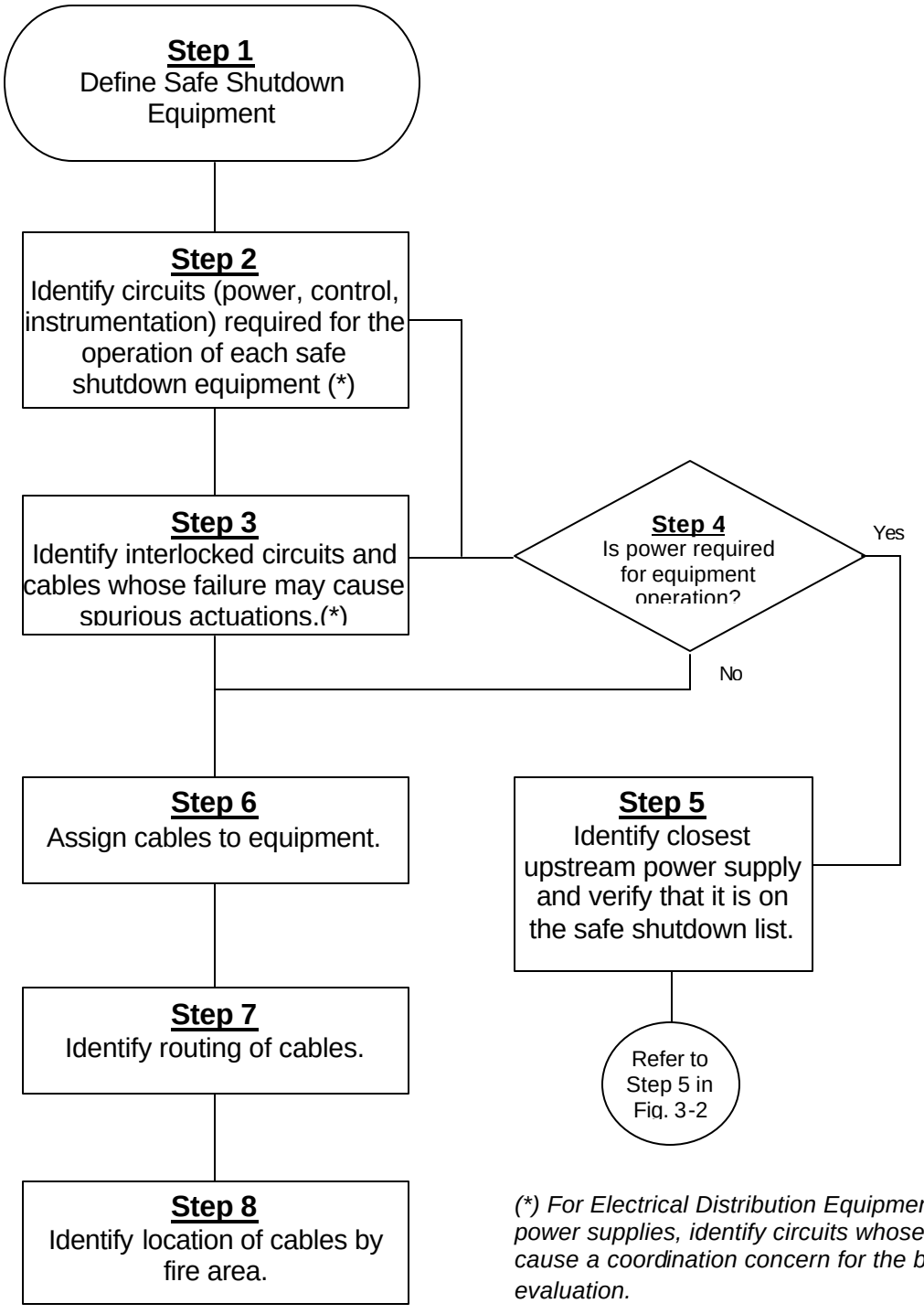
For electrical power distribution equipment such as power supplies, identify any circuits whose failure may cause a coordination concern for the bus under evaluation.

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 emergency power source.

#### 3.3.3.2 Identify interlocked circuits and cables whose failure may cause spurious actuations

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.

## Figure 3-4
## Safe Shutdown Cable Selection




*(*) For Electrical Distribution Equipment including power supplies, identify circuits whose failure may cause a coordination concern for the bus under evaluation.*

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 3-2) 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 which 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 be associated with 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.

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 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. Mitigate each potential impact one at a time. 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 manual actions where appropriate to achieve and maintain post-fire safe shutdown conditions. Refer to Appendix E for additional guidance on the use of manual actions as a mitigating technique.

3.4.1.5 Where appropriate, use repairs to equipment required to achieve or maintain cold shutdown in support of post-fire shutdown. Refer to Appendix E for additional guidance on the use of repairs as a mitigating technique.

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 adequate fire area 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 non-safety 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 non-safety 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 non-safety 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 operations, is to be addressed on a one-at-a-time basis. The focus is to be on addressing each equipment impact or each potential spurious operation and mitigating the effects of each individually[3].

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] Licensing Citation: Byron SSER 5 page 9-11. WNP2 Submittal dated May 23, 1986. Browns Ferry Inspection Report for July 17 thru July 21 Question No. 23 Item (3). Duane Arnold Response to NRC RAI dated April 20, 1982 Item 2.b page 14.

### 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).

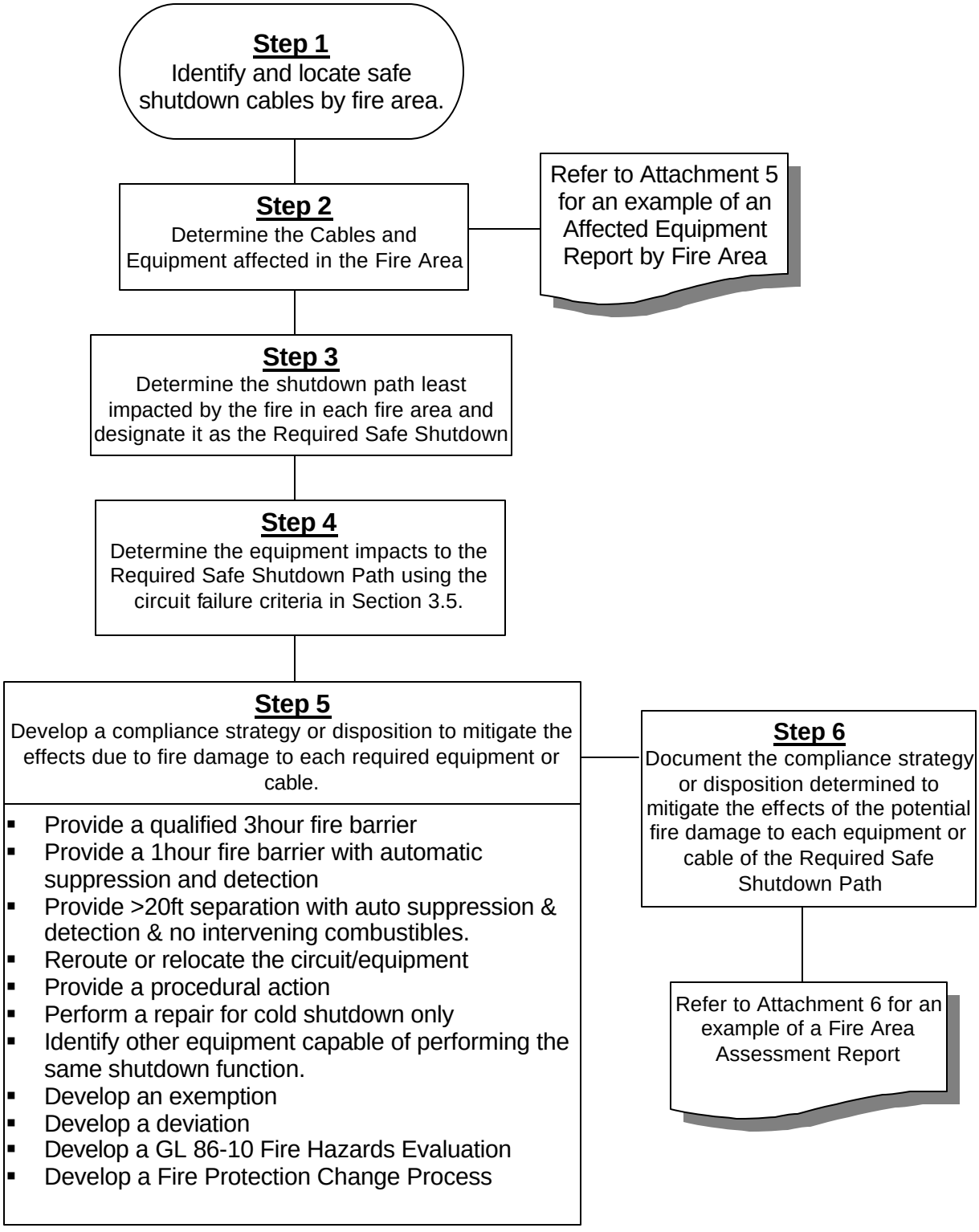
#### 3.4.2.2 Determine the shutdown paths least impacted by a fire in each fire area

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. For each of the safe shutdown cables (located in the fire area) associated with 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



#### 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 on the required safe shutdown path 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 methods for mitigating the effects of circuit failures are summarized as follows:

- 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.
- Reroute or relocate the circuit/equipment.
- Provide a procedural action (Refer to Appendix E for additional guidance)
- Perform a Cold Shutdown repair (Refer to Appendix E for additional guidance)
- Identify other equipment 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. Provide each piece of safe shutdown equipment 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 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 (one at a time) of each unprotected safe shutdown cable in order 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 MSIV solenoid valves due to an open circuit will result in the closure of the MSIVs). NOTE: The EPRI circuit failure testing indicated that open circuits are not likely to be the initial fire-induced circuit failure mode. Consideration of this may be helpful within the safe shutdown analysis.

- 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 failures within the licensing basis, evaluate the effects of each of these types of circuit failures on each conductor one at a time. For failures outside the licensing basis, evaluate component combinations as identified through the analysis methods in Section 4 of this document.

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 actuation. The fire is not assumed to eventually clear the circuit fault. However, EPRI fire test results indicate that short circuits typically clear after a short period of time. Consideration of this may be helpful within the safe shutdown analysis.

### 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 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, and 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

### 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.

Consider the following consequences in the safe shutdown circuit analysis when determining the effects of open circuits:

- 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.

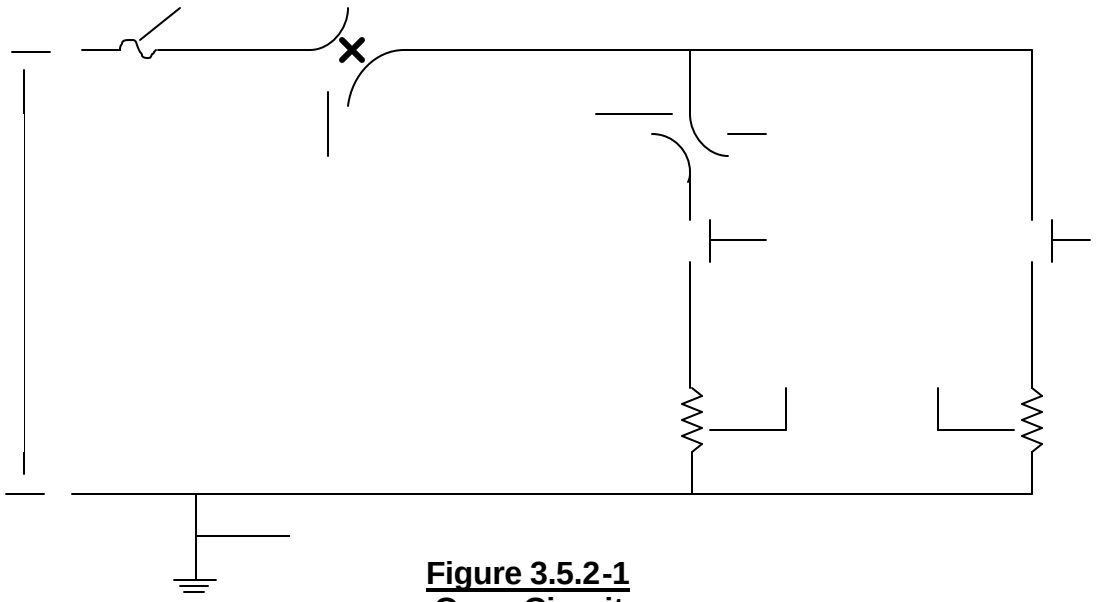


**Figure 3.5.2-1**
**Open Circuit**
**(Grounded Control Circuit)**

**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.

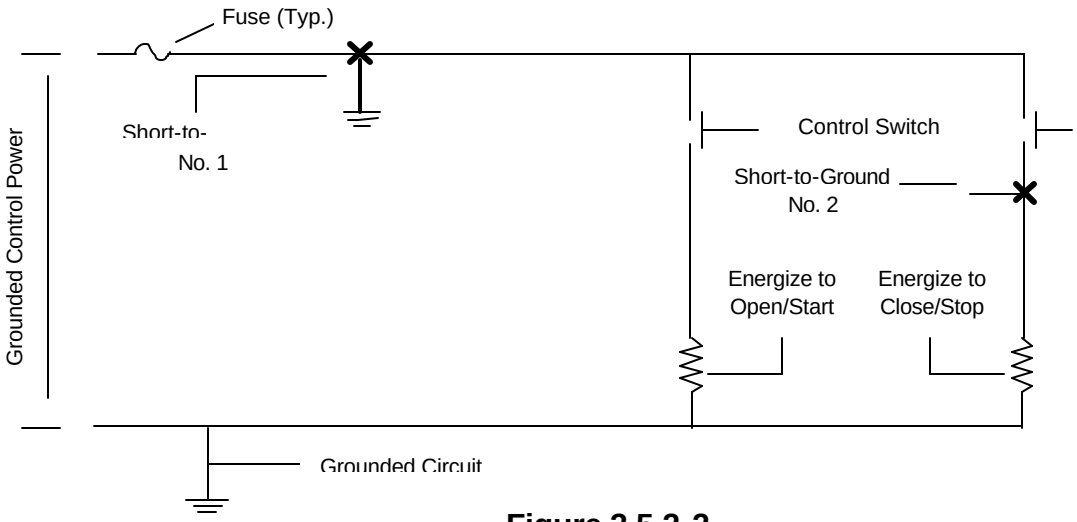



**Figure 3.5.2-2**
**Short-to-Ground**
(Grounded Control Circuit)

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 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. Since it is likely that an additional short to ground can occur, assume that the ungrounded circuit may become grounded as a result of the fire.

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

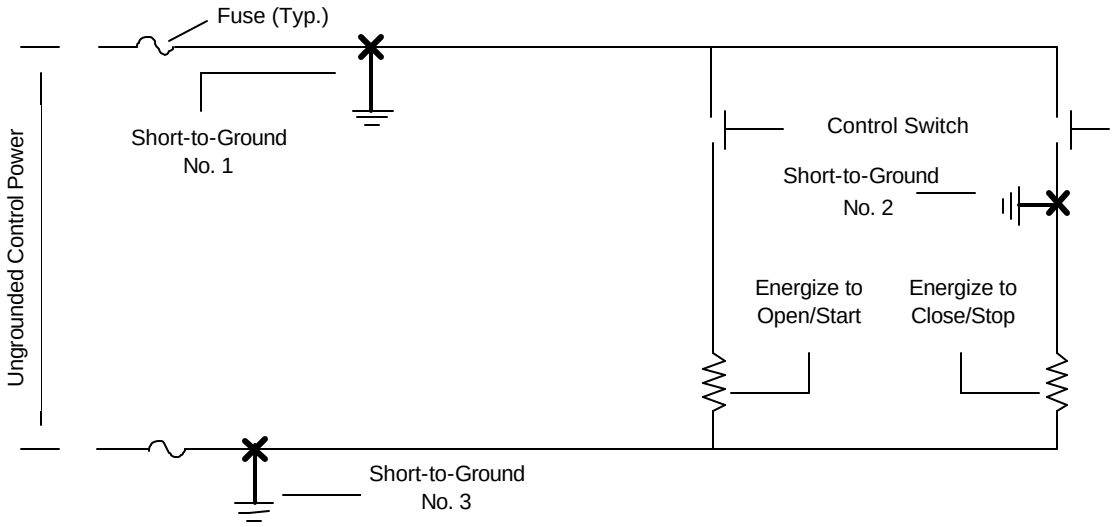



**Figure 3.5.2-3**
**Short-to-Ground**
**(Ungrounded Control Circuit)**

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 should be considered 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 actuation of equipment. The spuriously actuated device (e.g., relay) may be interlocked with another circuit that causes the spurious actuation of other equipment. This type of hot short is called a 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 actuation of equipment. This is called a cable-to-cable hot short or an external hot short.

**A Hot Short on Grounded Circuits**

A short-to-ground is a more likely 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.

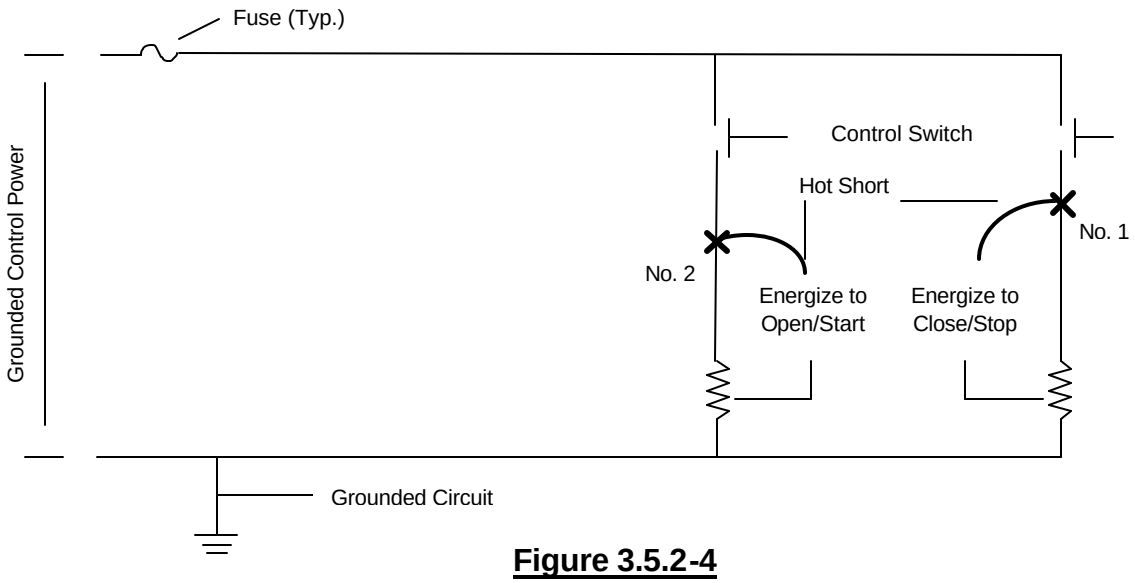



**Figure 3.5.2-4**
**Hot Short**
**(Grounded Control Circuit)**

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. There are also additional cases where a hot short on an ungrounded circuit in combination with a short-to-ground can cause a spurious operation.

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.

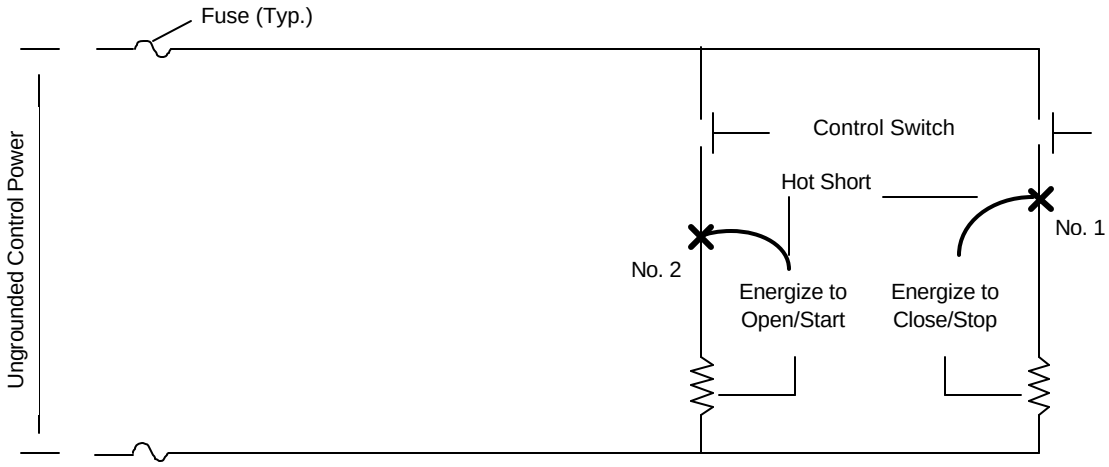



**Figure 3.5.2-5**
**Hot Short**
**(Ungrounded Control Circuit)**

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 to the Train B Pump, 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.

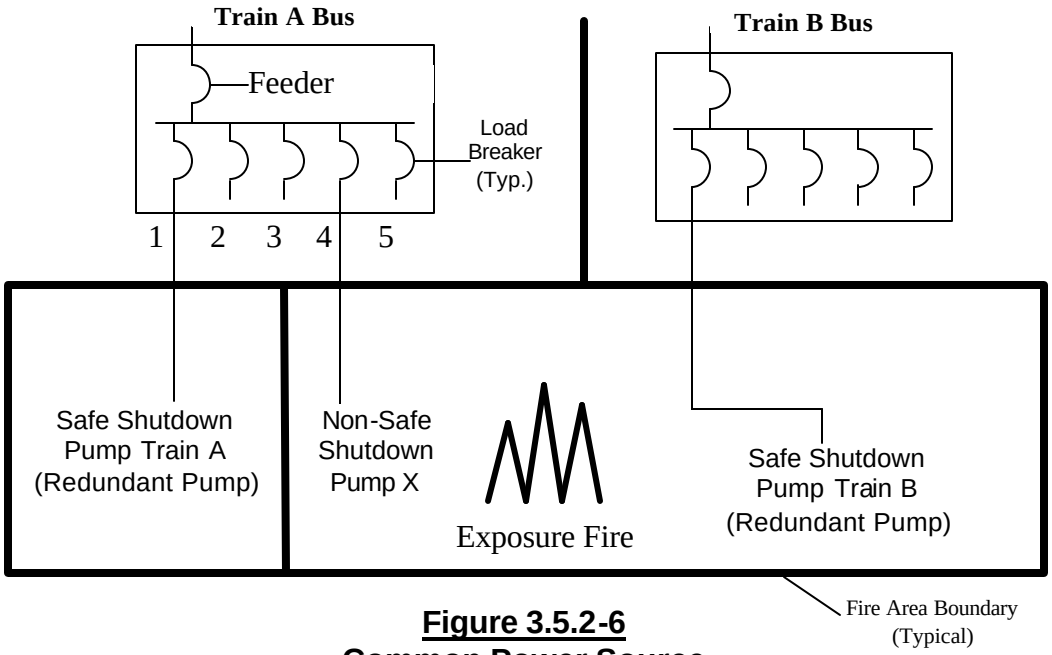



**Figure 3.5.2-6**
**Common Power Source**
**(Breaker Coordination)**

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 Section III.G.2 of Appendix R.

### 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 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. Adequate electrical circuit protection and cable sizing is included as part of the original plant electrical design maintained as part of the design change process. 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.

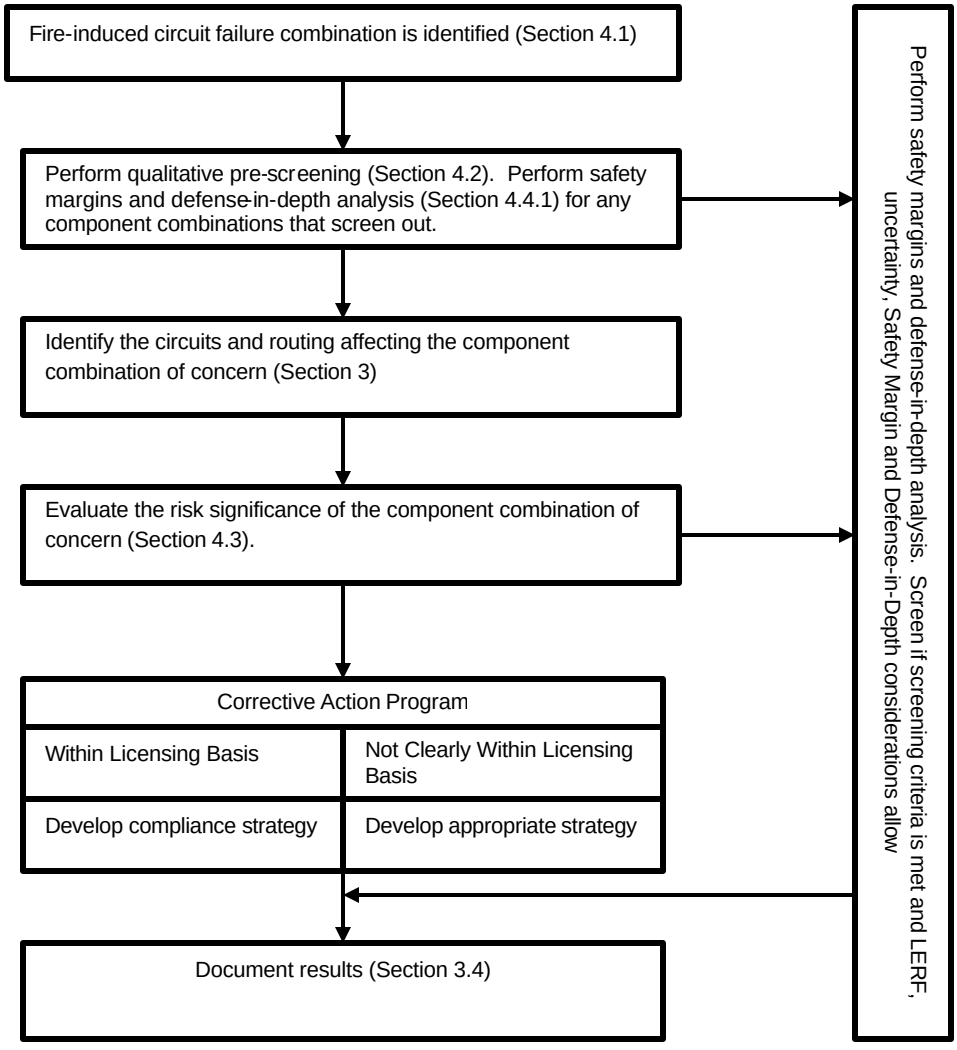
# 4 RISK SIGNIFICANCE ANALYSIS

This section provides a method for determining the risk significance of identified fire induced circuit failure component combinations to address the risk significance of the current circuit failure issues between the NRC and the industry.

Section 4.2 focuses on the preliminary screening of these circuit failures prior to the application of deterministic analysis methods. Section 4.3 provides a quantitative method for evaluating the risk significance of identified component combinations. Section 4.4 covers integrated decision making for the risk analysis, including consideration of Safety Margins and Defense-in-Depth considerations.

**FIGURE 4-1**

**SIMPLIFIED PROCESS DIAGRAM**



## 4.1 COMPONENT COMBINATION IDENTIFICATION

For those plants (both BWRs and PWRs) choosing to implement NEI 00-01, this section provides guidance for identifying potential plant-specific spurious actuation component combinations for further review.

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. These component combinations may be identified as follows:

- NRC inspectors may have identified issues with a potential for loss of safety function or unacceptable consequences.
- Plants may have identified component combinations or issues based on self-assessment findings.

Additional methods for identifying component combinations are discussed in Appendix F. These methods are provided as guidance for plants that wish to perform scoping studies on the general importance of spurious operation following a fire. Plants are not expected to use these methods as a matter of course for the following reasons:

- Plants have approved safe shutdown analyses

- Plants have already performed vulnerability analyses as part of the IPEEE. The results of the pilot evaluation of NEI 00-01, which evaluated the methods of Appendix F, did not indicate that there was a safety issue with hitherto unidentified component combinations.

If additional component combinations are selected, a review of the selected component combinations should be performed to ensure that the selection is the limiting component combination from a risk standpoint. It is possible that separating a combination into two or more component combinations would result in an overall higher risk. This could occur if one or more of the separated combinations had a high conditional core damage, or the reliability of the component removed from the combination were worse than the spurious operation probability, including fire damage.

Additionally, if there are more than one component combination in a given fire area, a review should be performed to ensure that combining the component combinations would not result in an overall higher risk. If this cannot be determined based on the factors affecting the risk (spurious operation probability, SSD equipment credited, location of cables, etc.), then several component combinations may need to be screened using the processes in the remainder of Section 4. For example, if there is one component combination with components A and B, and another with C and D, the plant may need to evaluate combinations with A, B and C, A, B, and D, etc, or with all components A, B, C, and D.

The purpose of this component combination review is to ensure the proper risk is assessed for the possible component combinations prior to screening a combination for consideration. This review may also be performed when the component combinations are screened, but may require additional screening if additional combinations are identified.

## 4.2 PRELIMINARYSCREENING

The purpose of the screening step is to qualitatively examine the risk significance of the component combinations in question. The approach to establish criteria for pre-screening of fire-induced circuit failures based on the following premises:

- Risk is characterized by frequency of core damage
- Risk is composed of two components: Frequency of undesired fire induced circuit failure, and consequences of undesired fire induced circuit failure (conditional core damage probability given the failures).

The risk significance may result from the adverse failure mode of this component(s). The method outlined below is one way to determine the potential risk significance.

Use Table 4-1 to qualitatively determine the risk significance of these component combinations. The criteria for risk significance are based on the criteria defined above and consistent with the Regulatory Guide 1.174 guidance. The factors in Table 4-1 represent the number of risk-reducing activities (represented by parameters of the probabilistic formula in Section 4.2) that would need to be deterministically credited for evaluated components in order to screen out the fire induced circuit failure from further analysis. Factors to be considered include circuit design (i.e., normally energized circuits that must de-energize to carry out the safety action, or vice versa) and timing (i.e., a lock-in device that prevents damage from a momentary spurious signal).

Criteria for evaluating high, medium and low for $\mathbf{F_f}$ (fire frequency) and $\mathbf{P_{SA}}$ (probability of spurious actuations) are provided in Table 4-2. [Note: More information about these two parameters can be found in Section 4.3.] Criteria for crediting detection, suppression, and safe shutdown features are provided in Table 4-3.

The following are several examples of the use of Table 4-1:

- If for an evaluated component combination $\mathbf{F_f}$ is qualitatively judged to be low and $\mathbf{P_{SA}}$ is judged to be low, no further screening is required. In other words, the combination of a low fire frequency and a low spurious actuation probability makes it very unlikely that unacceptable consequences will result.
- If for an evaluated component combination $\mathbf{F_f}$ is qualitatively judged to be medium and $\mathbf{P_{SA}}$ is judged to be medium, it can be screened out as risk insignificant if at least

two other reducing factors (such as automatic detection and suppression and manual suppression) can be credited qualitatively as effective. In other words, a medium fire frequency and a medium spurious actuation probability will require at least two other mitigating factors (such as automatic detection and suppression, and protected safe shutdown equipment) to be credited according to Table 4-3 to prevent the unacceptable consequences.

- If for an evaluated component combination $\mathbf{F_f}$ is qualitatively judged to be high and $\mathbf{P_{SA}}$ is judged to be high, the next step involves further analysis. Explained in another way, if both the fire frequency and the circuit failure probability are high, one cannot rule out unacceptable consequences at this stage without more detailed probabilistic analysis.

Component combinations that do not screen out in this step are subject to further analysis. The analyst can apply the NEI 00-01 Section 3 methods (steps 3.1.3.1 through 3.4.2.5) to selection of safe shutdown equipment, their associated target cables, and the physical location of target cables. Following this analysis, the analyst can develop resolution strategies that may involve further plant-specific risk significance screening using the methods of Section 4.3 or a plant-specific fire PRA analysis.

Component combinations that do screen out at this step are subject to further analysis (Safety Margins and Defense-in-Depth) in Section 4.4.

# TABLE 4-1
## Preliminary Screening

| | | Fire frequency ($F_f$) | | |
|---|---|---|---|---|
| | | **High** | **Medium** | **Low** |
| **Probability of spurious actuations of components combinations ($P_{SA}$)** | **High** | **Analyze** | Screen if all 3 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. | Screen if 2 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. |
| | **Medium** | Screen if all 3 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. | Screen if 2 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. | Screen if 1 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. |
| | **Low** | Screen if 2 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. | Screen if 1 of automatic suppression, detection and manual suppression, or safe shutdown capability can be credited. | **Screen** |

# TABLE 4-2
## Criteria for Evaluating $F_f$ and $P_{SA}$ (High, Medium or Low) in Table 4-1

| Element | High | Medium | Low |
|---|---|---|---|
| **Fire Frequency.** Defined as the frequency of those fires with a potential to damage critical equipment if left alone. | **Criteria:** High number of fixed ignition sources that have potential for damaging fire. These sources include switchgear, ignition sources with liquid combustibles or flammables such as large pumps and compressors, transformers. Example fire areas are: Switchgear room, turbine buildings, Control room, Diesel Generator rooms, cable spreading rooms or electrical rooms with more than a few cabinets, and pump rooms. Fire areas in the Auxiliary Building or Reactor Building with high concentration of fixed ignition sources, e.g., Relay Room or Auxiliary Electrical Equipment Room should be categorized as high.<br><br>**Basis:** Quantitative criterion used in Table 4-1 for "High" is based on frequency of fire of 1E-2/yr. Fires greater than 1E-03/year are categorized as high. Fire areas mentioned above could have area fire frequencies around 1E-2/yr depending on the number of the location type at each plant (FIVE). | **Criteria:** The fire area has limited number of fixed ignition sources that have potential for damaging fires, or no fixed combustibles but transient combustible for extended periods. The area has higher potential for transient fires due to maintenance activities in the area or its adjacent rooms. Example fire areas are; those cable spreading rooms with few, i.e., one or two electrical cabinets, and Battery Rooms. Fire areas in the Auxiliary Building or Reactor Building that do not contain more than one or two fixed ignition source may be categorized as Medium.<br><br>**Basis:** Quantitative criterion used in Table 4-1 for "Medium" is based on frequency of fire of 1E-3/yr. Fires between 1E-3 /year and 1E-4/year are categorized as medium. With few fixed ignition sources the frequency of a damaging fire in a Cable spreading room will remain below 1E-3/yr. Frequency of a fire in a battery room is around 1E-3/yr in a plant with at least two battery rooms. . | **Criteria:** No fixed ignition source such as pumps or electrical cabinets. Transient combustibles are administratively controlled with provisions for possible staging of combustibles when fire watch will be in effect. Example fire areas are; cable tunnels and cable spreading rooms with no fixed ignition source.<br><br>**Basis:** Quantitative criterion used in Table 4-1 for "Low" is based on frequency of fire of 1E-4/yr. Fires less than 1E-04/year are categorized as low fire frequency. The plant-wide transient fire ignition frequency is between 1E-02/year and 1E-03/year (FIVE), with a majority of these fires occurring due to welding or cutting. The area specific frequency depends on several factors, including the possible ignition sources in the area, the procedural controls performed at the plant for both ignition sources and combustible controls, and the location of sufficient combustibles needed to damage equipment. A damaging transient fire needs to pass the presence of the plant personnel (maintenance worker or fire watch in case of welding and cutting) and occur in specific location with respect to the potential targets to be of damaging potential. Combined with these factors fire area ignition frequency in an area with no fixed ignition source and administratively controlled combustibles will be less than 1E-4/yr. |

Note: When available, IPEEE or Fire PRA Initiating Event Frequencies should be used to categorize the Fire Frequency. The frequency used in this screening is the total fire area fire frequency, either severe or non-severe

| Element | High | Medium | Low |
|---|---|---|---|
| **Probability of Spurious Actuation of Component(s)**<br><br>Probability of undesirable or non-recoverable spurious actuation of the redundant component. Note that at this point in the screening some information on the component combinations including their circuits and routing including the raceway may be known. Factors to be considered include; circuit design, e.g., normally de-energized circuits that are required to remain de-energized, timing, e.g., lock-in device that prevents damage from a momentary hot short resulting in spurious signal and proximity of the circuits associated with the component combinations. | **Criteria:** The conductors of component combinations as follows: a) Thermoset/ Thermoplastic Inter-cable, b) Thermoset / Thermoplastic, M/C or 1/C to 1/C Intra-cable, or c) Cable in Conduit W/O CPT. Basis: Quantitative criterion for "High" is based on conditional probability of 0.1 to 1. See Table 4-4 and EPRI TR-1006961, "Spurious Actuation of Electrical Circuits due to Cable Fires," Table 7-2 (Ref. 6.4-39). | **Criteria:** The conductors of the component combination(s) are routed:<br>▪ In cable tray(s) within separate multi-conductor (MC) cables with CPT, OR<br>▪ In conduit where: a) located in same cable with CPT, OR located separate single conductor cables (1C-1C) with CPT, OR separate 1C-MC or MC-MC cables w/o CPT<br>▪ In armored cables w/o fuses.<br>Additionally, one can include combinations such as two T-set intra-cable failures with CPT where the product of the failures is between 0.01 and 0.1. Lastly, the Medium category will include combinations where the initial probability is greater than 0.1, but is required to be sustained for greater than 5 minutes (see below). **Basis:** Quantitative criterion for "Medium" is based on conditional probability of 0.01 to 0.1. See Table 4-4 and EPRI TR-1006961, "Spurious Actuation of Electrical Circuits due to Cable Fires," Table 7-2. | **Criteria:** Conductors of the component combination(s) are routed in separate conduits or in fused armored cables. Additionally, one can include combinations such as two cables in conduit (with CPTs) where the product of the failures is less than 0.01. Lastly, the Low category will include component combinations where the initial probability is between 0.1 and 0.01, but is required to be sustained for greater than 5 minutes (see below). **Basis:** Quantitative criterion for "Low" is based on conditional probability of less than 0.01. See Table 4-4 and EPRI TR-1006961, "Spurious Actuation of Electrical Circuits due to Cable Fires," Table 7-2 (Ref. 6.4-39). |

# TABLE 4-3
# Criteria for Crediting Mitigation and Safe Shutdown in Table 4-1

| Mitigation and Safe Shutdown for Preliminary Screen | Criteria for Crediting |
|---|---|
| **Automatic Suppression** | **Criteria:** Automatic suppression (AS) may be credited when it can be demonstrated that the AS can protect the circuits associated with the component combinations from damage caused by the ignition sources in the fire area. This may be demonstrated in one of two ways. (1) Area-wide or local AS system is installed such that it can control a fire from all major ignition sources in the fire area prior to damage to circuits of the component combinations. Major ignition sources may be defined as the "Fire Ignition/Fuel Source" type in the FIVE methodologies (EPRI TR100370, Table 1.2). (2) The location of the circuits for the component combinations is known and the AS is designed to protect these circuits. If the automatic suppression system in the area deviates from applicable NFPA codes, an equivalency examination may be warranted to demonstrate that the installed system is equivalent in protecting the intended circuits.<br><br>**Basis:** The quantitative criterion for crediting automatic suppression is 0.1. Considering the reliability of these systems, the question is their effectiveness to prevent damage to specific target in time. Above criteria can ensure that AS is credited only in appropriate source-target configurations. It is understood that ability of a fire protection system in protecting the circuits of the component combination against a fire initiated in the circuits of the component combination itself is questionable. Frequency of fires starting in such limited areas, e.g., the part of the cable tray or electrical cabinet that contains circuits of the component combination is a small fraction of the fire area frequency which when combined with probability of spurious actuation will result in low risk. Note that appropriate credit for suppression can only screen areas where it can be demonstrated the fire frequency and likelihood of spurious actuation are either Medium or Low. |
| **Detection and Manual Suppression** | **Criteria:** Detection/Manual Suppression (DM) may be credited when it can be demonstrated that DM can protect the circuits associated with the component combination from damage caused by the ignition sources in the fire area. This can be demonstrated if the fire area is covered by area-wide (or over the major ignition sources) early warning detection system, the plant maintains a fire brigade that meets the requirements of the applicable NFPA codes and standards (i.e., adequacy of equipment and training), and a response time of 10-15 minutes for the fire area can be demonstrated.<br><br>**Basis:** An early detection system can provide 10 minutes or more warning for brigade response prior to damage from an external exposure. The fire requires at least 5 minutes to develop into a damaging exposure and cables exposed to external fires need between 2-20 minutes to show functional failures (NUREG/CR-5384 and NUREG/CR-5546). Also see above (under automatic suppression) for fires involving the component combination circuits. |

| Mitigation and Safe Shutdown for Preliminary Screen | Criteria for Crediting |
|---|---|
| **Safe Shutdown Capability** | **Criteria:** Safe shutdown may be credited if it can be demonstrated that, given damage to the component combination, at least one division of equipment (safe shutdown or otherwise) remains available including manual actions as long as it can be demonstrated that the required functions can be performed within the available time. This may include restoring equipment damaged by the spurious actuation(s) if possible. Note that the impact on safe shutdown from damage to the component combinations may not be known if the combination was not within the plant SSD methodology (licensing basis). Thus, credit might not be applied in the screening for beyond licensing basis component combinations. If the component combination requires new safe shutdown methods or equipment, then availability of components, especially the feasibility of any new manual actions, should be demonstrated.<br><br>**Basis:** The quantitative criterion for crediting this element is defined as 0.1. This is upper bound unavailability for a single division if it requires moderate number of manual actions with procedure and time available. A "moderate number of manual actions" is defined based on<br><br>• Where all manual actions required in response to post-fire conditions are in response to a component or functional failure, i.e., verification and recovery actions. In case of shutdown from outside the Control Room (CR), actions needed prior to CR abandonment should be recoverable from outside the CR; OR<br><br>• Where post-fire manual actions required in the safe shutdown method are limited to remote operation of mechanical equipment (such as valves), and local manual recovery is possible.<br><br>Use of this criterion for other conditions should be examined and justified on a case-by-case basis. |

### 4.2.1 Expert Panel Results

EPRI TR-1006961, "Spurious Actuation of Electrical Circuits due to Cable Fires, Results of an Expert Elicitation" (Reference 6.4-39) is used in both the preliminary screening and detailed screening in the determination of $\mathbf{P_{SA}}$, probability for spurious actuation. Use of these results is summarized below.

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

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

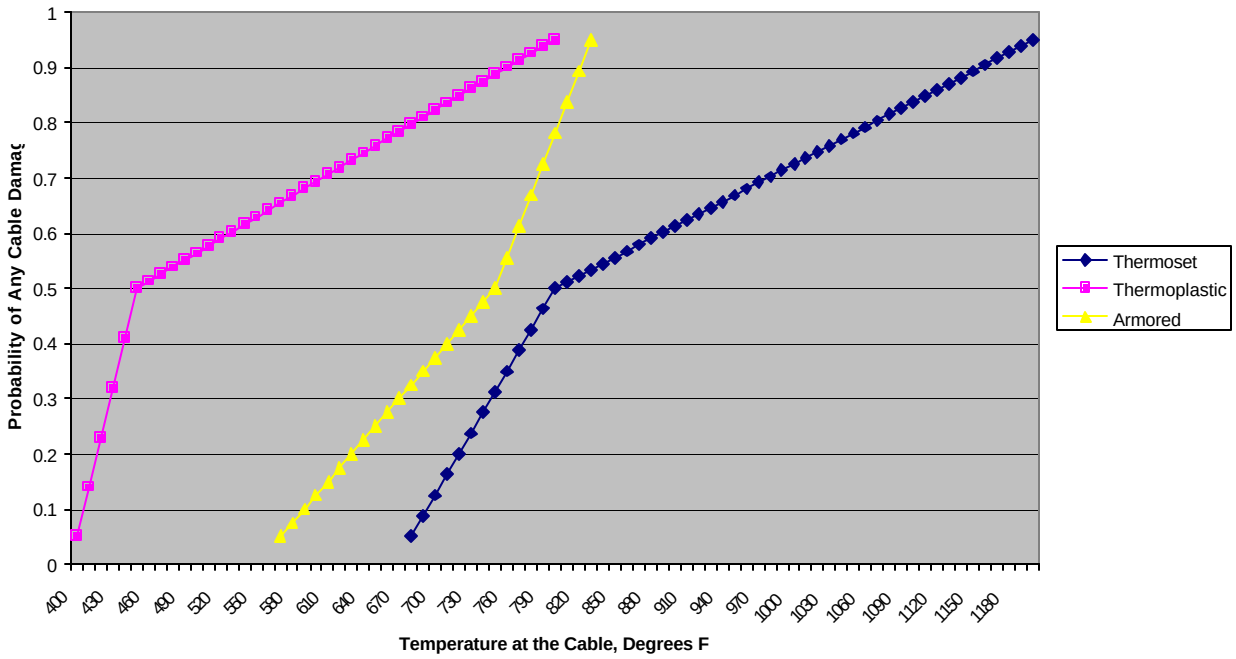
$P_{CD}$ = The probability of cable damage given a specified set of time-temperature and fire-severity conditions, and

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

$P_{CD}$ can be calculated using fire modeling, taking into 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 T-set, T-plastic and armored cables. This curve is provided below:

**FIGURE 4-2**

**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)**



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 4.3), $P_{CD}$ 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 4-4. Some general guidance on this is as follows:

- Values in the table, other than B-15, assume 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 6.5-39, 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.

- The "high confidence range" can be used in the uncertainty and sensitivity analysis requirements. For those cases, where a range is given for the best estimate, the upper value should be used for the preliminary screening while the midpoint should be used for the detailed analysis. The two given are M/C to M/C inter-cable (T-set and T-plastic). For these, 0.05 should be used for preliminary screening (medium $P_{SA}$), while 0.025 would be used in the quantitative screening.

Additional guidance on the use of this table is provided in the expert panel report (Reference 6.4-39).

EPRI TR-1003326, "Characterization of Fire-Induced Circuit Failures: Results of Cable Fire Testing," when published, will provide 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 detailed 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. If Table 4-2 were changed to indicate a sustained failure is anything greater than 5 minutes, then the category reduction for any sustained versus momentary is consistent with the test data. That is, a sustained short is approximately 10 times less likely than a momentary short. This factor of ten reduction in $P_{SA}$ can be used for either the preliminary screening (see Table 4-2) or in the detailed screening calculation.

## TABLE 4-4
## (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 |

## 4.3 PLANT-SPECIFIC RISK SIGNIFICANCE SCREENING

Based on the evaluations performed in Section 4.2 and Section 3 of this document, the licensee may determine that additional safety significance analysis is warranted. This analysis should be viewed as one method for mitigating potential fire-induced failures of component combinations. Other deterministic or probabilistic means may be employed.

### 4.3.1 Objective

The objective of this section is to provide a quantitative approach to determine the risk significance of the component combinations identified in Section 4.1. An alternative to applying this screening methodology is to determine the risk significance of component combinations using a plant-specific fire PRA.

### 4.3.2 General Description

This screening method will evaluate the risk associated with potential fire-induced failures of component combinations.

This screening method progressively estimates the risk associated with these component combinations and screens those that are deemed to pose insignificant risk to the plant. The criteria for determining that component combinations are not risk significant are as follows:

- If the change in core damage frequency (?CDF) for each component combination for any fire area is less than 1E-7 per reactor year, AND

- If the ?CDF for each component combination is less than 1E-6 per reactor year for the plant, i.e. sum of ?CDF for all fire areas where circuits for the component combination (circuits for all) are routed, AND

- If the ?CDF for each fire area is less than 1E-6 per reactor year for the plant, i.e., the sum of ?CDF for all combinations of circuits in the fire area.

The criteria in the second and third bullets above should be applied only after completion of all five screening steps in Section 4.2.4.2. These criteria are summations of CDF changes for the same component combination over several fire areas (the second criterion) and of CDF changes for several combinations within the same fire area (third criterion). Unless all screening steps are complete, screening against these two criteria would provide an overly conservative result. All three criteria must be satisfied for a component combination to be screened out.

These criteria are based on the general premise that the total fire ?CDF due to concurrent spurious operations should be no greater than 1E-05 per reactor year based on conservative assessment. Assuming, for example, an average of ten

component combinations with potential risk significance, and ten fire areas through which each component combination passes, conservatively screening each individual component combination in each fire area at 1E-07 per reactor year provides reasonable assurance that the total of 1E-05 per reactor year will not be exceeded. Similarly, showing that the sum of the conservative ?CDF values from the Screen 5 results for each component combination and fire area, respectively, is less than 1E-06 per reactor year provides reasonable assurance that the total of 1E-05 per reactor year will not be exceeded even if the number of potentially risk significant component combinations or the number of fire areas through which any specific component combination passes exceeds ten, respectively.

If a component combination screens out of a single fire area based on the first criterion, it must still be evaluated for all fire areas where the component combination has power, instrument, or control cables. If the component combination screens out based on the second criteria, i.e. the sum of ?CDF for all fire areas is <1E-6/year, the component combination may be screened from further consideration. If the fire area screens out based on the third criterion, i.e. the sum of ?CDF for all component combinations is <1E-6/year, the fire area may be screened from further consideration. If the sum of ?CDF is >1E-6/year using the second or third criterion above, further analysis using detailed plant fire PRA models or actions to reduce the summed ?CDF below 1E-6/year will be evaluated. The screening process can result in a conservative CDF estimate for any step in the analysis, which may result in failure to screen using the second and third criteria. For example, a fire area may have 50 scenarios screened, each at a CDF of 9E-08/year, which results in the fire area not screening (area CDF = 50 * 9E-08 = 4.5E-06/year). Additional analysis may be required on scenarios already screened using the first criteria in order to meet the second or third screening criteria.

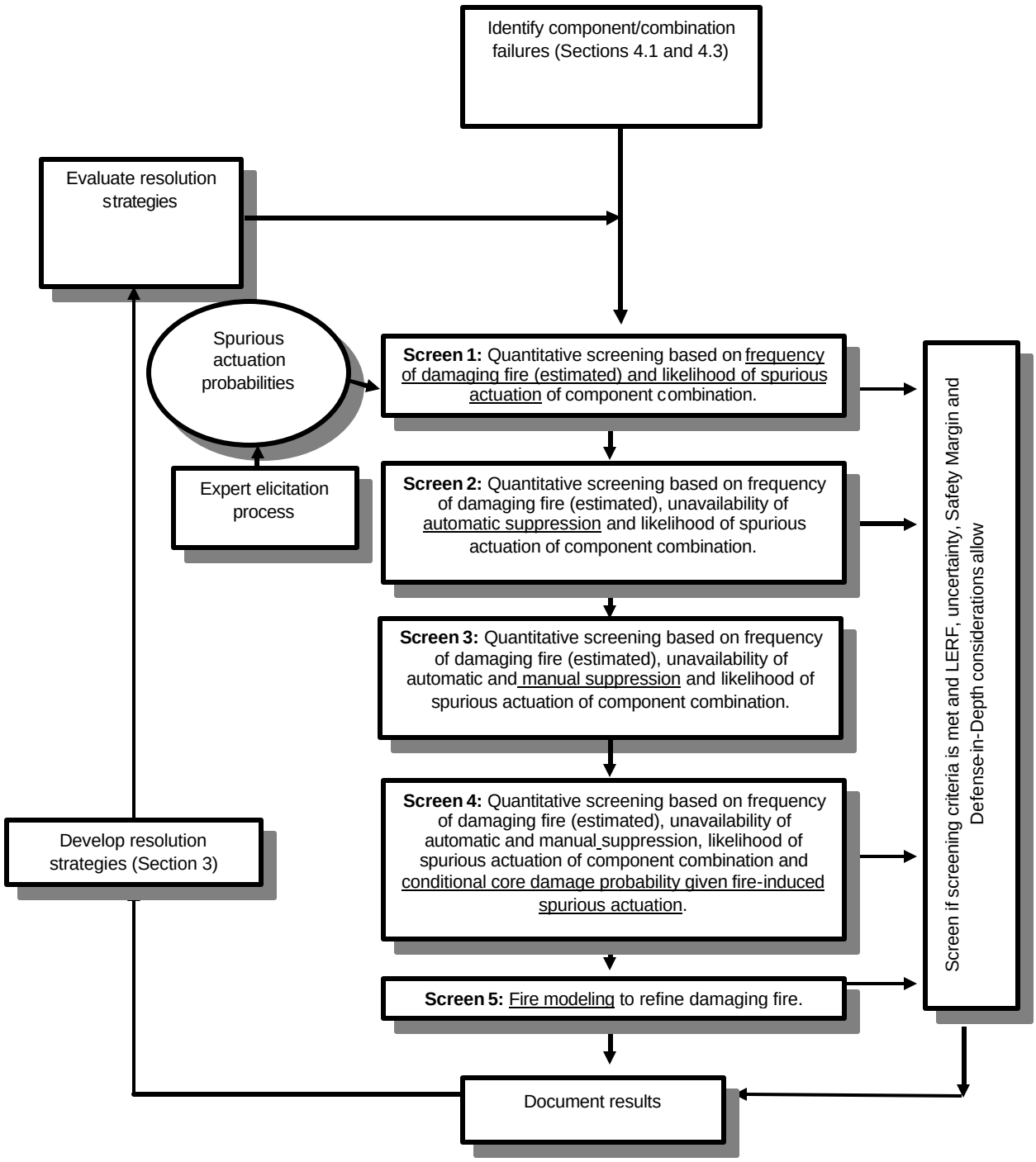
If circuits for more than one component combination are routed in the same fire area such that the sum of the ?CDFs associated with all component combinations of concern in a fire area is >1E-6/year, corrective actions should be considered. In such cases, changes in the fire area that lower fire hazard or provide better prevention may lower the risk to all components combinations.

This method involves a phased approach that successively multiplies the previously calculated risk factors by new ones at each phase, and compares the ?CDF against the 1E-7 criterion. This allows the option of stopping the analysis at any phase where the ?CDF or probabilistic contributors thereto have been determined to be “insignificant” because they meet the criteria described above.

If, when all evaluation phases are completed, the criteria established above are not met for specific component combination or in a fire area, further actions will be evaluated based on the ability to reduce risk in a cost effective manner and consistent with appropriate regulatory guidance.

An overview of this approach is illustrated in Figure 4-3.

**FIGURE 4-3**
**Safety Significance Analysis Overview**



The screening steps in this method are provided generally in the order of ease of analysis and robustness of acceptable methods, but they may be conducted in any order of the factors noted below.

The probabilistic formula used for this analysis follows. The factors listed below are defined such that they may be considered independent.

**? CDF = $F_f$ * $P_E$ * $P_{SA}$ * $P_{AS}$ * $P_{DM}$ * ? $P_{CCD}$** (per reactor-year)

**$F_f$** = fire frequency. Frequency of fires of any size anywhere within the fire area

**$P_E$** = fire size parameter; fraction of fires in the area capable of reaching damaging combinations of time and temperature

**$P_{SA}$** = probability of spurious actuations of a component combination given cable damage

**$P_{AS}$** = probability that automatic suppression will fail to control the fire before damage to the cable(s) is such that spurious actuation could occur

**$P_{DM}$** = probability that detection and manual suppression will fail to control the fire before damage to the cable(s) is such that spurious actuation could occur

**$P_{CCD}$** = conditional probability of core damage given fire-induced failures including spurious actuations of a component combination

These terms are further defined in the appropriate screening step. In applying these factors, standard Fire PRA methodology should be applied in order to ensure accurate risk results are developed [6.4.36]. For example, automatic suppression that does not protect the entire fire area (or the entire cable under consideration, if the location is known) cannot be applied to the entire fire frequency. Similarly, independence of the risk factors should be ensured when applying these factors. For example, application of automatic and manual suppression should be predicated on a severe fire since a fire size parameter is already applied. If independence cannot be ensured for the factors applied, conservative application of the factors (i.e., the factor is set to 1.0) should be performed until more accurate estimates can be developed.

For a single component, this calculation is performed for that component in each fire area where its power, control, or instrument cables are run, and the results are summed for all areas. The thresholds for safety significance are applied as described above. For component combinations, this calculation is performed for that combination in each fire area where power, control, or

instrument cables for both components are routed, and the results are summed for all such areas.

### 4.3.3 Screening Analysis

**Screen One**

*The purpose of Screen One is to screen out potential spurious actuation scenarios based on frequency of damaging fire times spurious actuation conditional probability. The spurious actuation conditional probability is available from Table 4-4.*

1. Fire frequency, $\mathbf{F_f}$ - Using the guidance in EPRI's Fire Induced Vulnerability Evaluation (FIVE), Fire PRA Guide or other methods, determine the fire frequency $\mathbf{F_f}$ for the fire area. This frequency is representative of fires of any size anywhere in the fire area. These fires may be damaging depending on where they are and how big they get. The area fire frequency information should be available in most existing plant examinations performed under the IPEEE program.

2. Fire size parameter, $\mathbf{P_E}$ - This parameter defines the fraction of the fires in the fire area that are capable of damaging cables/circuits for the component combination. Potential for damage is determined by three factors, fire size, fire location (with respect to the target), and target damage criteria. Fire size is a characteristic of the source and is generally described by the rate at which the fire generates heat, i.e., Heat Release Rate, duration of the fire or the total heat, and foot-print of the fire, i.e., point source vs. pool fire. References for fire size include EPRI PRA Guide (Appendix E) and its supplement for Resolution of Generic RAIs and numerous other publications by Sandia and international institutes such as VTT in Finland. Fire location is a characteristic of source-target configuration and is unique to the fire area that defines the exposure temperature the target will see. Damage criteria are a characteristic of the target and defines the exposure at which the target will fail. One source for damage criteria is Appendix F of the EPRI PRA Guide.

   One method to estimate the fire size parameter ($\mathbf{P_E}$) is by developing the zone-of-influence first. Zone-of-influence (ZOI) is a combination of all three factors above and is defined as a radius that a fire source is capable of damaging a target with known damage criteria. EPRI's Fire PRA Guide (Section 4, step 5.1) describes one method for estimating ZOI for typical fire sources in a nuclear power plant. This requires reviewing the characteristics of the fire hazard (combustible types and potential initiators) in the fire areas where the target conductors are located. Once the ZOI is developed, the overall fire frequency of the sources in the fire area capable of a damaging fire to circuits of the component combination is $\mathbf{F_f} * \mathbf{P_E}$.

The NRC's fire scenario calculation tool may also be considered.

Again, $\mathbf{P_E}$ is the ratio of damaging fires to total fires in the particular area.

3. Probability of spurious actuations of component combination, $\mathbf{P_{SA}}$ - Select the appropriate $\mathbf{P_{SA}}$ value from Table 4-4. The probabilities of single spurious actuations will be utilized when evaluating IN 92-18 type failures. Otherwise, the probabilities of two (or more) concurrent spurious actuations will be employed for the specific combination of failures being evaluated. If the concurrent failures are in the same multiconductor cable, the failures are considered dependent, and a single $\mathbf{P_{SA}}$ value should be used for both failures together. If the two failures are in separate multiconductor cables they are considered independent, and the $\mathbf{P_{SA}}$ value in the equation should be the product of the two values from Table 4-4.

4. If **? CDF =** $\mathbf{F_f}$ * $\mathbf{P_E}$ * $\mathbf{P_{SA}}$ < 1E-7 per reactor year for the component combination in the fire area, and < 1E-6 for all fire areas, screen this component combination from further review if SM and DID considerations permit. If these thresholds are not reached, or if circuits for more than one component combination are routed in the same fire area such that the sum of the ?CDFs associated with all component pairs of concern in a fire area is >1E-6/year, proceed to Screen Two or consider corrective actions.

**Screen Two**

*The purpose of Screen Two is to credit the capability of the automatic suppression systems (including supporting detection equipment) for controlling the fire before it reaches damaging proportions.*

5. Automatic Suppression Capability $\mathbf{P_{AS}}$ - Calculate the probability that automatic detection and suppression systems do not prevent undesirable consequences (cable damage) to the cables of the component combination ($\mathbf{P_{AS}}$). Techniques described in "Automatic and Manual Suppression Reliability Data for Nuclear Power Plant Fire Risk Analyses", NSAC-179L, "Fire-Induced Vulnerability Evaluation (FIVE)", EPRI TR-100370, and "Fire PRA Implementation Guide", EPRI TR-105928 may be used. The probability should include the unreliability, unavailability, and effectiveness of automatic suppression. Since severity factors/fire size parameters ($\mathbf{P_E}$) have already been considered in the screening process, Screen 1, the automatic suppression effectiveness should be determined based on the fire being severe.

   a. Obtain reliability values from "Automatic and Manual Suppression Reliability Data for Nuclear Power Plant Fire Risk Analyses", NSAC-179L, Table 1-1.

b. Consider the contribution of unavailability negligible unless plant-specific data indicates that the systems have been unavailable for more than four weeks in any one of the past five years. If that is the case, calculate the unavailability for the worst of the five years and use that value.

c. Sum the unreliability (1 – reliability) and unavailability figures.

d. The system is considered effective if the criteria in Table 4-3 for automatic suppression are satisfied. If this is the case, $\mathbf{P_{AS}}$ = the value calculated in Step 5c. If not, $\mathbf{P_{AS}}$ = 1.0.

e. If automatic suppression is effective for only some of the fire ignition sources considered (i.e., partial area coverage), then this may be included in the analysis. For this application, the change in CDF is then the sum of the various scenarios in the area:

$$\mathbf{? CDF = S F_f * P_E * P_{SA}}$$

See the pilot evaluation report for examples on how to apply the summation method for this screening.

6. If $\mathbf{? CDF = F_f * P_E * P_{SA} * P_{AS}}$ < 1E-7 per reactor year for the component combination in the fire area, and < 1E-6 for all fire areas, screen the component(s) from further review if SM and DID considerations permit. If circuits for more that one component combinations are routed in the same fire area such that the sum of the ?CDFs associated with all component pairs of concern in a fire area is >1E-6/year, proceed to Screen Three or consider corrective actions.

**Screen Three**

*The purpose of Screen Three is to credit the ability to manually suppress the fire before it reaches damaging proportions. Manual suppression is considered effective if it can be demonstrated that all fires from important fixed ignition sources and transients in the area can be controlled prior to damage to cables that cause the spurious actuation(s) in question.*

7. Manual Suppression Capability $\mathbf{P_{DM}}$ - Calculate the probability that detection and manual suppression fail to control the fire before cable damage thresholds are reached ($\mathbf{P_{DM}}$). Without time-to-damage and time-to-detection available (no detailed fire modeling), use fire brigade effectiveness (calculate using the techniques described in the "Fire PRA Implementation Guide", EPRI TR-105928 (Appendix K) or "Fire-Induced Vulnerability Evaluation (FIVE)", EPRI TR-100370 (Section 6.3.6.2)) and credit if the criteria described in Table 4-3 are met. When both automatic and manual suppressions are credited, it is important to consider their dependency (EPRI SU-105928, Sections 3.5 and 4.5). Since severity factors/fire size parameters ($\mathbf{P_E}$) have

already been considered in Screen One, the detection and manual suppression effectiveness should be determined based on the fire being severe.

When applying manual suppression probabilities developed for an IPEEE or previous Fire PRA, these values must be reviewed to ensure that they are applicable to this screening analysis. This evaluation should include evaluation of time to damage as well as independence of the manual suppression factor. If damage cannot be prevented prior to the expected time to manual suppression, then a factor of 1 should be used for $\mathbf{P_{DM}}$.

EPRI TR-1003326, "Characterization of Fire-Induced Circuit Failures: Results of Cable Fire Testing," Table 12-29, provides some general guidance on the expected time to spurious operation for the Fire Tests performed in support of NEI-00-01. The EPRI report states "The results imply that early action in a fire is highly likely to be effective at accomplishing a desired function. Preplanned high value actions appear to be a significant contributor to reducing both likelihood and consequence of serious fires. Similarly, early preemptive action for high risk components to eliminate spurious concerns should substantially reduce risk." The EPRI table for time to spurious operation is repeated here.

**Table 4-5**
**Time to Spurious Operation**

| | **Armored Cable (min)** | **Thermoset (min)** | **Thermoplastic (min)** | **Overall (min)** |
|---|---|---|---|---|
| Longest Time | 36.1 | 85.7 | 40.4 | 85.7 |
| Shortest Time | 36.1 | 14.0 | 2.5 | 2.5 |
| Average Time | 36.1 | 46.3 | 25.9 | 37.6 |
| Standard Deviation | 0 | 20.4 | 14.9 | 20.3 |

This table demonstrates that, given the types of fires and configurations used in the fire testing, we would not expect to see spurious operations on average for at least 30 minutes. This data can be used in support of the determination of $\mathbf{P_{DM}}$, given the fire characteristics for the component combination being analyzed is similar or bounded by the fire testing reported in EPRI TR-1003326. Larger fires, such as large transformer fires, large pump fires, etc., or cables directly in a fire plume may not be bounded by the EPRI tests. Similarly when looking at damage of cables not in overhead raceways (such as cables in cabinets), the estimates above are not applicable. Application of this type of approach would provide some uncertainty and should be conservatively applied. This should also be considered in the uncertainty analysis of the screening process.

8. If **? CDF = $F_f$ * $P_E$ * $P_{SA}$ * $P_{AS}$ * $P_{DM}$** < 1E-7 per reactor year for the component(s) in the fire area, and < 1E-6 for all fire areas, screen the component(s) from further review if SM and DID considerations permit. If these thresholds are not met, or if circuits for more that one component combinations are routed in the same fire area such that the sum of the ?CDFs associated with all component pairs of concern in a fire area is >1E-6/year, proceed to Screen Four or consider corrective actions.

**Screen Four**

*When Screen Three is complete, one has calculated the probability of spurious actuation(s) for the component combination being evaluated. The purpose of Screen Four is to determine the change in the conditional core damage probability given that spurious actuation(s) have occurred.*

9. Change in conditional probability of core damage given fire-induced failures including spurious actuations of component combination **? $P_{CCD}$** – using a modified internal events PRA or fire IPEEE analysis, determine the change in CCDP (**?$P_{CCD}$**) of the component combination of concern for the target component(s) and other credited components damaged by a fire. This is done by assigning a failure probability of 1.0 for these damaged components that are in the PRA, using the area fire frequency as the initiating event and an appropriate event tree. This analysis does not quantify the size or extent of the fire, except that it is confined to the fire area in question. Calculate the difference from the nominal CDF (**?$P_{CCD}$**). Further details can be found in the "Fire PRA Implementation Guide," EPRI TR-105928 (Appendix K).

   This analysis may be performed using the current internal events PRA modified to include a fire risk sources or the plant's IPEEE fire PRA to determine the change in CCDP (conditional core damage probability) for all available mitigation systems, some of which may not have been credited in safe shutdown analyses. The CCDP calculation may be as simple as a single point estimate value, or may be more complicated to determine. If a single point estimate value is used, this can come directly from the PRA or IPEEE analysis. However, if the CCDP requires model changes, it is likely the PRA or IPEEE would require restructuring to determine the impact of the fire scenario. This evaluation may be performed to determine the incremental risk reduction benefit provided by systems or equipment not previously credited for safe shutdown, to mitigate the unacceptable consequences of the spurious actuation. Note that if potential circuit failures in the target conductors are not addressed by the deterministic mitigation techniques (see Step 3), then further analysis to address the value of potential recovery actions may be useful.

The calculation for CCDP should be reviewed to ensure the credited SSD equipment is free of fire damage for the area or scenario being analyzed. This includes both primary cables for a function, and cables that may fail a component or system due to spurious operation. If the credited SSD equipment is in the fire area, but not initially damaged by the fire assumed for the component combination fire scenario, then additional analysis may be required to bound the analysis and determine the core damage risk.

Since the NEI-00-01 method performs a limited Fire PRA for the selected scenarios, no previous Fire PRA is required. The PRA models used for the CCDP calculations should however represent the present plant design, and should be reviewed to assure accuracy. Feedback from the pilot evaluations has shown that many of the scenarios analyzed either did not require a CCDP calculation (Screened early) or the CCDP calculation was limited by a single evaluation/data point. For example, the McGuire analysis Scenario 1 was a loss of all Auxiliary Feedwater. The CCDP was basically the availability of MFW following a plant trip. This was a point estimate evaluation, based on plant specific data. The quality of the PRA for this sequence is limited to the assurance that this CCDP represents the as-built plant. Other evaluations may require additional quality. A living internal events PRA, representing the as-built plant, should provide sufficient quality for this evaluation.

10. Determine whether systems not previously credited, but are capable of mitigating the consequences of the spurious actuation, have components or cables located outside the fire area. The configuration management of this alternate equipment needs to be addressed.

11. If $\Delta CDF = F_f * P_E * P_{SA} * P_{AS} * P_{DM} * \Delta P_{CCD}$ < 1E-7 per reactor year for the component(s) in the fire area, and < 1E-6 for all fire areas, screen the component(s) from further review if SM and DID considerations permit. If these thresholds are not reached, or if circuits for more that one component combinations are routed in the same fire area such that the sum of the ?CDFs associated with all component pairs of concern in a fire area is >1E-6/year, proceed to Screen Five or consider corrective actions.

**Screen Five**

*The purpose of Screen Five is to use fire modeling techniques to recalculate fire damage more representative of the fire scenario.*

12. Screen 1 is based on estimating fire propagation and damage using simplified methods that make bounding assumptions in fire size and source-target geometry. In this screening step, fire propagation and damage will be evaluated using various fire modeling techniques. Such techniques are

described in EPRI's FIVE, Fire PRA Guide methodologies and Appendix C of NFPA 805.

13. Modify estimates for, fire size parameter ($\mathbf{P_E}$), automatic ($\mathbf{P_{AS}}$) and manual suppression ($\mathbf{P_{DM}}$) as appropriate to reflect calculated time to damage and time to detection for the detailed fire modeling.

14. If $\mathbf{F_f} * \mathbf{P_E} * \mathbf{P_{SA}} * \mathbf{P_{AS}} * \mathbf{P_{DM}} * \mathbf{?}\ \mathbf{P_{CCD}} < 1E\text{-}7$ per reactor year for the component combination in the fire area, and < 1E-6 for all fire areas, screen the component combination from further review if SM and DID considerations permit. If these thresholds are not reached, or if circuits for the component combination are routed in the same fire area such that the sum of the ?CDFs associated with all component pairs of concern in a fire area is >1E-6/year, corrective actions should be considered.

### 4.3.4 Large Early Release Frequency Evaluation

Screening of any component combination requires the consideration of Large Early Release Frequency (LERF) risk 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, and are as follows:

- If $\mathbf{F_f} * \mathbf{P_E} * \mathbf{P_{SA}} * \mathbf{P_{AS}} * \mathbf{P_{DM}} * \mathbf{?}\ \mathbf{P_{LERF}} < 1E\text{-}8$ per reactor year for the component combination in the fire area, and < 1E-7 for all fire areas, screen the component combination from further review if SM and DID considerations permit. If these thresholds are not reached, or if circuits for the component combination are routed in the same fire area such that the sum of the ?LERFs associated with all component pairs of concern in a fire area is >1E-7/year, corrective actions should be considered

The following are three methods that can be used to meet the LERF criteria above:

- No LERF review is needed if the screened scenario is shown to have a CDF < 1E-08 with 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. Barrier 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.

Component combinations screened in the preliminary screening do not need a LERF evaluation is the combination has one or more than one DID factor than is required to screen. For example, if based on Table 4-1, two DID elements are required, and the combination has three, then no LERF evaluation is required since the LERF criterion is met. If the condition is not met, then a qualitative LERF review is required per c) above to screen the combination.

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

### 4.3.5 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. 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 that 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. For the above screening process, this guidance is interpreted as follows:

- Scenarios screened in the qualitative screening or with a risk at least a factor of 10 lower than all acceptance criteria discussed above, can be treated with a qualitative discussion of uncertainty. If uncertainty is determined to be too large to reasonably assure that the risk is below the acceptance criteria, then a more detailed consideration of uncertainty is needed.

- Scenarios whose risk, either in a given area or total risk, is within a factor of 10 of the acceptance criteria, quantitative uncertainty and/or sensitivity analysis is required.

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

a) Sensitivity of the results to uncertainty of the factors in the screening formula. 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.*

## 4.3 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 can not 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.

### 4.4.1 Defense-In-Depth and Safety Margins Considerations

The information in Section 4.4.4.1 is derived from Appendix A to NFPA 805, 2001 Edition, and Regulatory Guide 1.174, July 1998. These methods should be applied to issues that are screened out either after the application of Tables 4-1 through 4-3, or after the quantitative risk significance screen in Section 4.3.

#### 4.4.1.1 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 Reg. Guide 1.174, Section 2.2.1.1. Reg. Guide 1.174 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 LB 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 quickly and suppressing those fires that occur, thereby limiting damage
- Designing the plant to limit the consequences of fire relative to life, property, environment, continuity of plant operation, and nuclear safety capability

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, with fire areas with likely fires having automatic suppression, while areas with less likely and smaller fires not having automatic suppression, some areas allowing transient combustible storage, and some not, etc. Fire PRA would show balance in DID if the risk to the public is low. 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 among prevention of fires, early detection and suppression of fires, and fire confinement is preserved.

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.

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, Safety Margins, 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.

#### 4.4.1.2 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:

- 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 provides sufficient margin to account for analysis and data uncertainty.

### 4.4.2 Corrective Action

If, when all evaluation phases are completed, the ? 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 ? 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 ?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 ? 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 ? CDF of 1E-5 per reactor year for any fire area after completing the screening process, a corrective action which 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 place within the plant's Corrective Action Program. 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, refer to Figure 3-4, Step 5, to 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.

### 4.4.3 Documentation

The accurate and comprehensive documentation of this assessment will be prepared and maintained as a retrievable plant record following established practices. These practices will generally not be 10CFR 50 Appendix B criteria, but good plant practices. The documentation should be maintained in accordance with existing plant procedures.

# 5 DEFINITIONS

The following definitions are derived using the general industry recognized definition of the term around the time of inception of Appendix R.

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 6.4.32.

**Associated circuits**

*Generic Letter 81-12* – Those cables (safety related, non-safety 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., RHR/RCS isolation valves, ADS valves, PORVs, 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. Refer to Appendix E to this document for additional information related to cold shutdown repairs.

**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**

An emergency control station includes the remote shutdown panel(s), local starters, electrical distribution panels, MOV handwheels and other equipment locations designed for operator use or monitoring.

**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 9.5.1* - 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 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**

Achieved when the structure, system or component under consideration is capable of performing its intended function during and after the postulated fire, as needed. It may perform this function automatically, by remote control (which includes manual operations and/or remote manual operations) or by local operation.

**Generic Letter 86-10 Fire Hazards Evaluation**

A technical engineering evaluation used to document equivalent fire protection features to that required by the regulations or to document 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. 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 on the required safe shutdown path by an operator when automatic, remote manual or manual operation are no longer available (e.g. opening of a motor operated valve using the hand wheel).

**Manual Operation**

Operation of safe shutdown equipment on the required safe shutdown path using the control room control devices (e.g., switches) in the event that automatic control of the equipment is either inhibited based on plant procedures or unable to function as a result of fire-induced damage.

**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.2.

**Open Circuit**

See 'Circuit failure modes'.

**Probability of Spurious Actuation ($P_{SA}$)**

The probability of undesirable spurious actuation(s) of the component or component 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 of 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 of the control room with remote control capability.

**Remote Shutdown Panel**

The plant location included within the plant design for the purpose of satisfying the requirements of 10 CFR 50 Appendix A General Design Criteria 19. If electrical isolation and redundant fusing is 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 in order 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 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 in order that the required safe shutdown path will be capable of achieving and maintaining safe shutdown in a particular fire area.

**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**

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.

**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 included in the analysis of post-fire safe shutdown capability to demonstrate compliance with Appendix R.

**Short-to-Ground**

See 'Circuit failure modes'.

**Spurious Operation**

The inadvertent operation or repositioning of a piece of equipment.

# 6 REFERENCES

## 6.1 NRC GENERIC LETTERS

6.1.1 80-45: Proposed Rule Fire Protection Program for Nuclear Power Plants

6.1.2 80-48: Proposed Rule Fire Protection Program for Nuclear Power Plants

6.1.3 80-56: Memorandum and Order RE: Union of Concerned Scientists Petition

6.1.4 80-100: Resolution of Fire Protection Open Items

6.1.5 81-12: Fire Protection Rule, dated February 20, 1981

6.1.6 81-12: Clarification of Generic Letter 81-12, Letter from the NRC to PSE&G, dated April 20, 1982, Fire Protection Rule - 10CFR50.48(c) - Alternate Safe Shutdown - Section III.G.3 of Appendix R to 10CFR50

6.1.7 82-21: Tech Specs for Fire Protection Audits

6.1.8 83-33: NRC Positions on Appendix R

6.1.9 85-01: Fire Protection Policy Steering Committee Report

6.1.10 86-10: Implementation of Fire Protection Requirements, dated April 24, 1986

6.1.11 86-10: Supplement 1 to Generic Letter, Implementation of Fire Protection Requirements

6.1.12 88-12: Removal of Fire Protection Requirements from Tech Specs

6.1.13 88-20: Supplement 4 IPEEE

6.1.14 89-13: Supplement 1 Biofouling of Fire Protection Systems

6.1.15 92-08: Thermo-Lag Fire Barriers

6.1.16 93-06: Use of Combustible Gases in Vital Areas

6.1.17 95-01: Fire Protection for Fuel Cycle Facilities

## 6.2 BULLETINS

6.2.1 75-04: Browns Ferry Fire

6.2.2 77-08: Assurance of Safety

6.2.3 81-03: Flow Blockage Due to Clams and Mussels

6.2.4 92-01: Failure of Thermo-Lag

6.2.5 92-01: Supplement 1 Failure of Thermo-Lag

## 6.3 NRC INFORMATION NOTICES

6.3.1 80-25: Transportation of Pyrophoric Uranium

6.3.2 83-41: Actuation of Fire Suppression System causing Inoperability of Safety-Related Equipment, June 22, 1983

6.3.3 83-69: Improperly installed Fire Dampers

6.3.4 83-83: Use of Portable Radio Transmitters Inside Nuclear Power Plants

6.3.5 84-09: Lessons learned from NRC Inspections of Fire Protection Safe Shutdown Systems (10CFR50, Appendix R), Revision 1, March 7, 1984

6.3.6 84-16: Failure of Automatic Sprinkler System Valves to Operate

6.3.7 84-92: Cracking of Flywheels on Fire Pump Diesel Engines

6.3.8 85-09: Isolation Transfer Switches and Post-fire Shutdown Capability, January 31, 1985

6.3.9 85-85: System Interaction Event Resulting in Reactor Safety Relief Valve Opening

6.3.10 86-17: Update - Failure of Automatic Sprinkler System Valves

6.3.11 86-35: Fire in Compressible Material

6.3.12 86-106: Surry Feedwater Line Break

6.3.13 86-106: Supplement 1 Surry Feedwater Line Break

6.3.14 86-106: Supplement 2 Surry Feedwater Line Break

6.3.15 86-106: Supplement 3 Surry Feedwater Line Break

6.3.16 87-14: Actuation of Fire Supp. Causing Inop of Safety Related Ventilation

6.3.17 87-49: Deficiencies in Outside Containment Flooding Protection

6.3.18 87-50: Potential LOCA at High and Low Pressure Interfaces from Fire Damage, October 9, 1987

6.3.19 88-04: Inadequate Qualification of Fire Barrier Penetration Seals

6.3.20 88-04: Supplement 1 Inadequate Qualification of Fire Barrier Penetration Seals

6.3.21 88-05: Fire in Annunciator Control Cabinets

6.3.22 88-45: Problems in Protective Relay and Circuit Breaker Coordination, July 7, 1988

6.3.23 88-56: Silicone Fire Barrier Penetration Seals

6.3.24 88-60: Inadequate Design & Installation of Watertight Penetration Seals

6.3.25 88-64: Reporting Fires in Process Systems

6.3.26 89-52: Fire Damper Operational Problems

6.3.27 90-69: Adequacy of Emergency and Essential Lighting, October 31, 1990

6.3.28 91-17: Fire Safety of Temporary Installations

6.3.29 91-18: Resolution of Degraded & Nonconforming Conditions

6.3.30 91-37: Compressed Gas Cylinder Missile Hazards

6.3.31 91-47: Failure of Thermo-Lag

6.3.32 91-53: Failure of Remote Shutdown Instrumentation

6.3.33 91-77: Shift Staffing at Nuclear Power Plants

6.3.34 91-79: Deficiencies in Installing Thermo-Lag

6.3.35 91-79: Supplement 1

6.3.36 92-14: Uranium Oxide Fires

6.3.37 92-18: Loss of Remote Shutdown Capability During a Fire, February 28, 1992

6.3.38 92-28: Inadequate Fire Suppression System Testing

6.3.39 92-46: Thermo-Lag Fire Barrier Special Review Team Final Report

6.3.40 92-55: Thermo-Lag Fire Endurance Test Results

6.3.41 92-82: Thermo-Lag Combustibility Testing

6.3.42 93-40: Thermal Ceramics Fire Endurance Tests

6.3.43 93-41: Fire Endurance Tests - Kaowool, Interam

6.3.44 93-71: Fire at Chernobyl Unit 2

6.3.45 94-12: Resolution of GI 57 Effects of Fire Prot. Sys. Actuation on SR Equipt.

6.3.46 94-22: Thermo-Lag 3-Hour Fire Endurance Tests

6.3.47 94-26: Personnel Hazards From Smoldering Material in the Drywell

6.3.48 94-28: Problems with Fire-Barrier Penetration Seals

6.3.49 94-31: Failure of Wilco Lexan Fire Hose Nozzles

6.3.50 94-34: Thermo-Lag Flexi-Blanket Ampacity Derating Concerns

6.3.51 94-58: Reactor Coolant Pump Lube Oil Fire

6.3.52 94-86: Legal Actions Against Thermal Science Inc.

6.3.53 94-86: Supplement 1

6.3.54 95-27: NRC Review of NEI Thermo-Lag Combustibility Evaluation Methodology

6.3.55 95-32: Thermo-Lag 330-1 Flame Spread Test Results

6.3.56 95-33: Switchgear Fire at Waterford Unit 3

6.3.57 95-36: Problems with Post-Fire Emergency Lighting

6.3.58 95-36: Supplement 1

6.3.59 95-48: Results of Shift Staffing Survey

6.3.60 95-49: Seismic Adequacy of Thermo-Lag Panels

6.3.61 95-49: Supplement 1

6.3.62 95-52: Fire Test Results of 3M Interam Fire Barrier Materials

6.3.63 95-52: Supplement 1

6.3.64 96-23: Fire in Emergency Diesel Generator Exciter

6.3.65 97-01: Improper Electrical Grounding Results in Simultaneous Fires

6.3.66 97-23: Reporting of Fires at Fuel Cycle Facilities

6.3.67 97-37: Main Transformer Fault

6.3.68 97-48: Inadequate Fire Protection Compensatory Measures

6.3.69 97-59: Fire Endurance Tests of Versawrap Fire Barriers

6.3.70 97-70: Problems with Fire Barrier Penetration Seals

6.3.71 97-72: Problems with Omega Sprinkler Heads

6.3.72 97-73: Fire Hazard in the Use of a Leak Sealant

6.3.73 97-82: Inadvertent Control Room Halon Actuation

## 6.4 OTHER RELATED DOCUMENTS

6.4.1 10 CFR 50.48 Fire Protection (45 FR 76602)

6.4.2 10 CFR 50 Appendix A GDC 3 Fire Protection

6.4.3 10 CFR 50 Appendix R Fire Protection for Operating Nuclear Power Plants

6.4.4 Branch Technical Position APCSB 9.5-1 Guidelines for Fire Protection

6.4.5 Appendix A to Branch Tech Position 9.5-1 Guidelines for Fire Protection

6.4.6 NUREG-0800 9.5.1 Fire Protection Program

6.4.7 NRC Insp. Procedure 64100 Postfire Safe Shutdown, Emergency Lighting, Oil Collection

6.4.8 NRC Insp. Procedure 64150 Triennial Postfire Safe Shutdown Capability

6.4.9 NRC Insp. Procedure 64704 Fire Protection Program

6.4.10 NUREG/BR-0195 Enforcement Guidance

6.4.11 NUREG-75/087 Standard Review Plan (No revision level listed)

6.4.12 NUREG-75/087 Standard Review Plan, Rev. 1

6.4.13 NUREG-75/087 Standard Review Plan, Rev. 2

6.4.14 Reg Guide 1.120 Fire Protection Guidelines for Nuclear Power Plants

6.4.15 Reg Guide 1.120 Rev. 1, Fire Protection Guidelines for Nuclear Power Plants

6.4.16 Reg Guide 1.189 Fire Protection for Operating Nuclear Power Plants

6.4.17 NUREG-0654 Criteria for Preparation of Emergency Response Plans

6.4.18 Temporary Instruction 2515/XXX Fire Protection Functional Inspection

6.4.19 SECY-82-13B (4/21/82) Fire Protection Schedules and Exemptions

6.4.20 SECY-82-267 (6/23/82) FP Rule for Future Plants

6.4.21 SECY-83-269 FP Rule for Future Plants

6.4.22 SECY-85-306 Recommendations Regarding the Implementation of App R to 10CFR50

6.4.23 NRC Temp Instruction 2515/62 Inspection of Safe Shutdown Requirements of 10CFR50

6.4.24 NRC Temp Instruction 2515/61 Inspection of Emergency Lighting & Oil Collection Requirements

6.4.25 NUREG-0050, 2/76; Recommendations Related to Browns Ferry Fire

6.4.26 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 uncovery occurs.

6.4.27 SECY-93-143 Assessment of Fire Protection Programs

6.4.28 SECY-95-034 Re-assessment of Fire Protection Programs

6.4.29 SECY-96-134 Fire Protection Regulation Improvement

6.4.30 Appendix S Proposed Rulemaking

6.4.31 NRC letter to NEI dated March 11, 1997; general subject NRC positions on fire-induced circuit failures issues

6.4.32 NEI letter to NRC dated May 30, 1997, general subject industry positions on fire-induced circuit failures issues

6.4.33 GE-NE-T43-00002-00-02, Revision 0, "Generic Guidance for BWR Post-Fire Safe Shutdown Analysis," November 1999

6.4.33 NFPA 805, "Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants," November 2000 ROP

6.4.34 NSAC-179L, "Automatic and Manual Suppression Reliability Data for Nuclear Power Plant Fire Risk Analyses", February 1994

6.4.35 EPRI TR-100370, "Fire-Induced Vulnerability Evaluation (FIVE)", April 1992

6.4.36 EPRI TR-105928, "Fire PRA Implementation Guide", December 1995

6.4.37 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"

6.4.38 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

6.4.39 EPRI Report 1006961, "Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of An Expert Elicitation"

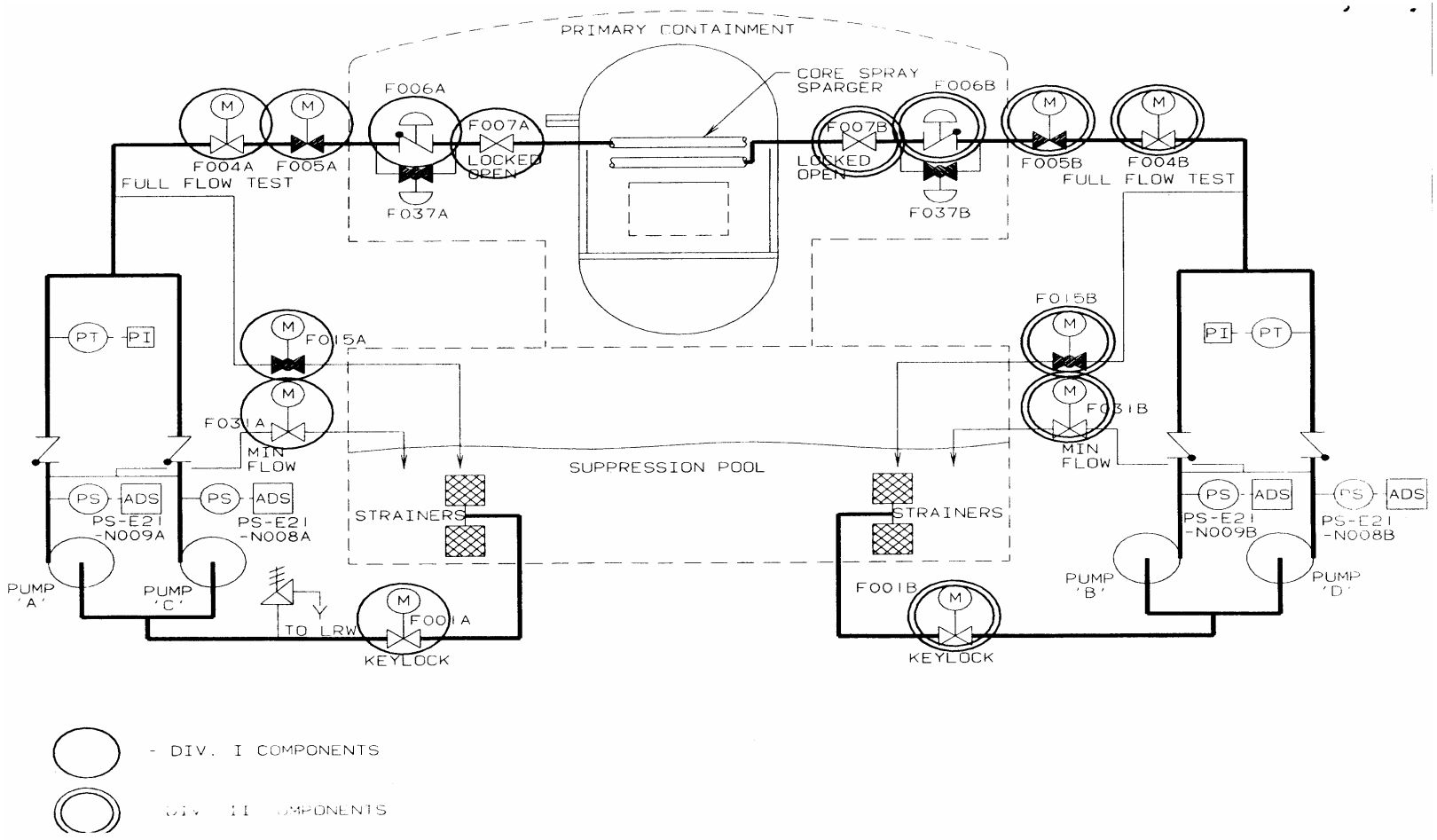
## 6.5 ADMIN LETTERS

6.5.1 95-06 Relocation of Technical Specification Administrative Controls

# Attachment 1
# Example for Typical BWR Safe Shutdown Path Development

| Safe Shutdown Path 1 | Safe Shutdown Path 2 | Safe Shutdown Path 3 |
|---|---|---|
| ***Reactivity Control*** | ***Reactivity Control*** | ***Reactivity Control*** |
| CRD (Scram Function)<br>Manual Scram | CRD (Scram Function)<br>Manual Scram | CRD (Scram Function)<br>Manual Scram |
| ***Pressure Control*** | ***Pressure Control*** | ***Pressure Control*** |
| Manual ADS/SRVs | SRVs | Manual ADS/SRVs |
| ***Inventory Control*** | ***Inventory Control*** | ***Inventory Control*** |
| Core Spray | RCIC<br>RHR LPCI | RHR LPCI |
| ***Decay Heat Removal*** | ***Decay Heat Removal*** | ***Decay Heat Removal*** |
| RHR Supp. Pool Cooling Mode<br>Service Water<br>Core Spray, Alt. SDC Mode | RHR Supp. Pool Cooling Mode<br>Service Water<br>RHR Shutdown Cooling Mode | RHR Supp. Pool Cooling Mode<br>Service Water<br>RHR, Alt. SDC Mode |
| ***Process Monitoring*** | ***Process Monitoring*** | ***Process Monitoring*** |
| Supp. Pool Monitoring<br>Nuc. Boiler Instru. | Supp. Pool Monitoring<br>Nuc. Boiler Instru. | Supp. Pool Monitoring<br>Nuc. Boiler Instru. |
| ***Associated Support Functions*** | ***Associated Support Functions*** | ***Associated Support Function*** |
| ***Cooling Systems*** | ***Cooling Systems*** | ***Cooling Systems*** |
| RHR Room Coolers<br><br>Service Water Pumphouse<br>HVAC<br>EDG HVAC | RHR Room Coolers<br>RCIC Room Coolers<br>Service Water Pumphouse<br>HVAC<br>EDG HVAC | RHR Room Coolers<br><br>Service Water Pumphouse<br>HVAC<br>EDG HVAC |
| ***Electrical*** | ***Electrical*** | ***Electrical*** |
| EDGs or Offsite Power<br>Electrical Distribution<br>Equipment | EDGs or Offsite Power<br>Electrical Distribution<br>Equipment | EDGs or Offsite Power<br>Electrical Distribution<br>Equipment |

# Attachment 2
# Annotated P&ID Illustrating SSD System Paths [BWR Example]



# Attachment 3
# Safe Shutdown Equipment List

*(Sorted by Equipment ID)*

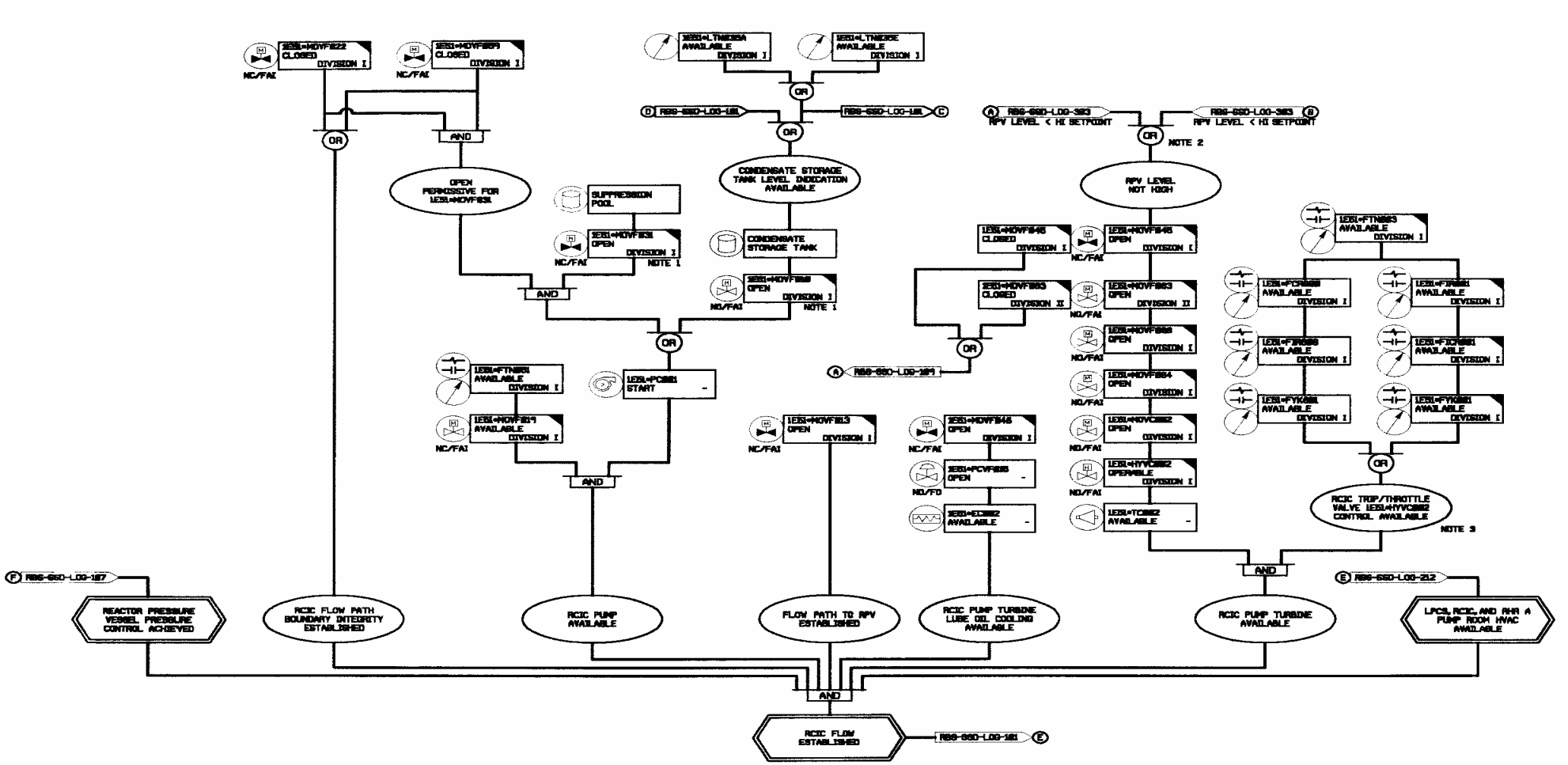
| Equipment ID | Logic Diagram | System | Unit | Equipment Type | SSD Path | Equipment Description | Equip FA | Normal Mode | Shutdown Mode(s) | Hi/Lo | Air Fail | Power Fail | Reference |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

# 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. |
| **Hi/Lo** | 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
# Example Safe Shutdown Logic Diagram [BWR Example]



# Attachment 5
# Affected Equipment Report

*(Sorted by Fire Area, System, Unit & Equipment ID)*

| Fire Area: | | Required Path(s): | | FA Description: | | Suppression: | | Detection: | |
|---|---|---|---|---|---|---|---|---|---|

| System | Unit | Logic Diagram | Equipment ID | Equip Type | SSD Path | Equip FA | Equipment Description | Normal Mode | Shutdown Mode(s) | Hi/Lo | Air Fail | Power Fail | Disp Code | Compliance Strategy |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

# Attachment 5
# (Continued)

A description of the Affected Equipment 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. |
| **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. |
| **Hi/Lo** | 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
## Fire Area Assessment Report
*(Sorted by Fire Area, System, Unit & Equipment ID)*

| **Fire Area:** | | | **Required Path(s):** | | | **System:** | | | | | **Unit:** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Equipment ID | Logic Diagram | Equip Type | SSD Path | Equip FA | Equipment Description | Normal Mode | Shutdown Mode(s) | Hi/Lo | Air Fail | Power Fail | Cable | Cable Funct | Disp Code | Compliance Strategy |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

# 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. |
| **Hi/Lo** | 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 it's failure can result in a spurious actuation. |
| **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.1.0 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.2.0 INTRODUCTION

Each licensee's Fire Protection Program is based on the concept of defense-in-depth (refer to Section 4.4.1.1). 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 Brown's 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 Brown's Ferry is not expected to re-occur.

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 pndustry relative to these recommendations.

## A.3.0 OVERVIEW

### A.3.1 Brown's 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 shutdown 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, alternate 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, 10CFR50.48 and 10CFR50 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 10CFR50, Appendix R included requirements for safe shutdown capability, emergency lighting, fire barriers, fire barrier penetration seals, associated circuits, reactor coolant pump lubrication system, and alternate 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 individual plant, 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 $CO_2$ and dry chemical extinguishers, continued for approximately 7 hours with little success until water was used to complete the final extinguishing process.

During the seven-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 shutdown. 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 shutdown. 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, have 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 non-safety 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).

- Failure to provide automatic fire suppression (e.g., sprinklers) in an area highly congested with cabling and other combustibles, containing redundant divisional open tray raceway systems carrying circuits necessary for safe shutdown.

### 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 APCSB 9.5-1, Appendix A, 10CFR50 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, 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.

**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.
- Non-combustible or less flammable materials including penetration seals, cable jackets, 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 that 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.
- 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 alternate or dedicated fire safe shutdown system has been established as follows:

  Alternate 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 is provided.

## A.4.0 CONCLUSION

The changes made to the plant fire protection programs in response to the Brown's 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.

## .5.0 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

# APPENDIX B

# DETERMINISTIC CIRCUIT FAILURE CHARACTERIZATION

## B.1.0 PURPOSE

The purpose of this appendix is to provide guidance in evaluating circuit failures within a deterministic analysis. This appendix serves to identify the types of circuit failures that have been typically considered as part of a deterministic analysis. In addition, rationale supporting the elimination of certain types of circuit failures from a plant's deterministic analysis criteria are provided as sub-appendices. Reference to industry experience and fire test results is made to support the characterization of whether certain combinations of circuit failures should be considered as credible in performing a deterministic evaluation.

## B.2.0 INTRODUCTION

Appendix R requires that equipment and circuits required for safe shutdown be free of fire damage and that these circuits be evaluated for the fire-induced effects of a hot shorts, shorts-to-ground, and open circuits. As proposed by this document, Section 3 provides a deterministic methodology for evaluating the effects of fire damage within the licensing basis by determining the effects of each of these types of circuit failures on each conductor one at a time. Section 4 provides a method for evaluating the effects of combinations of failures (whether multiple circuit failure modes or multiple spurious component actuations), which are generally considered by industry to be outside plant licensing bases.

## B.3.0 CIRCUIT FAILURES CONSIDERED IN DETERMINISTIC ANALYSIS

A typical Appendix R analysis includes identifying the location of safe shutdown cables by fire area and postulating fire damage to occur to the unprotected cables within the fire area. Initially, it may be assumed that any cable related to a required safe shutdown component in a given fire area will cause the component to fail either due to a loss of motive power, loss of control power or spurious actuation. In order to evaluate the impact of fire damage on each cable, the deterministic approach considers three types of circuit failures (hot short, short to ground, open circuit) to occur individually on each conductor of each unprotected safe shutdown cable on the required safe shutdown path in the fire area. A method to mitigate the result from each postulated circuit failure type is typically provided.

Typically, a short to ground or an open circuit would result in a loss of control power or motive power to the safe shutdown component and a hot short on specific conductors may cause a spurious actuation. Upon further investigation of the conductors within each

cable, it is possible to distinguish the actual cables of concern that may cause component failure especially in the cases involving spurious actuations.

The deterministic method is conservative because it postulates the failure of all the unprotected cables within a fire area unless adequate separation is provided. In most cases, the levels of combustibles and fire hazards within a fire area may be insufficient to result in the damage of all the cables that are assumed to fail. Nevertheless, the deterministic approach assumes that power is lost to operate and control each component affected by fire damage to the unprotected cables in the fire area. In addition, spurious actuations are postulated in cases where specific cable conductors with the capability to cause a component to spuriously operate are routed together in the fire area under evaluation. Although conservative, this approach provides a consistent and widely accepted method for identifying Appendix R impacts.

Selected high/low pressure interface equipment is also evaluated but to more stringent requirements than non-high/low pressure interfaces when considering spurious operations to ensure that a fire induced LOCA does not occur. Since the high/low pressure interface components are relatively few in number and these were identified as part of the analysis, spurious actuations of multiple high/low pressure interface components were included as part of the deterministic analysis.

## B.4.0 CIRCUIT FAILURES EXCLUDED FROM DETERMINISTIC ANALYSIS

The deterministic analysis provides a consistent and established method to mitigate the effects from postulating specific types of circuit failures (hot short, short to ground, open circuit) on each conductor of each unprotected safe shutdown cable on the required safe shutdown path in the fire area. Typically, the components whose cables are damaged by the fire in a fire area are assumed to be out of service and to be unavailable for supporting post-fire safe shutdown.

In recent years growing concern has been expressed regarding the combination of spurious actuations of other than non-high/low pressure interface components. Not only are many of these combinations of circuit failure types unlikely to occur, but also there is no consistent way to address the multitude of scenarios that may occur when postulating combinations of circuit failure types and/or combinations of component spurious actuations. To consider the effects of multiple concurrent circuit failure types and affected components that may spuriously actuate as a result of the fire damage re-designing the various circuits within a fire area becomes a daunting and overwhelming task.

Therefore, additional guidance is necessary to ensure that the deterministic analysis is performed in a consistent manner throughout the industry. The guidance provided in NRC Generic Letter 86-10, Question 5.3.1 states in part the following regarding the probability of hot shorts:

"*…. 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 clearly establishes a basis for limiting the number of credible circuit failure modes because it acknowledges the existence of circuit failure combinations that are highly improbable.

A sense of balance is needed when considering combinations of spurious actuations, many of which are caused by a hot short. Therefore, determinations have been made to exclude certain combinations of circuit failures from the deterministic analysis. For example, the following sub-appendices have been developed to provide a basis for the elimination of certain types of combination circuit failures from the deterministic analysis since these were determined by the industry to be highly unlikely:

- Appendix B.1 Justification for the Elimination of Multi-Conductor Hot Shorts Involving Power Cables
- Appendix B.2 Justification for the Elimination of Multiple High Impedance Faults

## B.5.0 INSIGHTS FROM CABLE FIRE TESTS

Based on further cable failure research including cable fire test results, additional insights have been gained in understanding the factors that contribute to cable fire damage. The purpose of this testing was to expose realistic control circuits and cables to a range of fire conditions, and try to determine the timing and duration of any failures (including spurious actuations) in any of the monitored electrical circuits.

The following key observations and conclusions are derived from the results of this testing:

1. Observation: Specific behavior and characteristic of any one circuit fault is difficult, but some clear behavioral trends can be seen.

   Conclusion:
2. Observation: Open circuits did not occur..

   Conclusion: Open circuits are not likely to be the initial fire-induced circuit cable failure mode

3. Observation: Failure temperatures for thermoset and armored cable were higher than for thermoplastic cable

   Conclusion: Thermoset and armored cable have much higher thresholds for damage than does thermoplastic cable

4. Observation: The probability of hot shorts in thermoset and thermoplastic cable is about the same

   Observation: The probability of spurious actuations in thermoset cable is lower than for thermoplastic. There were no spurious actuations observed in thermoset cable from external cable hot shorts

   Conclusion: Cable type has a stronger influence on the probability of spurious actuations than on the probability of hot shorts. The probability of spurious actuations from external cables is low for thermoset cables

5. Observations: Conductor-to-conductor hot shorts are more likely to occur than cable-to-cable hot shorts. The probability of multiple internal hot shorts in multiconductor cables is high

   Conclusion: Multiple simultaneous spurious actuations is likely if there is fire-induced cable damage and if circuits for these devices are in the same multiconductor cable. However, considering the Conclusion #4, they are not likely if there is no damage to thermoset cable or if the circuits are in separate cables. Pre-fire proximity of conductors is a predominant factor in determining the ultimate failure mode of the cable.

6. Observation: Depending on circuit grounding, short to ground faults and hot shorts are equally likely in multiconductor cable.

   Conclusion: Based on this and other observations, statistical characterization of circuit failures is achievable, but definitive predictions of specific localized failure modes are not

7. Observation: High impedance faults were not observed

   Conclusion: This observation provides further support for the view that, if certain criteria are met, consideration of multiple high impedance faults is not necessary. See Appendix B.2 for further information.

8. Observation: Spurious actuations are significantly less likely under the following conditions:

   Thermoset or armored cable
   Greater percent tray fill

Connection patterns other than Source Centered
Circuits with current limiting devices such as Control Power Transformers

Conclusion: Important influence factors in determining the probability of spurious actuations include cable type, tray fill, conductor connection pattern, and power source characteristics.

9. Observation: The average time to spurious actuation averaged 46 minutes for thermoset cable and 25 minutes for thermoplastic cable. The single observed spurious actuation for armored cable was 36 minutes.

   Conclusion: These statistics demonstrate that significant opportunities for fire suppression are available before significant cable damage can occur

10. Observation: Spurious actuations lasted an average of 2 minutes before shorting to ground occurred to terminate the hot short.

    Conclusion: This may be useful for AOVs that return to the non-actuated state when power is removed.

# APPENDIX B.1

# JUSTIFICATION FOR THE ELIMINATION OF MULTI-CONDUCTOR HOT SHORTS INVOLVING POWER CABLES

## B.1-1 THREE-PHASE AC POWER CIRCUIT

Generic Letter (GL) 86-10 implied a limit on the potential combination of circuit failures for other non-High/Low components. Consequently, it is reasonable to conclude that there should be a limit as to the intelligence given to a fire to rewire a circuit even for high/low pressure interface components. The potential for a fire to cause a hot short on all three phases in the proper sequence to cause spurious operation of a motor is highly unlikely for the following reasons.

For a three phase short to occur that would cause a High/Low Pressure Interface valve to reposition to the undesired position (open), the three phase cabling for the High/Low Pressure Interface valve would have to be impinged upon by another three phase "aggressor" cable in the same raceway. This would have to occur downstream of the MCC powering the motor since the motor starting contacts (which are only closed when the valve's control circuitry drives the motor) located within the MCC would prevent any short upstream of the MCC from affecting the valve. This aggressor cable would also have to be a cable that was supplying a continuously running load; otherwise the aggressor cable would normally be de-energized and therefore would be of no consequence. Furthermore, the aggressor cable would have to be supplying a load of such magnitude that the overcurrent protective relaying (specifically, the time overcurrent feature) would not trip when the valve motor initially started running, since now the upstream breaker would be supplying both its normal load and the considerable starting amperage of the High/Low Pressure Interface valve.

Additionally, in order to cause the High/Low pressure interface valve to open, the aggressor cable would have to short all three of its phases to the three phases on the cable for the High/Low valve. These three phases would have to be shorted to the valve power cabling in the exact sequence such that the High/Low valve would fail in the open position (a one-out-of-two probability, assuming three hot shorts of diverse phases were to occur.).

The High/Low valve cabling conductors, as well as the aggressor's conductors, could not be shorted to ground or shorted to each other at any time. Since three-phase cabling is typically in a triplex configuration (three cables, each separately insulated, wound around each other – similar to rope), for three shorts to occur, the insulation would have to be broken down sufficiently on all three phases in both cables such that a direct short would occur. However, the rest of the cables would have to be insulated sufficiently such that

any other area of insulation breakdown would not result in a ground or a short to any of the other conductors within the cables. This is highly unlikely.

Therefore, based upon the unique characteristics of three phased cabling and loads, a consequential three phase short on a High/Low Pressure Interface valve need not be postulated.

### B.1-2 DC POWER CIRCUIT

Similar arguments may be used to demonstrate the implausibility of consequential hot shorts on a DC reversing motor of a motor operated valve. A typical reversing DC compound motor power circuit uses five conductors and must energize a series field, shunt field, and armature to cause the motor to operate. The polarity of the armature determines the direction of the motor. For this type of motor, two specific conductors of the power cable would require a hot short from an aggressor cable (of the same and correct polarity). In addition a conductor-to-conductor short must occur between another two specific conductors of the power cable, in order to bypass the open or close contactor. Furthermore, the power fuses for the affected valve must also remain intact, in order to provide an electrical return path. An additional hot short of the opposite polarity would be required to cause valve operation if the power fuses were blown by the faults. The likelihood of all of these faults occurring, without grounding causing fuses of the aggressor, or victim circuits to blow seems very low. Additionally, there are far fewer DC power cables in a plant, and even fewer (if any) continually running DC loads in the plant to serve as aggressors, making the possibility of consequential hot shorts in DC power cables for compound motors as implausible as three phase consequential hot shorts.

Therefore, based upon the specific design characteristics of DC compound motors, a consequential combination of hot shorts capable of opening the valve need not be postulated.

# APPENDIX B.2

# JUSTIFICATION FOR THE ELIMINATION OF MULTIPLE HIGH IMPEDANCE FAULTS

## B.2-1.0 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.2-2.0 INTRODUCTION

### B.2-2.1 Overview

In 1986 the NRC issued Generic Letter 86-10 [1] to provide further guidance and clarification for a broad range of 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[4]. MHIFs are a unique type of common power supply associated circuit, as discussed in Section B.2-2.2 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 protective devices. Confirmation of adequate electrical coordination for safe shutdown power supplies is the primary means of addressing common power supply associated circuits.

[4] A general discussion of associated circuits is contained in Section 2.2 and 3.3.2 of this guidance document.

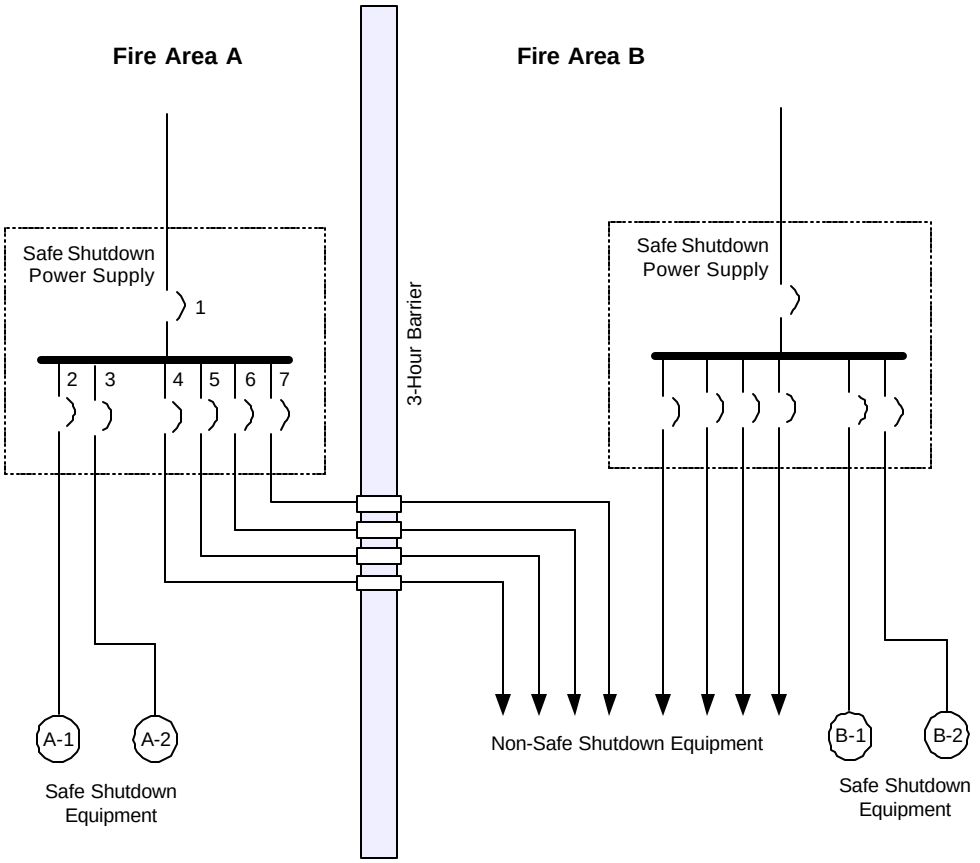
### B.2-2.2 Defining the MHIF Concern

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 entire range of possible fault current. 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 shutdown power supply before the downstream (load-side) protective devices clear individual circuit faults.

Figure B.2-1 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.




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 affect 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.

**Figure B.2-1**
**Example MHIF Sequence**

### B.2-2.3 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.2-2.2 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 probabilistic-based and employ risk-informed arguments. This approach is deemed acceptable within the framework of a deterministic analysis and is not without precedent[5]. However, consistent with risk-informed decision making, consequence of failure shall be addressed by the analysis.

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

## B.2-3.0 ANALYSIS METHOD AND APPROACH

The approach for conducting this analysis is depicted by the flow chart of Figure B.2-2. 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.

[5] 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 hi-lo pressure interfaces).

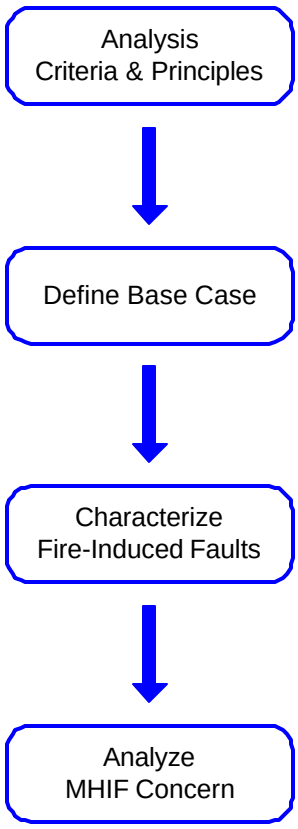



**Figure B.2-2**
**MHIF Analysis Flow Chart**

**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.2-4.0 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. MHIF 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 MHIF. 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, performance, and grounding 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 IEEE 242, or equivalent 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 IEEE 242 recommended practices, they are considered viable and credible source reference 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 possible 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.

- Arcing faults become increasingly more likely as system voltage increases because of the higher voltage gradient and longer creepage distances[6]. 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 is discussed in detail in Section B.2-6.1)

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.2-6.1). 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, yet creepage distances are much larger. 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.

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

## B.2-5.0 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 concern[7]. Achievement of proper selective tripping shall be based on the guidance of IEEE 242, or equivalent criteria.

- For 120 V AC and 125 V DC power supplies, in addition to adequate electrical coordination, a minimum selectivity 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.

- 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:
  - 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.

[7] 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. In general, however, the goal is to not rely on circuit location and routing to demonstrate acceptability, for the reasons discussed in Section B.2-2.2.

- 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. Conductive, non-current carrying components shall be *effectively grounded* as mandated by electrical code requirements.

## B.2-6.0 CHARACTERIZATION OF FAULTS

### B.2-6.1 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.2-6.1.1 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 nature and behavior of fire-induced cable faults.

##### B.2-6.1.1.1 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 kO – 1,000 O. 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 kO down to 600 O. Note that at 600 O 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 phase typically occurs within seconds.

Figures B.2-3 and B.2-4 show current and fault resistance for a typical set of cables driven to failure.

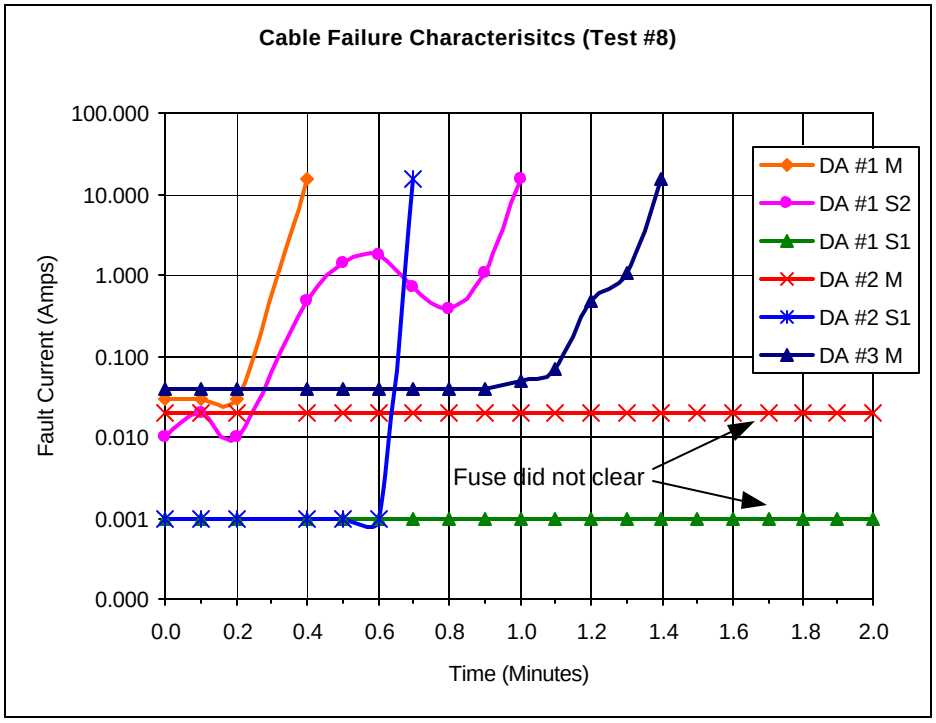



**Figure B.2-3**
**Fault Current for Fire-Induced Cable Failure**

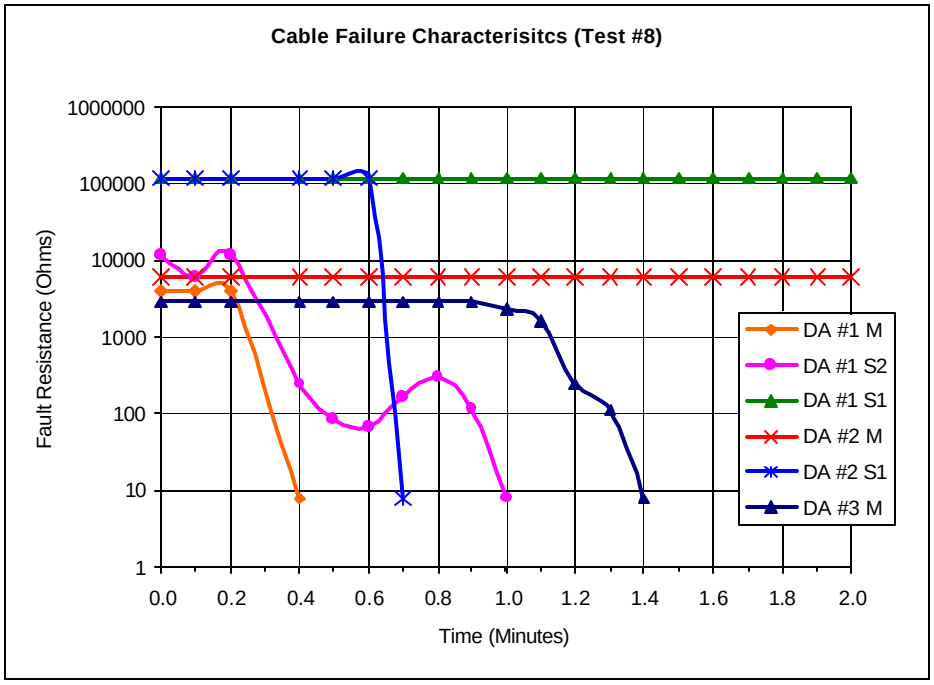



**Figure B.2-4**
**Fault Resistance for Fire-Induced Cable Failure**

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 predicable 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 able to produce sufficient fault current to ensure the protective devices operate predictable.

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. 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.2-6.1.1.2 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.2-1. 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.2-1**

**Fault Clearing Time**

| | Time to Clear Fault (min) | | |
|---|---|---|---|
| Current Threshold | 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 quicker than thermoplastic cable.

### B.2-6.1.1.3 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.2-2.

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.2-2**
**Probability of Clearing Faults within a Specified Time**

| | Percentage of Faults Cleared | | |
|---|---|---|---|
| Time (min) | 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.2-5 and B.2-6 graphically illustrate the data contained in Table B.2-2.

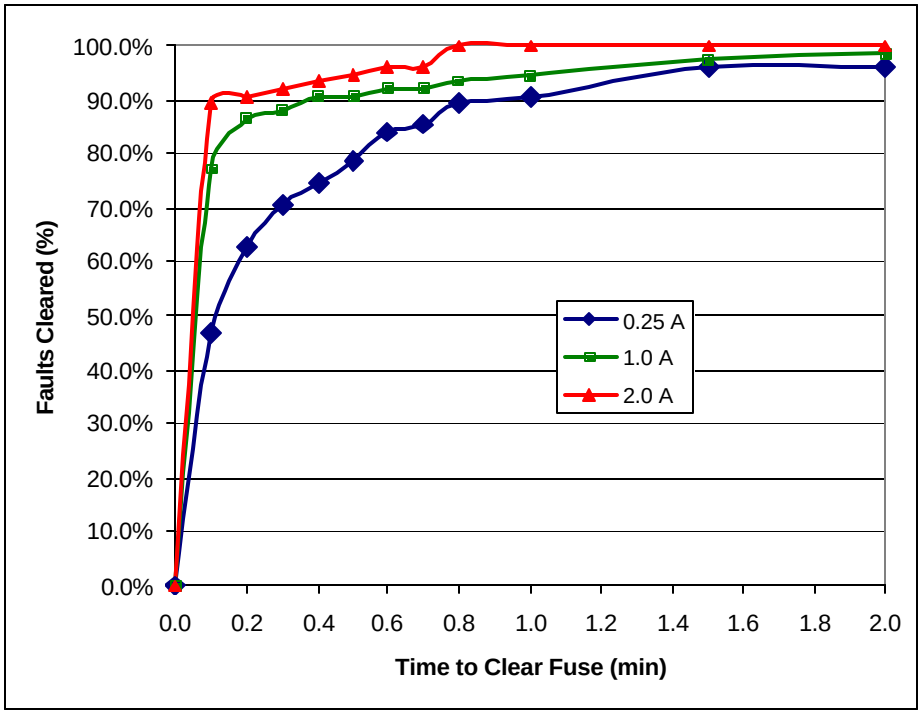



**Figure B.2-5**
**Percent Faults Cleared for Specified Time – Thermoset Cable**

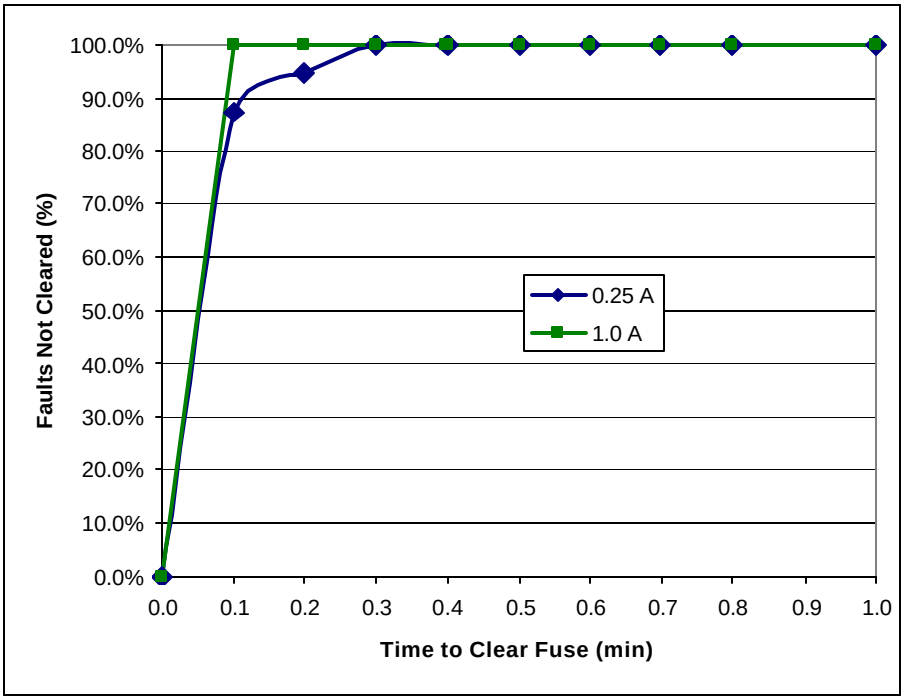



**Figure B.2-6**
**Percent Faults Cleared for Specified Time – Thermoplastic Cable**

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.2-5 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 were 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.2-6.1.1.3 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 thermoset cable data is included in the calculation since is 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:

$$P_l = 1 - \frac{x}{n} \quad \pm \quad z\sqrt{\left(\frac{1}{n}\right) x \left(\frac{x}{n}\right) x \left(1 - \frac{x}{n}\right)}$$

*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.2-3 shows the calculated 95% confidence factors and Table B.2-4 shows the 95% lower confidence limit values for the dataset.

**Table B.2-3**
**Binomial Distribution 95% Confidence Factors**

| | Binomial Distribution 95% Confidence Factors | | |
|---|---|---|---|
| Time (min) | 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.2-4**
**Fault Clearing Time 95% Lower Confidence Limit**

| | 95% Lower Confidence Limit | | |
|---|---|---|---|
| Time (min) | 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.2-7 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.

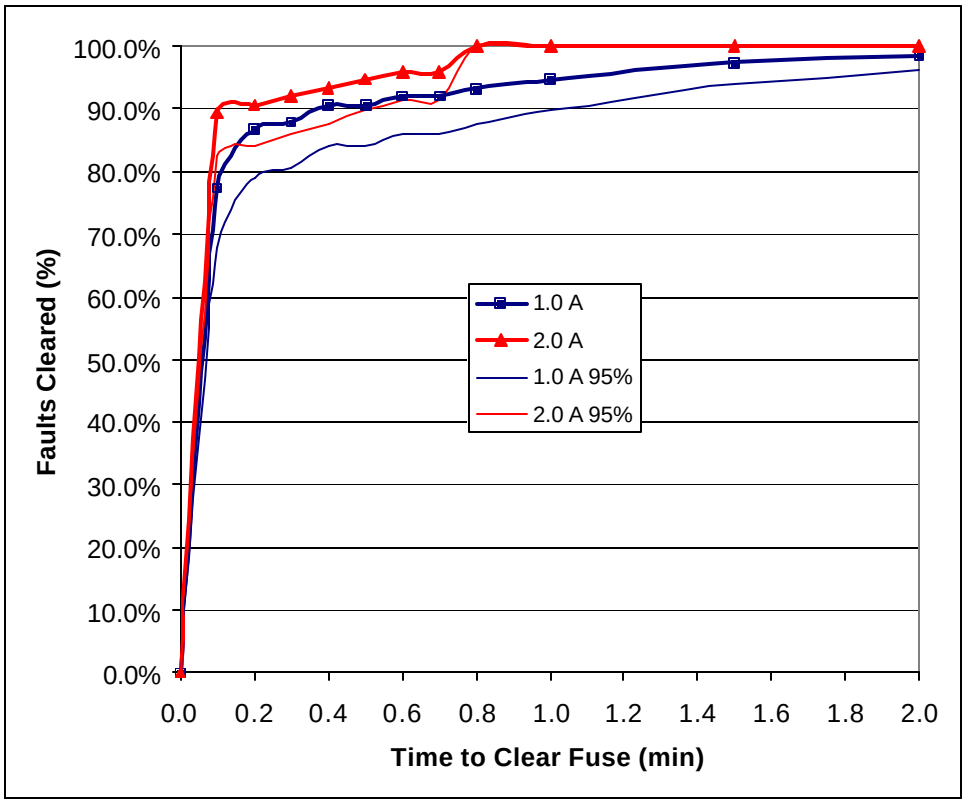



**Figure B.2-7**
**Probability of Clearing Fault within Specified Time**
**with 95% Uncertainty Bound Applied**

### B.2-6.1.1.5 Leakage Current for Non-Failures

The data presented in Sections B.2-6.1.1.2 and B.2-6.1.1.3 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 O. No cases existed in which the failure progresses to the cascade point and did not ultimately fully fail.

### B.2-6.1.2 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 kO to 1,000 O 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.2-8.

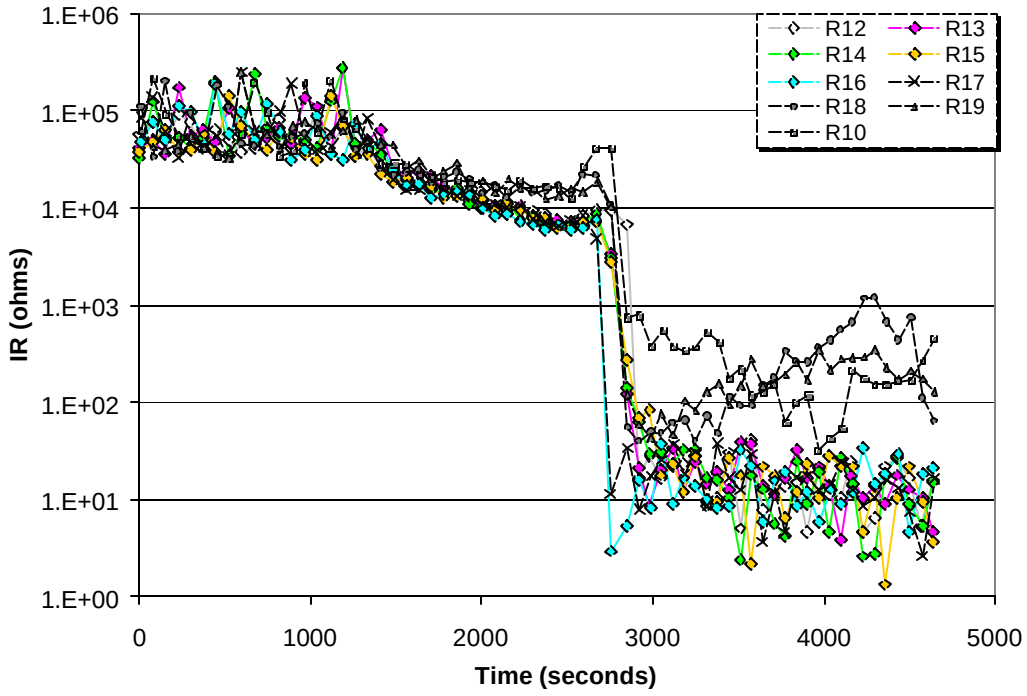



**Figure B.2-8**
**Insulation Resistance Values for Typical Test Series**
***(Courtesy of USNRC and Sandia National Laboratories)***

### B.2-6.2 Characterization of Arcing Faults

As discussed in Section B.2-4.0, 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.2-6.2.1 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 which escalates into an arcing fault
- Surface conduction due to dust, moisture, or other contaminates 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.2-6.2.2 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 wide-spread 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.2-6.2.3 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 re-ignites when instantaneous voltage reaches some threshold value. A key relationship exists between the re-ignition, or re-strike voltage, and the level of fault current. The lower the re-ignition voltage the higher the fault current. As re-ignition 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 occur very seldom.

- The fault current associated with arcing faults increases as a percentage of the bolted fault current as system voltage increases. This characteristic is due 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.2-6.2.4 Arc Fault Current

The current waveshape consists of non-continuous alternating pulses, with each pulse lasting about ¼ - ¾ of a cycle. The arc is extinguished each half cycle and re-ignited in the succeeding half cycle as discussed in Section B.2-6.2.3 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.2-6.2.3 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.2-6.2.5 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.2-7.0 ANALYSIS OF MHIFS

This section analyzes the MHIF concern within the framework of knowledge about fire-induced fault behavior developed in Section B.2-6.0. Our 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.2-7.1 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.2-6.2. 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.2-6.2.4, 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 IEEE 242 (or equivalent) 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 100s of amps and not 1,000s 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:

  Volume Vaporized = (140 x 2.00 x 1/20) / 50 = 0.4515 in3 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. 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.2-7.2 480 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.2-6.2. 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.2-6.2.4. 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 IEEE 242 (or equivalent) 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:

  Volume Vaporized = (100 x 1.90 x 1/20) / 50 = 0.190 in3 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 wide spread 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.2-7.3 120 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 cable faults on 120 V systems behave fundamentally different than 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 re-ignition 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.2-6.1. 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.2-6.1. 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. This phenomenon was observed consistently in all the EPRI/NEI test data and NRC/SNL data, with the exception of instrument circuits[8], which are not within the scope of this analysis. The transition region at which the cascading effect begins appears to range from approximately 10 kO to 1,000 O. 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 O 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.

[8] 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 O 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 determinate 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 triggered 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.2-7.4 125 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.2-6.0 applies 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 is 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 is limited to AC power systems.

### B.2-7.5 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.

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 shots, 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 most all safe shutdown power supplies require some local action for alternative shutdown or spurious actuation 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.

This analysis strives to maintain consistency with existing regulatory positions. Since the stated precedent for the analytical approach (risk-informed arguments for deterministic analysis) is the NRC's low-likelihood argument for three-phase AC hot shorts and proper polarity DC shorts (Generic Letter 86-10, Question 5.3.1), this analysis shall impose the same stipulation for hi/lo pressure interfaces:

> The MHIF failure mode should be considered in assessing the acceptability of safe shutdown power supplies in which de-energization of the power supply would directly result in failure of a hi/lo pressure interface boundary.

This restriction should not prove limiting in that hi/lo pressure interface components are most always designed to fail safe in the "closed" or "isolated" state.

## B.2-8.0 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 have 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.

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 applied under the following conditions:

- The power supply conforms to the *Base Case* requirements
- The power supply will not cause a direct failure of a hi/lo pressure interface boundary if de-energized

## B.2-9.0 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.1.0 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.2.0 INTRODUCTION

Appendix R analyses must evaluate the potential for spurious actuations that may adversely affect the ability to achieve and maintain safe shutdown. A subset of components considered for spurious actuation involves Reactor Coolant Pressure Boundary (RCPB) components whose spurious operation can lead to an unacceptable loss of RPV/RCS inventory via an Interfacing System LOCA. Because an Interfacing System LOCA 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.

## C.3.0 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 re-iterates:

> *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. However, if the spurious opening of RCS boundary valves cannot result in a pipe rupture (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., RHR, DHR, 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. Furthermore, GL 81-12 specifically applied to Alternative/Dedicated Shutdown capability. The application of High/Low criteria to redundant shutdown capability has also been the result of conservative interpretations by licensees and the NRC.

Based on the above guidance, the following criteria 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 on the downstream piping, an interfacing LOCA (i.e., pipe rupture in the low pressure piping).*

## C.4.0 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. Two types of circuit failures are discussed as requiring further evaluation for cases involving high/low pressure interfaces. Appendix B-1 provides justification for eliminating these circuit failures from the analysis since they are not credible. The first is the spurious energization of a three-phase AC circuit by postulating a hot short on each of the three phases. The second is 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.5.0 FIRE AREA ASSESSMENT OF HIGH/LOW PRESSURE INTERFACES:

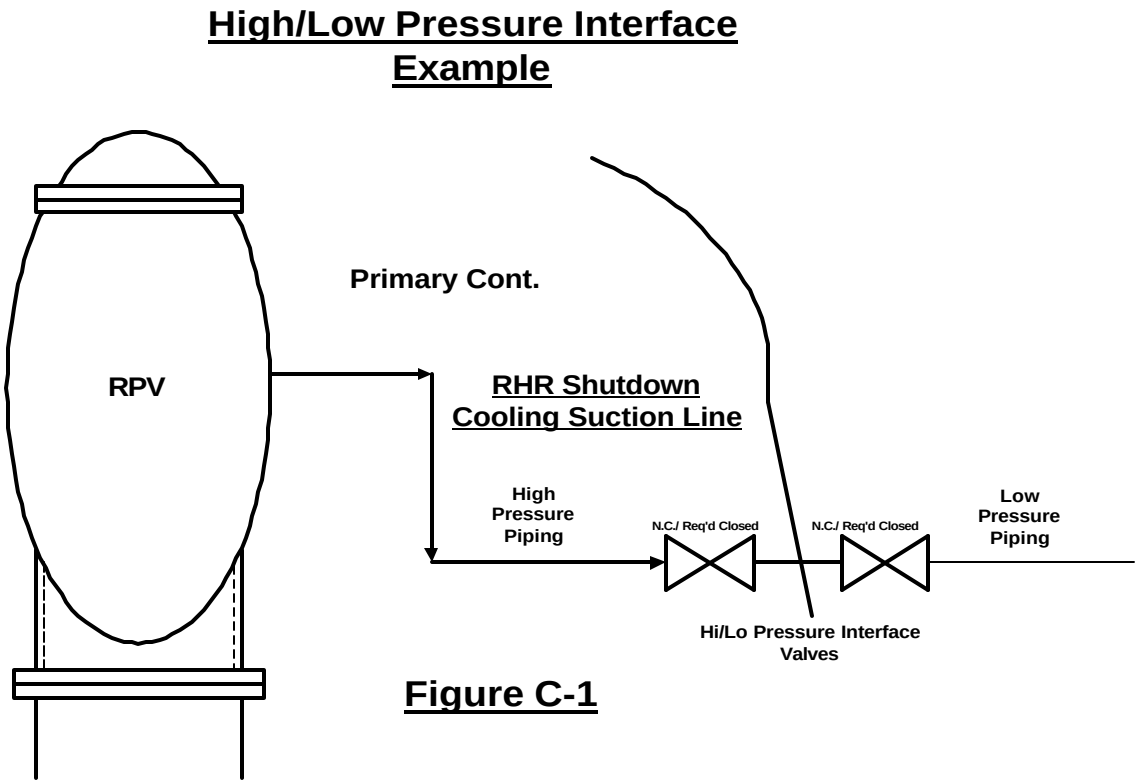



**Figure C-1 Discussion for High/Low Pressure Interface Example -**

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 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.

## C.6.0 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.1.0 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.2.0 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 either "redundant" or "Alternative/Dedicated" shutdown capability, and do not form the basis for determining which capability is being utilized.

"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. 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 for feasibility with respect to manpower, timing, lighting and tenability (accessibility) to ensure that an unrecoverable condition does not occur.

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 of 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 includes 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 their 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.3.0 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.4.0 describes the regulatory requirements for Alternative and Dedicated Shutdown. Section D.5.0 itemizes the differences in shutdown methodology between Alternative/Dedicated Shutdown and those supplied in the body of this document for Redundant Shutdown. Section D.6.0 recommends additional operator actions that should be considered for use on a plant unique basis for fires requiring Control Room evacuation.

## D.3.0 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 extremely small. The worst case expected fire for a Control Room would be one that is contained to 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. While the fire is being extinguished, 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 shutdown the unit from an emergency control station(s). The size and intensity of the exposure fire necessary to cause this damage is not determined, but is 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. In addition, concurrent with

the Control Room fire are spurious actuations that are postulated to occur one at a time. The analysis must consider the effects of each potential spurious actuation 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, unprotected circuits in a given fire area are assumed to be 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 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 HVAC systems for the 72 hour fire coping period.

### D.4.0 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[2], 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 2 - 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" 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 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 standby[3] conditions for a PWR (hot shutdown[3] 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.*

*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 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 uncovery (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 goals.

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 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 plants, the areas where "Alternative/Dedicated" Shutdown is specified are required to have area-wide suppression and detection.

Additional guidance regarding the requirements for suppression and detection in rooms or fire zones relying on Alternative 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.l requires one train of hot shutdown systems be free of fire damage and damage to cold shutdown systems be limited.* [As clarified in Section 5 of this document, the term free of fire damage allows for the use of operator actions to complete required safe shutdown functions. Repairs to equipment required for cold shutdown are also allowed.]

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, 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.]

*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.l 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 Control Room fire that ultimately requires evacuation. During a fire in the Control Room, 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 Control Room fire, however, could cause damage that affects the operator's ability to use all systems available for controlling the unit. As described in Appendix B, the level of damage is not expected to be such that shutdown from the Control Room is impossible. However, in the unlikely event that Control Room evacuation is required, the response to question 5.3.10 provides a bounding plant transient which describes the expected worse 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 Control Room 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 actuation may occur as a result of the fire and this spurious actuation cannot adversely impact the safe shutdown capability. This condition was specified as a part of the Control Room fire design basis because there is some potential for a spurious actuation to occur due to the high concentration of equipment controls within the Control Room. The specific worst-case single spurious actuation, however, was not defined. The requirement for addressing a worst-case spurious signal is met by identifying any spurious actuation 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 actuation 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.

- 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 actuation of two redundant valves in any high-low pressure interface line. Preventing the spurious actuation of two redundant valves in a high-low pressure interface during a control room evacuation can be important because the systems available during this scenario may not be specifically designed to mitigate the effects of a LOCA. By imposing this condition, it eliminates the need to require additional systems to be installed on the emergency control station(s) with the capability to mitigate the effects of an interfacing-system LOCA.

If the required safe shutdown path for Control Room evacuation has the capability to perform all of the required safe shutdown functions and meet the requirements of the response to question 5.3.10, there is an adequate level of safety for this unlikely event.

Because of its specialized nature, the "Alternative/Dedicated" Shutdown capability needs to be specifically directed by plant procedure(s). In many cases, special tools and equipment are also specified and must be readily available, dedicated for this use and administratively controlled for periodic inventory.

### D.5.0 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 must be physically and electrically independent of the area where the fire has occurred. Isolation transfer switches and redundant fusing unaffected by the fire or electrical and physical isolation and manual manipulation of equipment must be provided for Hot Shutdown equipment. 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, as is the case in all other fire areas, potential spurious operations are assumed to occur one-at-a-time. Typically, Alternative/Dedicated circuit designs provide isolation/transfer switches, for safe shutdown equipment circuits, that when actuated will remove faults/spurious actuations 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 actuation of the transfer switch is considered to be an adequate mitigating action. 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 it's 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 actions need to be evaluated for feasibility with respect to manpower availability, timing, lighting, communication and tenability (accessibility) to ensure that an unrecoverable condition does not occur.

- Actuation of an isolation transfer switch is an acceptable technique for mitigating the effects of a potential spurious operation of the equipment controlled by the transfer switch.

- Cold shutdown must be achievable within 72 hours.

- Areas where Alternative/Dedicated Shutdown is credited must have fixed (automatic) suppression and detection.

## D.6.0 ADDITIONAL OPERATOR ACTIONS RECOMMENDED FOR CONTROL ROOM EVACUATION

Although not credited without prior NRC approval, additional operator actions could be useful, if included in the plant procedures for Control Room Evacuation, in helping to minimize the impact of the effects of a fire on the ability to safely shutdown the unit. 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, with NRC prior approval, include these in the governing procedures.

The following actions should be included 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) and minimize the potential of an overcooling event (PWRs) and conserves 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 people 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 to protect the RCP seals.

## D.7.0 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

# MANUAL ACTIONS AND REPAIRS

## E.1.0 PURPOSE

This appendix provides guidance regarding the use of manual actions and repairs to equipment required for post-fire safe shutdown.

## E.2.0 INTRODUCTION

Manual actions may involve manual control, local control or manual operation of equipment. Manual actions on equipment for the purpose of performing its required safe shutdown function is allowed under the definition of "free of fire damage." Repairs may be performed to equipment required for cold shutdown. This Appendix provides the criteria to assure that the reliance on 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.

## E.3.0 RELIANCE ON MANUAL ACTIONS VS. AUTOMATIC OPERATION OF EQUIPMENT

Automatic function circuitry is a design feature provided to mitigate or limit the consequences of one or more design basis accidents. Section I (Introduction and Scope) of Appendix R states the following:

*When considering the effects of fire, those systems associated with achieving and maintaining safe shutdown conditions assume major importance to safety because damage to them can lead to core damage resulting from loss of coolant through boil-off.*

The post fire safe shutdown analyses provide assurance that fire damage will not result in a condition more severe than boil-off, and that manual actions can be performed in a time frame sufficient to restore level prior to the onset of core damage. Analysis shows that fuel damage will not rapidly occur, since boil-off is a gradually progressing event. Operator training and procedures assure that the necessary system alignment(s) are capable of being made in the times required to prevent such occurrence. Thus manual actions are equivalent in mitigation capability to automatic operation.

## E.4.0 DIFFERENTIATING BETWEEN MANUAL ACTIONS AND REPAIRS

The fundamental difference between 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 a manual action or a repair, since the same considerations apply.

## E.5.0 DEFINITIONS

Manual actions include the following:

**Emergency Control Station:** An emergency control station includes the remote shutdown panel(s), local starters, electrical distribution panels, MOV handwheels and other equipment locations designed for operator use or monitoring.

**Free of Fire Damage:** Achieved when the structure, system or component under consideration is capable of performing its intended function during and after the postulated fire, as needed. It may perform this function automatically, by remote control (which includes manual operations and/or remote manual operations) or by local operation.

**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.

**Manual Operation**: Operation of safe shutdown equipment on the required safe shutdown path using the control room control devices (e.g., switches) in the event that automatic control of the equipment is either inhibited based on plant procedures or unable to function as a result of fire-induced damage.

**Local Operation**: Operation of safe shutdown equipment on the required safe shutdown path by an operator when automatic, remote manual or manual operation are no longer available (e.g. opening of a motor operated valve using the hand wheel).

**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 of the control room.

**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 in order 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.

## E.6.0 CRITERIA

In order to credit the use of manual actions or repairs to achieve post-fire safe shutdown, certain criteria must be met. Due to the similarity between manual actions and repairs from the operational perspective, most of these criteria 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 manual actions and repairs**

- There shall be sufficient time to travel to each action location and perform the action. 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 operator action time. For example, manual actions to lock out charging pumps or close PORV block valves may be considered feasible.

- There shall be a sufficient number of plant operators to perform all of the required actions in the times required, based on the minimum shift staffing. The use of operators 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.

- The action location shall be accessible. 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. 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 that confirms that an action has achieved its objective. This indication is not required to be a direct reading instrument and may be a system change (level, pressure, flow, etc.).

- Any tools, equipment or keys required for the action shall be available and accessible. This includes consideration of SCBA and personnel protective equipment if required.

- There shall be provisions for communications to allow coordination of actions with the Main Control Room or the remote shutdown facility, if required.

- Guidance (e.g., procedures, pre-fire plan, etc.) should be provided to alert the operator as to when manual actions may be required in response to potential fire damage. The guidance may be prescriptive or symptomatic. Specific procedures are required for activities not addressed in existing procedures (normal, abnormal, EOPs) for operator actions and repairs as a result of fire induced failures that cannot be readily diagnosed using fire protected information to the operator. Typically, plant operators should be capable of performing manual actions without detailed instructions. Detailed instructions should be readily available, if required. Procedures should likewise be provided to the operator as to when to perform repairs in response to potential fire damage. The procedures shall provide the level of detail required to enable plant personnel to perform the task.

**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, I&C technicians, electricians) may be relied upon to perform repairs, provided their availability is consistent with plant emergency response 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 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, manual actions specified as precautionary or confirmatory back up 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.

## E.7.0 REFERENCES

E.7.1 10 CFR 50 Appendix R Fire protection for Operating Nuclear Power Plants

# APPENDIX F

# SUPPLEMENTAL SELECTION GUIDANCE (DISCRETIONARY)

## F-1.0 INTRODUCTION

This appendix provides potential methods that can be used to select additional circuit failure combinations. These methods were used during the pilot evaluation process on a limited basis to identify a few combinations for each pilot plant. For example, in the McGuire pilot process, 4 circuit failure combinations were identified using the PRA review and 4 were identified using a Logic Diagram Review. The methodology below is one of several ways to identify component combinations for review.

Because plants have previously conducted vulnerability evluations, and because the pilot evaluations of NEI 00-01 did not indicate a significant benefit from performing this supplemental process, this supplemental selection is an optional part of the NEI-00-01 process. It is provided for the use of any plant wanting to determine the general importance of circuit failures for their plant.

## F-2.0 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. Only one component at a time needs to be considered for IN 92-18 evaluations.

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 on P&IDs or Safe Shutdown Logic Diagrams (if available) or both. The review should focus in on "pinch points" where the system function or 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 PRA input may be helpful for determining potentially unreliable equipment or manual/operator actions.

Some pre-knowledge of component cable routing is useful in this review. This would save time in the process by eliminating component combinations where cables are known to not be located in the same fire area. Without some cable routing knowledge, an identified component combination would be analyzed through several steps of NEI-00-01 prior to screening, which may require detailed cable routing.

The results of the PI&D or Logic diagram review would be a list of potentially important component combinations to be treated with the NEI-00-01 methodology. Since the PRA scope and Fire Protection SSD scope are different, the SSD review may provide potential combinations that have not been included in the 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 PRA (because of a high level of redundancy). The final list of identified component combinations should be combined with any PRA combinations (from the PRA review below) for a final list for analysis.

### F.3.0 PRA REVIEW

The 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 PRA scope includes additional equipment that are 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 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 cutsets. For example, by setting all of the MOV spurious

operation events to 1.0 and resorting, the top cutsets may not include potentially important component combinations for MOV cables.

Generally, the significance of each combination can not 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, with two similar cutsets, one with two spurious operations required, and one with the same two and one additional spurious operation required can be 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 can not 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. A review of the plants Fire 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 4 of this document.

The level and amount of model manipulation can range from a single re-solution of the model, to many re-solutions 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 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 to lead 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.

Pre-knowledge of general component cable location is helpful when reviewing PRA results and identifying the component combinations. The top cutset may contain two components whose cables are not located in the same fire area or zones, making this combination unimportant. More commonly, you may see two components whose cables are located near each other only in the cable spreading room and control room. Selection and analysis of a group of component combinations with no common fire areas damaging all components would result in wasted effort. The pilot applications of NEI-00-01 used pre-knowledge of component cable routing to determine the recommended combinations for review.

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 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, cutset 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.4.0 Selection of Potentially Important Component Combinations

Based on the pilot 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 these combinations is not possible. The final selection of component combinations for analysis needs to account for various factors affecting the final expected risk for the combinations, including:

- Pre-knowledge of component cable locations, if possible

- Expected spurious operation probability, including the combined frequency for multiple components. For example, it can easily be shown that 3 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 bgic diagram review should provide a comprehensive list of potentially important component combinations.