GUIDANCE FOR POST-FIRE SAFE SHUTDOWN ANALYSIS

1 INTRODUCTION

Difficulties in interpreting NRC requirements of 10 CFR 50.48 (reference 5.4.1) and 10 CFR 50 Appendix R (reference 5.4.3), and regulatory guidance such as US NRC Branch Technical Position 9.5-1 (reference 5.4.4) and Generic Letter 86-10 (reference 5.1.10), in combination with the numerous variations in plant design, have resulted in wide variation in plant-specific approaches to post-fire safe shutdown analysis.

Some of these approaches are based on long-held industry interpretations of the foregoing NRC regulations and guidance. In an NRC letter to NEI in early March 1997 (reference 5.4.30) and the industry response (reference 5.4.31), it became evident that industry and NRC staff interpretations differ significantly.

With a greater emphasis being placed on risk-informed methods, such as those used in the on-line maintenance and outage risk management areas, industry proposed a risk-informed approach for resolving the circuit failures issues. That approach is detailed in this guideline by integrating the deterministic approach documented in a BWR Owners Group topical report (reference 5.4.32) with circuit failure characterization and probabilistic elements developed by the NEI Circuit Failures Issue Task Force.

The structure of this guideline is very similar to that of the BWR Owners Group guideline just described, with several key differences described below:

- Draft information with regard to PWR systems and PWR circuit analysis topics is reflected in the body of this document (Sections 1 through 5)

- To more clearly show the applicability of NEI 00-01 to all plants, most references to BWRs have been removed except where BWR-specific information is provided

- Appendix B (the BWROG risk significance review of Information Notice 92-18) will be revised to reflect updated information from the NEI circuit failure characterization activities

- Appendix C (The BWROG discussion of high/low pressure interfaces) will be revised to reflect updated information from the NEI/EPRI circuit failure characterization activities

- Appendix E (the BWROG discussion of multiple high impedance faults) be revised to reflect updated information from the NEI/EPRI circuit failure characterization activities

- Appendix G (the BWROG discussion of combined equipment impacts) will be revised to describe a generic screening approach which will be used to identify any additional combined equipment impacts that need to be included into the post-fire

safe shutdown analysis (e.g. items similar to hi/lo pressure interface valves). The approach used to accomplish this will be risk-informed and will rely on information compiled in the IPE's. Through the application of the information in this appendix, the issue of multiple spurious signals and operations will be resolved either by identifying specific combinations of concern or by demonstrating on a generic basis that there are none with a sufficient likelihood of occurrence that would require their consideration.]

- A new Appendix H will be added which summarizes the conclusions from the NEI/EPRI circuit failure characterization work

- A new Appendix I was added which provides the industry method for determining the safety significance of fire-induced circuit failures

The reader should note that this document is a work in progress which will be finalized as further information is developed in each area.

1.1 PURPOSE

This document provides guidance on performing a post-fire safe shutdown analysis for any operating nuclear plant. Post-fire safe shutdown is one part of each plant's overall defense-in-depth fire protection program. Because of the uncertainties associated with the actual behavior of fires in a nuclear power plant, each of the echelons of the defense-in-depth fire protection program is important in assuring that the plant is safe from the adverse effects of fires. The methodology provided in this document, when implemented, provides the necessary assurance that post-fire safe shutdown capability, when viewed in the context of an effective overall fire protection program, will be preserved.

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 criteria are satisfied for a single fire in any plant fire area:

> That one safe shutdown path required to achieve and maintain hot shutdown is free of fire damage.
>
> That repairs to systems and equipment required to achieve and maintain cold shutdown can be accomplished within the required time frame.
>
> That any manual operator actions required to support achieving either hot or cold shutdown are identified and can be implemented within the time required.

The methodology outlined within this document assures that these criteria are

satisfied. This methodology provides an approach that:

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. These techniques include a method for licensees to determine the safety significance of concurrent spurious actuations, and potential fire-induced circuit failure modes described in NRC Information Notice 92-18 (reference 5.3.37). If the user determines that additional measures are needed to prevent or mitigate the consequences of the spurious actuations, this method can also be used to ensure the cost-effectiveness of these measures.

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. Therefore, each plant is responsible for comparing this generic guidance with plant-specific commitments in determining the applicability of this guidance.

Using this guidance document and the methodology contained within it to perform post-fire safe shutdown analysis will result in an analysis that meets the regulatory requirements, provides an acceptable level of fire risk and results in a safe plant design. By using this guidance document, industry believes that a comprehensive and understandable set of criteria has been provided for performing an adequate and appropriate post-fire safe shutdown analysis which satisfies 10 CFR50, Appendix R Sections III.G and III.L. This method, including the documentation of its use and any additional measures taken to address its results, constitute an acceptable method for resolving these circuit failure issues

This document integrates the requirements and interpretations related to post-fire safe shutdown into a single location, and provides response to the NRC-Industry issues related to fire-induced circuit failures. These responses are contained in the Appendices to this document. The information in the Appendices is provided in an effort to resolve the most recent circuit failures issues related to post-fire safe shutdown analyses.

By issuing this guidance document, NEI believes that a comprehensive and understandable criteria has been provided for performing an adequate and appropriate post-fire safe shutdown analysis which satisfies the intent of 10 CFR 50, Appendix R, Sections III.G and III.L. NEI also believes that the approach identified in Appendix I will resolve the issue related to consideration of multiple spurious actuations in the post-fire safe shutdown analysis.

1.2 BACKGROUND

The uncertainty associated with the behavior of actual plant fires can be substantiated by reviewing past fire events. 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. 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 reoccurrence of a fire event of the severity experienced at Brown's Ferry.

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. Complete clarity of these requirements is still a concern throughout the industry.

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 size would be a fire that is contained to a single electrical panel or a localized portion of one room or area. 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, it is recognized that the consequences of an event that damages plant equipment important to safe shutdown could be significant. The Brown's Ferry fire was an event that did result 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. A description of the improvements made in the fire protection design of Nuclear Power Plants in response to the Brown's Ferry fire event is provided in Appendix A to this document.

In addition to the changes made in the fire protection design features of the plants, increased attention has also been placed on identifying those systems and equipment important to the post-fire safe shutdown of the unit. 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, a safe plant design is achieved. When these aspects of post-fire safe shutdown design are viewed in combination with the changes made in the design of the plant fire protection features in response to the Brown's Ferry fire, this conclusion regarding plant safety is even further solidified.

This document provides a methodology for identifying systems and equipment important to post-fire safe shutdown, for evaluating the effects of fire damage on these systems and

equipment and for mitigating the effects of any impacts from the fire on these systems and equipment.

A basic assumption of this methodology is that there will be fire damage to systems and equipment located within a common fire area. The size and intensity of the exposure fire necessary to cause this damage is not determined. Rather, it 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 or the presence of automatic or manual suppression and detection capability. It is also postulated to damage all cables and equipment located 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 extremely conservative assumptions regarding fire damage that this methodology document begins. The methodology progresses by providing guidance on selecting systems and equipment important to 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 post-fire safe shutdown analysis, 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 only conservative 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 post-fire safe shutdown analysis is depicted in Figure 1-1.

1.3.1 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. power, ventilation) and process monitoring capability (e.g. reactor level, pressure indication) are also required.

In addition, it must be assured 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. The spurious operations that present a potential concern for the safe shutdown functions described above are: (1) those that can cause a loss of inventory in excess of make up capability from the reactor; (2) those that can cause a flow diversion or a flow blockage in the safe shutdown systems being used to accomplish the inventory control function; (3) those that can cause a flow diversion or a flow blockage in the safe shutdown systems being used to accomplish the decay heat removal function.

Although an inadvertent reactor vessel overfill condition is not a safe shutdown function listed above, it has been identified as a NRC concern in the past. 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 Safe Shutdown System and Path Identification

Using the safe shutdown functions described above, a system or combination of systems with the ability to perform each of these shutdown functions is identified. These systems are then combined into safe shutdown paths. By assuring the availability of a safe shutdown path in each fire area in the event of a fire in that fire area, safe shutdown is assured. By assuring safe shutdown, the stated goal for post-fire safe shutdown is assured.

1.3.3 Safe Shutdown Equipment Identification

Using the P&IDs for the mechanical systems comprising each safe shutdown path, the mechanical equipment required for the operation of the system is identified. The equipment whose spurious operation could affect the performance of the safe shutdown systems must also be identified. Equipment that is required for the operation of a safe shutdown system for a particular safe shutdown path is related to that path.

The equipment that could spuriously operate and result in a flow blockage or flow diversion is also identified by a review of the P&IDs. Similarly, this equipment is related to the particular safe shutdown path that it can affect.

The equipment that can result in a loss of reactor inventory in excess of make up capability is identified by a review of P&IDs for the systems physically connected to the reactor vessel. In performing this review, a special class of valves known as “Hi/Lo Pressure Interfaces” are identified. Refer to Appendix C to this document 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.

By assuring the availability of the equipment required for the safe shutdown systems on one safe shutdown path, safe shutdown is assured. By assuring safe shutdown, the stated goal for post-fire safe shutdown is assured.

1.3.4 Safe Shutdown Cable Identification

Using the electrical schematic drawings for the equipment identified above, the cables required for the operation of the safe shutdown equipment can be identified. In this step, all cables required for the equipment to function must be identified. 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.

In reviewing the electrical schematics for the equipment, the safe shutdown equipment from the electrical distribution system (EDS) is identified. The EDS equipment (bus) is then related to the safe shutdown path associated with the equipment that it powers. All up stream busses must also be 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.

By assuring the availability of the cables required for the safe shutdown equipment on one safe shutdown path, safe shutdown is assured. By assuring safe shutdown, the stated goal for post-fire safe shutdown is assured.

1.3.5 Safe Shutdown Circuit Analysis

Through the process described above, safe shutdown paths are identified. The equipment and cables required for the operation of each safe shutdown path are also identified and related to the safe shutdown path. Using information on the physical routing of these cables and the physical locations of all safe shutdown equipment, the equipment and cable impacts for each safe shutdown path in each plant fire area can be determined. Based on the number and types of impacts to these paths, each fire area can be assigned a required safe shutdown path(s). Any cables related to the required safe shutdown path in a given fire area can initially be assumed to cause the component to fail in the worst case position (i.e. if the safe shutdown position of a valve is closed, the valve will be assumed to be open in the fire area in which a required cable is routed) .

If necessary, a detailed analysis of the cable may be evaluated for the specific effect of the fire on that safe shutdown path. 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. If any of these circuit failure modes impacts the ability of the equipment to function, then the safe shutdown equipment is considered to be impacted. Equipment impacts must be assessed in terms of their effect on the safe shutdown system, the safe shutdown path, the safe shutdown functions and the goal for post-fire safe shutdown.

1.3.6 Safe Shutdown Equipment Impacts

Using the process described above, the potential impacts to safe shutdown equipment, systems, paths, and functions relied upon for each fire area are identified. The effects on safe shutdown for each safe shutdown equipment impacted by the fire must be mitigated.

By identifying impacts to all of the equipment on the required safe shutdown path(s) and providing a means of mitigating the effects of each impact, safe shutdown is assured. By assuring safe shutdown, the stated goal for post-fire safe shutdown is assured.

The process of identifying and mitigating impacts to the required safe shutdown path(s) described above is explained in more detail throughout this document. The next section of this document provides an overview of where specific information related to each step in the process can be found within the document.

1.4 OVERVIEW OF GUIDANCE DOCUMENT

This document provides a comprehensive review of the criteria and considerations for completing a post-fire safe shutdown analysis. It establishes references to NRC regulations and generic letters in support of the methodology defined for safe shutdown analysis. Verbatim wording that is extracted from the regulatory documents is shown as italicized in this document. The criteria and methodology provided in this document ensures the ability to satisfy the required safe shutdown functions of 10CFR50, Appendix R and assures the ability to achieve and maintain safe shutdown in the event of a single fire in any plant fire area.

Section 2.0 of this document provides a discussion of the regulatory requirements and guidance applicable to post-fire safe shutdown analysis. The shutdown requirements applicable to Alternative/Dedicated Shutdown are contained in Appendix D to this document.

Section 3.0 of this document outlines the methodology to be used for post-fire safe shutdown analysis. The methodology contained in Section 3.0 is considered to be a "baseline" methodology. It is presented in a straight-forward manner and provides a methodology for addressing the effects of each potential fire induced impact to safely shutting down a plant that is operating at 100% power. Any specific exceptions to this straightforward methodology or any special topics which are addressed in a manner different from the baseline methodology outlined in Section 3.0 or which require special consideration are discussed in appendices to this document.

Figure 1-2 illustrates the methodology steps outlined in this document for evaluating post-fire safe shutdown. The methodology section of this document discusses the following phases of the analysis:

Safe shutdown system selection and path development (Section 3.1)

This section discusses the process of identifying the safe shutdown systems and combining these into shutdown paths to be defined for each fire area. It also provides a general description of typical safe shutdown systems for BWRs and PWRs and how they support the required shutdown functions. Typical shutdown methods developed within the industry are also described including assumptions and methods considered in defining valid safe shutdown systems.

Safe shutdown equipment selection (Section 3.2)

The section on equipment selection discusses the criteria and method considered in defining valid safe shutdown equipment. Criteria are established for determining the types of equipment to be considered for the safe shutdown analysis and a methodology is provided for selecting equipment for each safe shutdown system and relating these to their appropriate shutdown system and path.

Safe shutdown cable selection (Section 3.3)

The section on cable selection discusses the assumptions and process considered in identifying Appendix R cables (safe shutdown and associated circuits of concern) and establishing their relationship to the affected safe shutdown equipment. Also included is a discussion on the process for locating these cables by fire area for further analysis.

Fire area assessment and compliance strategies (Section 3.4)

This section discusses the process for determining and resolving Appendix R concerns by fire area. It establishes the criteria and assumptions for developing compliance strategies for the cases where circuits of redundant systems are located in the same fire area.

Circuit analysis criteria (Section 3.5)

The section on circuit analysis criteria discusses the various types of circuit failures that should be considered when postulating fire-induced cable failures. Examples are provided for selected circuit failures. The information in this section can be used at various stages in the methodology. It can be used as a part of the initial cable selection process to screen out those circuits and cables that clearly have no potential to impact safe shutdown. It is used most heavily in the fire area assessment stage in identifying the circuits that will impact safe shutdown equipment.

Section 4.0 provides definitions for the terms used in this document. Section 5.0 provides a list of the references used in the development of this document. Figures depicting the process steps for the methodology are provided along with examples of suggested ways to document and organize the results of the post-fire safe shutdown analysis.

Finally, appendices attached to this document address topics requiring special consideration either because they represent adjustments to the baseline criteria, or methods for mitigating the effects of potential circuit failures.

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.

2.1 REGULATORY REQUIREMENTS

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

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. Section III.G.1.b allows for repairs to be performed on safe shutdown equipment used for achieving and maintaining cold shutdown. Appendix F 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 which 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, 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. As discussed in Appendix F to this document, manual operator actions and repairs may also be used for certain equipment required to achieve and maintain post-fire safe shutdown.

However, Section III.G.2 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, deviations and/or 86-10 evaluations supported by 50.59 Safety Determinations may be used to justify configurations that meet the underlying goals of Appendix R, while not meeting certain specific requirements.

In addition, proper utilization of probabilistic risk assessments may determine that the prescriptive separation requirements specified in Section III.G.2 are unnecessary based on the actual plant configuration (i.e. combustible loading, fire initiators, detection/suppression capabilities, etc.)

2.2 REGULATORY GUIDANCE 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.*

2.3 REGULATORY INTERPRETATION ON LOSS OF OFFSITE POWER

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

c) 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 postfire 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.

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 (e.g. additional electric heat loads may affect HVAC strategies.

3 METHODOLOGY

This section discusses a generic methodology and criteria which licensees can use to perform a post-fire safe shutdown analysis that meets the intent of the requirements of Appendix R. 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, these items are not necessary for completion of the required post-fire safe shutdown functions. Thus, these items are not governed by the requirements of Appendix R Section III.G. Therefore, the circuit analysis and fire impact mitigation techniques described in this guidance document are not applicable to fire detection and suppression, communications systems and 8-hour emergency lighting equipment and 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 damages 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 F to this document for the requirements associated with using manual operator actions and repairs to support post-fire safe shutdown.

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. 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 are as follows:

- 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 requires consideration of associated circuits with the potential for spurious operation. 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.

These 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. These considerations are directly related to the stated post-fire safe shutdown goal.

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, App. 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.

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, which could inhibit natural circulation. Therefore, feedwater (either auxilary 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, Exemptions, Deviations or 50.59 Safety Determinations, 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. However, for areas that use alternative shutdown capability, safe shutdown capability must be demonstrated where offsite power is available and where offsite power is not available for 72 hours.

3.1.1.8 Safe shutdown systems can be either safety-related or non 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.

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

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 is credited. The post-fire safe shutdown analysis must only provide the capability to manually scram/trip the reactor. For PWRs, 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

[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 raise pressurizer level/pressure. Manual control of the related pumps is acceptable.

3.1.2.3 Inventory Control

[BWR] Systems selected for the inventory control function should be capable of supplying sufficient reactor coolant, 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 under the assumption that 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.

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. 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 navigate existing 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

PWR

Reactor coolant pressure and temperature (Hot leg / Cold leg)
Pressurizer level
Neutron flux monitoring
Level indication for various tanks
Steam generator level and pressure

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 derived from 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.

DC Distribution System

Typically, the 125VDC distribution system supplies DC control power to various 125VDC control panels including 4.16KV 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 4KV switchgear, 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 and to assure room temperatures remain below those acceptable for performing required operators actions.

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 3-1 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"

3.1.3.2 Identify combinations of systems that satisfy each safe shutdown function

Given the criteria/assumptions defined in sections 3.1.1 and 3.1.2, identify the available combinations of systems capable of achieving the safe shutdown functions of Reactivity Control, Pressure Control Systems, Inventory Control, Decay Heat Removal, Process Monitoring and Support Systems such as Electrical and Cooling Systems. In addition to achieving the required safe shutdown functions, consideration must also be given to 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, additional support systems may be identified and these should also be listed for the appropriate path.

3.1.3.4 Assign shutdown paths to each combination of systems

A path designation should be assigned 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. 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

The following criteria and assumptions may be considered 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. Each licensee should determine which equipment should be included on the Safe Shutdown Equipment List (SSEL). As an option, secondary components could be associated 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 Exposure fire damage to manual valves and piping is not assumed to adversely impact their ability to perform their pressure boundary or safe shutdown function.

3.2.1.3 Manual valves are assumed to be in their normal position as shown on P&IDs or in the plant operating procedures.

3.2.1.4 A check valve that closes in the direction of potential flow diversion is assumed to seat properly with sufficient leak tightness to prevent flow diversion capable of adversely affecting the safe shutdown function.

3.2.1.5 Instruments (e.g., resistance temperature detectors, thermocouples, pressure transmitters, and flow transmitters) are assumed to fail up-scale or down-scale as a result of fire damage. The instrument fluid boundary is assumed to remain undamaged. Sight-glasses and mechanically linked tank-level indicators are not assumed to be damaged by the fire.

3.2.1.6 Equipment that could spuriously operate and impact the performance of equipment on a required safe shutdown path should be identified during the equipment selection phase.

3.2.1.7 Instrument tubing that may cause subsequent effects on instrument readings or signals as a result of fire damage should also be identified. The fire area location of the instrument tubing should be determined and considered 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 3-2 for a flowchart illustrating the various steps involved in selecting safe shutdown equipment. The following methodology may be used 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.

It is recommended that markups and annotations be made to 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 which may spuriously operate and affect system operation.

Review the applicable documentation (e.g. P&IDs, electrical drawings, instrument loop diagrams) to insure 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 such as valves. If additional systems are identified which are necessary for the operation of the safe shutdown system under review, these systems should also be included as systems required for safe shutdown. These new systems should be designated 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, additional equipment may be identified (e.g. electrical distribution system equipment). This additional equipment should also be included 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

Additional equipment related information necessary for performing the post-fire safe shutdown analysis should be collected for the equipment. In order to facilitate the analysis, it is recommended that this data be tabulated 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, additional supporting equipment such as electrical power and interlocked equipment are also identified. As an aid in assessing identified impacts to safe shutdown, the dependency between equipment within each safe shutdown path may be modeled 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.

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(s) 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. Careful consideration should be given to 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.

The following criteria may be considered when selecting cables which 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, the power, control, instrumentation, interlock, and equipment status indication cables related to the equipment need to be investigated. A review of additional schematic diagrams may be required to identify additional cables for interlocked circuits which 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, the screening criteria from Section 3.5 could be applied 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, the cable should be associated with each piece of safe shutdown equipment.

3.3.1.3 In the case of instrument loops, the isolation capabilities of the devices in the loop should be reviewed to determine if faults on non-safe shutdown cables in the loop would be isolated in such a way that the fault would not impact the performance of the safe shutdown instrument function.

3.3.1.4 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) may be screened out 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, the cable supplying power to each safe shutdown and/or required interlock component should be identified. Initially, only the power cables from the immediate upstream power source are identified for these interlocked circuits and components (i.e. the closest power supply, load center or motor control center). A further review of the electrical distribution system is needed 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 to the safe shutdown equipment. This equipment should be added to the safe shutdown equipment list. The power cables for this additional equipment should be evaluated for associated circuits concerns.

3.3.1.6 The automatic initiation logics for the credited post-fire safe shutdown systems is 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 4.16 KV switchgear 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 4.16 KV switchgear would also be associated with the 4.16 KV switchgear.

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. These cables are identified together with the remaining safe shutdown cables required to support control and operation of the equipment. A methodology for analyzing the impact of these cables on post-fire safe shutdown is contained in Section 3.5.2.4 of this document.

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). A methodology for analyzing the impact of these cables on post-fire safe shutdown is contained in Section 3.5.2.5 of this document.

3.3.3 Methodology for Cable Selection and Location

Refer to Figure 3-3 for a flowchart illustrating the various steps involved in selecting the cables necessary for performing a post-fire safe shutdown analysis. The following methodology may be used 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, any circuits whose failure may cause a coordination concern for the bus under evaluation should also be identified.

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

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

In reviewing each control circuit, interlocks will need to be investigated which may lead to additional circuit schemes, cables and equipment. Any cables for interlocked circuits that can affect the equipment will also need to be assigned to the equipment.

While investigating the interlocked circuits, additional equipment or power sources may be discovered. These interlocked equipment or power sources may also need to be included 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 sections 3.3.1 and 3.3.2, identify the cables required to operate or which may result in maloperation of each piece of safe shutdown equipment.

The list of cables potentially affecting each piece of equipment may be tabulated in a relational database including the respective drawing numbers, their revision and any interlocks which 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. The cables need to be related to each piece of equipment, but not necessarily to each supporting secondary component.

If adequate coordination does not exist for a particular circuit, then the power cable should also be related 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, the location of field routed cable may also need to be identified 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 Only one fire in any single fire area is assumed to occur at a time.

3.4.1.2 All unprotected cables and equipment within a fire area may be affected by the fire. This assumption does not imply that the fire instantaneously spreads throughout the fire area, but rather is intended as a conservative assumption to address the fact that, for this analysis, neither the fire size nor the fire intensity is rigorously determined.

3.4.1.3 All cable and equipment impacts affecting the required safe shutdown path in the fire area should be addressed. Each potential impact must be mitigated. 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 Appendix R compliance requires that one train of systems necessary to achieve and maintain Hot Shutdown conditions is free of fire damage (III.G.1.a). When adequate fire area separation does not already exist, one of the following means of separation can be provided for the required safe shutdown path(s):

Separation of cables and equipment and associated 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 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) and they must provide full area coverage.

Enclosure of cable and equipment and associated 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).

Exemptions, deviations and 86-10 Fire Hazards Analysis using 10CFR50.59 safety evaluations may be used to achieve the following mentioned above, depending upon the plant's license requirements. In certain cases, the application of risk insights may demonstrate that the specified prescriptive separation requirements are unnecessary to achieve the post-fire safe shutdown goal.

3.4.1.5 Manual actions may be used to achieve and maintain post-fire safe shutdown conditions. Refer to Appendix F to this document for additional guidance on the use of manual actions as a mitigating technique.

3.4.1.6 Repairs to equipment required to achieve or maintain cold shutdown in support of post-fire shutdown may be used. Refer to Appendix F to this document for additional guidance on the use of repairs as a mitigating technique.

Other equipment may be selected 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.

3.4.1.7 The effects of the fire on the density of the fluid in instrument tubing and any subsequent effects on instrument readings or signals should also be considered in evaluating post-fire safe shutdown capability.

3.4.2 Methodology for Fire Area Assessment

Refer to Figure 3-4 for a flowchart illustrating the various steps involved in performing a fire area assessment. The following methodology may be used 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. This information could be provided 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 path 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 path is 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. Consideration of the circuit failure criteria and the possible mitigating strategies, however, may also influence the selection of the required safe shutdown path in a particular fire area. Support systems should also be reviewed 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, realizing that a subset of a safe shutdown path can accomplish a specific goal that is not achievable by utilizing a single shutdown path. For each of the safe shutdown cables (located in the fire area) associated with the required safe shutdown path in the fire area, an evaluation is performed 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 and, even, 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. Information related to the normal and shutdown positions of equipment may be defined on the safe shutdown equipment list.

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:

Determine the safety significance of the failure (see Appendix I) and take subsequent actions from the remainder of this list if the circuit failures are shown to be safety-significant
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 F for additional guidance)
Perform a repair (Refer to Appendix F for additional guidance)
Identify other equipment capable of performing the same safe shutdown function.
Develop exemptions, deviations or 86-10 Fire Hazards Analysis with a 10 CFR 50.59 Safety Determination

Additional options are available for non-inerted containments as described in 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 equipment or cable

Compliance strategy statements or codes may be assigned to equipment or cables to identify the justification or mitigating actions proposed for achieving safe shutdown. Each piece of safe shutdown equipment and/or cable for the required safe shutdown path should be provided with a specific compliance strategy or

disposition. Refer to Attachment 6 to this document 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 is intended to 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

The following criteria/assumptions are applied when performing fire induced circuit failure evaluations.

3.5.1.1 The following circuit failure types shall be postulated on each conductor of each unprotected safe shutdown cable in order to determine the potential impact of a fire on the safe shutdown equipment associated with that cable.

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 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. loss of power to the MSIV solenoid valves due to an open circuit will result in the closure of the MSIVs).

A short-to-ground may result from a fire induced breakdown of a cable insulation system, resulting in the potential on the conductor being applied to ground potential. A short-to-ground may have all of the same effects as an open circuit and, in addition, a short to ground may also cause an impact to the control circuit or power train of which it is a part.

These three types of circuit failures identified above are to be

postulated to occur individually on each conductor of each safe shutdown cable on the required safe shutdown path in the fire area. The effects of each of these types of circuit failures are evaluated one at a time.

3.5.1.2 Circuit contacts are assumed to be positioned (i.e., open or closed) consistent with the normal mode/position of the safe shutdown equipment as shown on the schematic drawings. The position of the safe shutdown equipment must be considered 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 Fire-induced circuit failures to the following types of cables for safe shutdown equipment such as pumps, valves, fans and dampers can be readily determined to not impact safe shutdown:

Cables that provide indication only, where the indication circuit is isolated from the primary control circuit required to operate the equipment.

Cables with conductors that are part of an isolated auxiliary circuit that is interlocked with the safe shutdown circuit (auto signal, permissive), whose signal cannot result in a spurious operation or prevent operation of the equipment.

Cables whose conductors cannot cause spurious operation of safe shutdown equipment that is not required to be operated or repositioned from its normal position.

3.5.1.4 Circuit failure types resulting in spurious operations are postulated to 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. It is not postulated that the fire would eventually clear the circuit fault.

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 due to an open circuit will result in the closure of the MSIV.

The following consequences should be considered in the safe shutdown circuit analysis when postulating the effects of circuit failures related to 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. For equipment that does not fail safe, this should be evaluated.

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 below depicts the condition of an open circuit on a grounded control circuit.

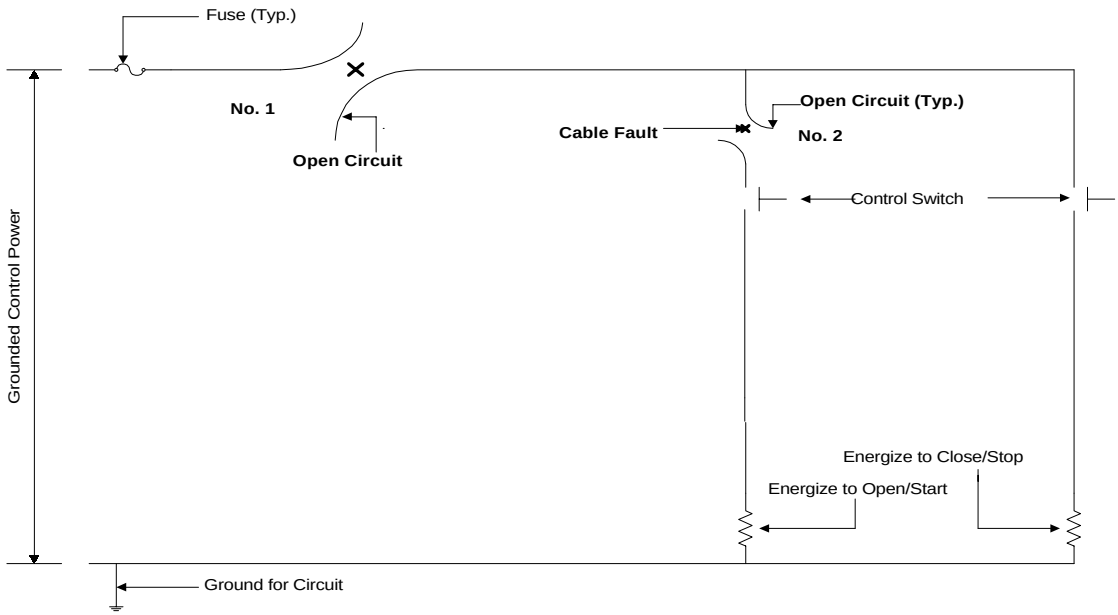


Figure 3.5.2-1 Open Circuit
(Grounded Control Circuit)

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.

The following consequences should be considered in the post-fire safe shutdown analysis when postulating 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.

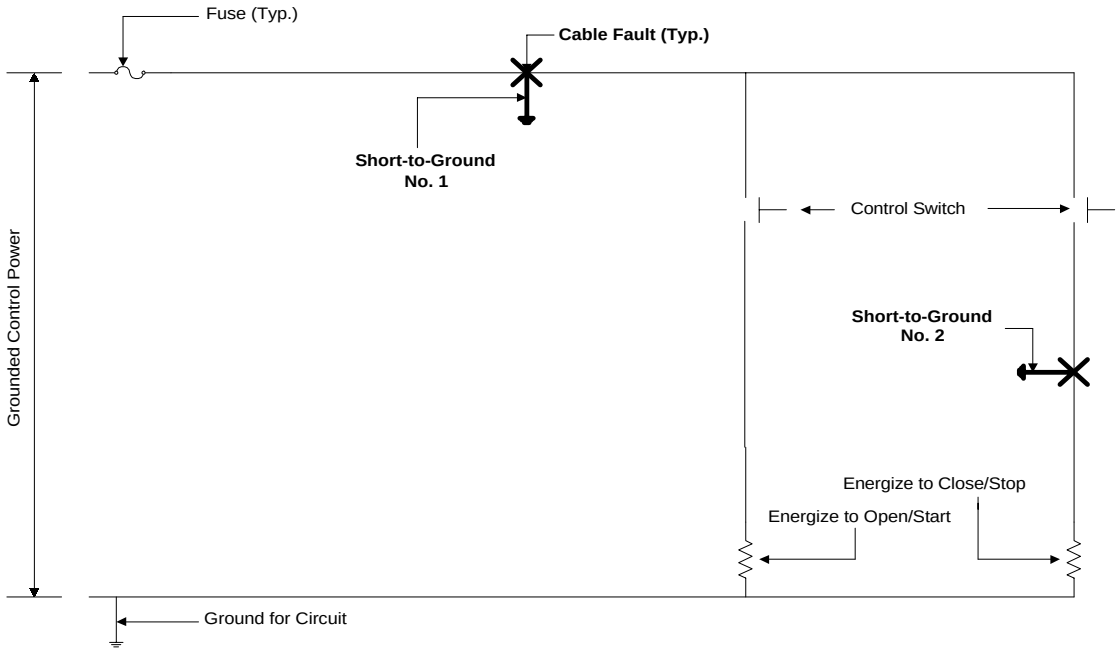


Figure 3.5.2-2 Short-to-Ground
(Grounded Control Circuit)

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 will 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, it would be prudent to assume that the ungrounded circuit may become grounded as a result of the fire unless one can demonstrate that no other conductors from the same power source were located in the fire area and that controls were in place to ensure that future modifications would not place such conductors in the fire area.

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

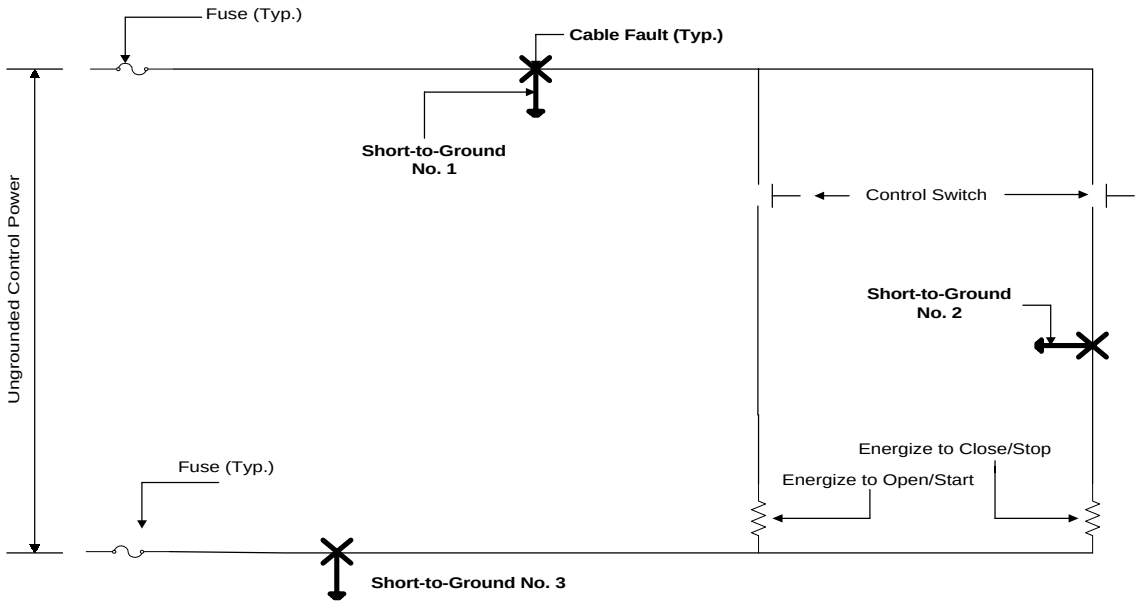


Figure 3.5.2-3 Short-to-Ground
(Ungrounded Control Circuit)

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 will 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 that is not desired to change state to operate and change state or to prevent equipment which is desired to change state to fail to operate.

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 which causes the spurious actuation of other equipment.

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.

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 these individual cable faults are to be addressed in terms of their impact on the operation of the equipment controlled by this circuit.

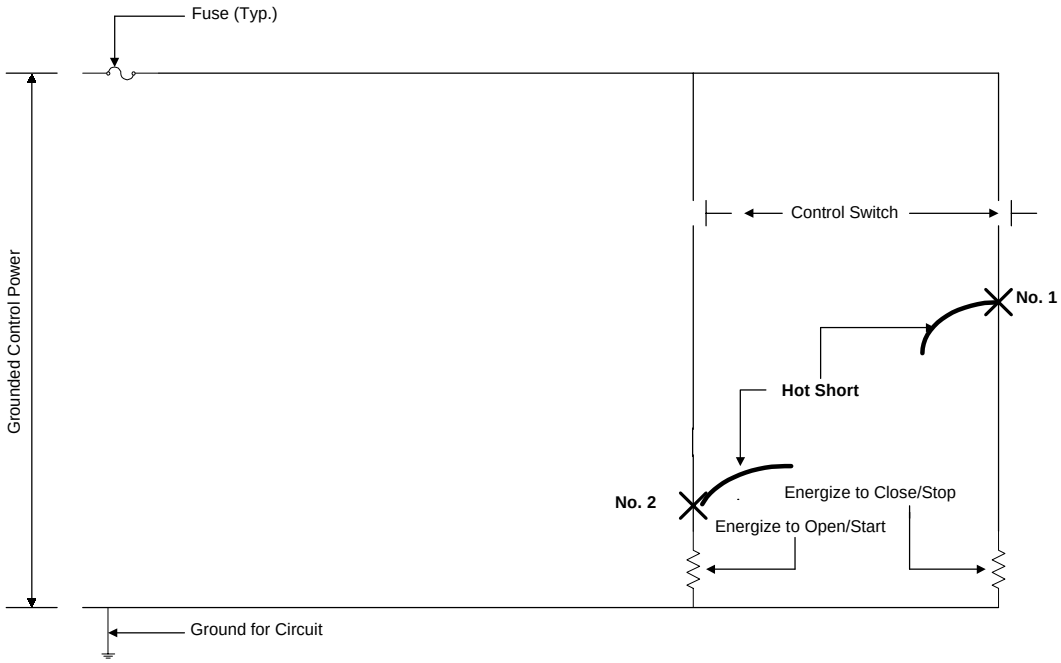


Figure 3.5.2-4 Hot Short
(Grounded Control Circuit)

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. Due to the likelihood of a short-to-ground being caused by a fire, it is considered to be prudent to assume that a spurious operation will result whenever the conductor between the control switch and the start/stop coil is affected by the fire. Since a hot short from the same source or grounding of ungrounded circuits cannot be ruled out, it is prudent to assume that ungrounded circuits will behave the same as grounded circuits in their response to hot shorts.

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 these individual cable faults are to be addressed in terms of their impact on the operation of the equipment controlled by this circuit.

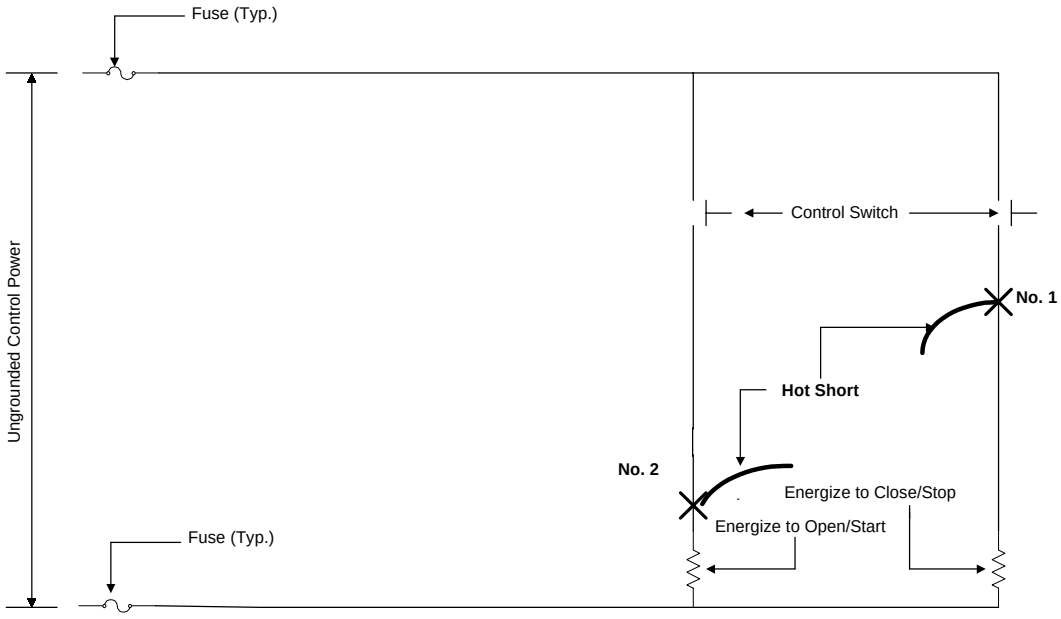


Figure 3.5.2-5 Hot Short
(Ungrounded Control Circuit)

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 Train B Pump, which is redundant to the Train A Pump powered from the Train B Bus.

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.

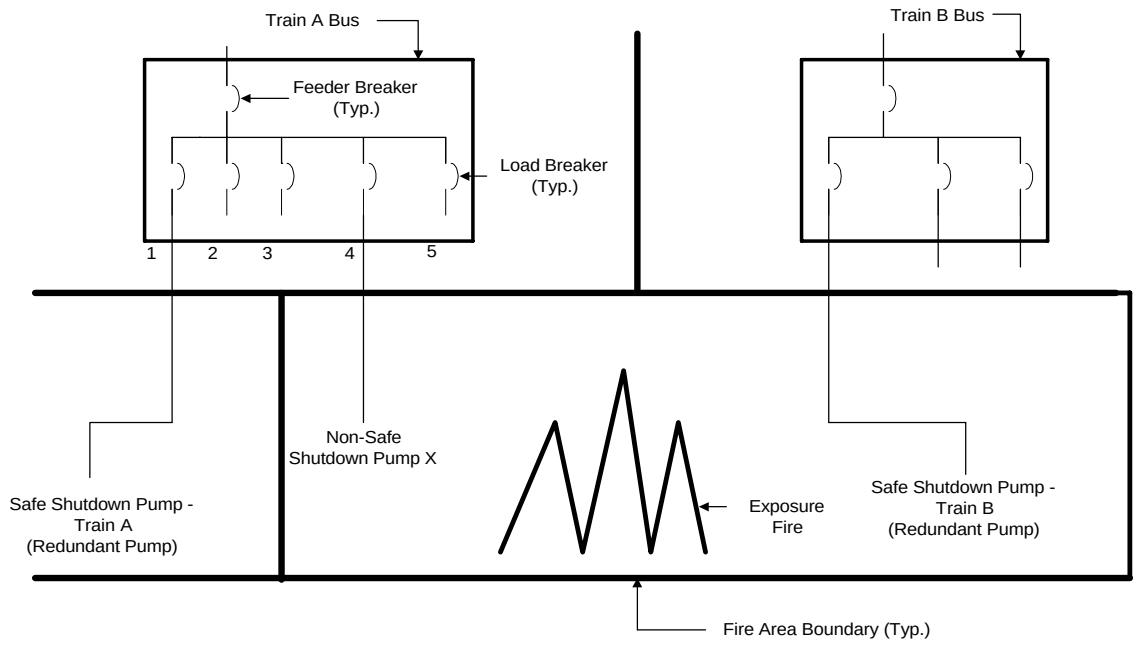


Figure 3.5.2-6 - Common Power Source (Breaker Coordination)

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 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:

The power sources required to supply power to safe shutdown equipment should be identified.

For each power source, breaker/fuse ratings, types, trip settings and coordination characteristics may be identified for the incoming source breaker supplying the bus and the breakers/fuses feeding the loads supplied by the bus.

For each power source, proper circuit coordination may be demonstrated by comparing the time current characteristic (TCC) curve for the largest size load breaker to the TCC curve for the incoming source breaker supplying the bus. Two breakers are coordinated if the downstream breaker trips before the upstream breaker over the entire current tripping range of both breakers up to and including the maximum fault current.

For cases in which the TCC curves for the supply circuit and a load circuit intersect, proper coordination may not exist. Thus, further analysis is required.

In certain cases, coordination relative to the available short circuit current is dependent upon the distance of the fault from the bus. Consideration of the cable impedance from the bus to the fire area being evaluated may reduce the maximum available fault current to a level that demonstrates adequate coordination.

For power sources not properly coordinated, the routing of cables whose breaker/fuse is not properly coordinated with the supply breaker/fuse is tabulated by fire area. The potential for disabling power to the bus is evaluated 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. A list of the following information is prepared 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.

Analyzed safe shutdown circuit dispositions are developed for the associated circuit of concern cables routed in an area of the same path as required by the power source. Adequate separation is evaluated 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 and this may be demonstrated by reviewing the plant's electrical design criteria for compliance with the National Electrical Code. The fire rated barrier and penetration designs which preclude the propagation of fire from one fire area to the next should also be reviewed to demonstrate that adequate measures are in place to alleviate fire propagation concerns.

4.0 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.

Unless otherwise noted, the definitions referenced in this section are taken from reference 5.4.32.

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 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 potential.

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 F 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.

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 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

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.

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 which prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits. [384]

Local Control

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 (see Appendix F for additional information related to local control).

Manual Operation

Operation of safe shutdown equipment on the required safe shutdown path by an operator when automatic, local or manual controls are no longer available (e.g., opening of a motor operated valve using the hand wheel). Refer to Appendix F for additional information related to manual actions.

Manual Control

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 (see Appendix F for additional information related to manual control).

Multiple High Impedance Fault(s)

A condition where multiple circuits fed from a single power distribution source each have a high impedance fault. See 'High Impedance Fault' (see Appendix E).

Open Circuit

See 'Circuit failure modes'.

Raceway

IEEE Standard 380-1975 - Any channel that is designed and used expressly for supporting wires, cable, or bus bars. 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 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.

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 Guidance 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 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

Where none of the hot shutdown trains of the redundant safe shutdown capability is "free of fire damage" and dedicated equipment is not provided, the shutdown systems used are 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'.

Shutdown Paths

A specific combination of analyzed systems and equipment capable of achieving and maintaining a safe shutdown condition during and following an exposure fire.

Spurious Operation

The inadvertent operation or repositioning of a piece of equipment.

5.0 REFERENCES

5.1 NRC GENERIC LETTERS

5.1.1 80-45: Proposed Rule Fire Protection Program for Nuclear Power Plants

5.1.2 80-48: Proposed Rule Fire Protection Program for Nuclear Power Plants

5.1.3 80-56: Memorandum and Order RE: Union of Concerned Scientists Petition

5.1.4 80-100: Resolution of Fire Protection Open Items

5.1.5 81-12: Fire Protection Rule, dated February 20, 1981

5.1.6 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

5.1.7 82-21: Tech Specs for Fire Protection Audits

5.1.8 83-33: NRC Positions on Appendix R

5.1.9 85-01: Fire Protection Policy Steering Committee Report

5.1.10 86-10: Implementation of Fire Protection Requirements, dated April 24, 1986

5.1.11 86-10: Supplement 1 to Generic Letter, Implementation of Fire Protection Requirements

5.1.12 88-12: Removal of Fire Protection Requirements from Tech Specs

5.1.13 88-20: Supplement 4 IPEEE

5.1.14 89-13: Supplement 1 Biofouling of Fire Protection Systems

5.1.15 92-08: Thermo-Lag Fire Barriers

5.1.16 93-06: Use of Combustible Gases in Vital Areas

5.1.17 95-01: Fire Protection for Fuel Cycle Facilities

5.2 BULLETINS

5.2.1 75-04: Browns Ferry Fire

5.2.2 77-08: Assurance of Safety

5.2.3 81-03: Flow Blockage Due to Clams and Mussels

5.2.4 92-01: Failure of Thermo-Lag

5.2.5 92-01: Supplement 1 Failure of Thermo-Lag

5.3 NRC INFORMATION NOTICES

5.3.1 80-25: Transportation of Pyrophoric Uranium

5.3.2 83-41: Actuation of Fire Suppression System causing Inoperability of Safety-Related Equipment, June 22, 1983

5.3.3 83-69: Improperly installed Fire Dampers

5.3.4 83-83: Use of Portable Radio Transmitters Inside Nuclear Power Plants

5.3.5 84-09: Lessons learned from NRC Inspections of Fire Protection Safe Shutdown Systems (10CFR50, Appendix R), Revision 1, March 7, 1984

5.3.6 84-16: Failure of Automatic Sprinkler System Valves to Operate

5.3.7 84-92: Cracking of Flywheels on Fire Pump Diesel Engines

5.3.8 85-09: Isolation Transfer Switches and Post-fire Shutdown Capability, January 31, 1985

5.3.9 85-85: System Interaction Event Resulting in Reactor Safety Relief Valve Opening

5.3.10 86-17: Update - Failure of Automatic Sprinkler System Valves

5.3.11 86-35: Fire in Compressible Material

5.3.12 86-106: Surry Feedwater Line Break

5.3.13 86-106: Supplement 1 Surry Feedwater Line Break

5.3.14 86-106: Supplement 2 Surry Feedwater Line Break

5.3.15 86-106: Supplement 3 Surry Feedwater Line Break

5.3.16 87-14: Actuation of Fire Supp. Causing Inop of Safety Related Ventilation

5.3.17 87-49: Deficiencies in Outside Containment Flooding Protection

5.3.18 87-50: Potential LOCA at High and Low Pressure Interfaces from Fire Damage, October 9, 1987

5.3.19 88-04: Inadequate Qualification of Fire Barrier Penetration Seals

5.3.20 88-04: Supplement 1 Inadequate Qualification of Fire Barrier Penetration Seals

5.3.21 88-05: Fire in Annunciator Control Cabinets

5.3.22 88-45: Problems in Protective Relay and Circuit Breaker Coordination, July 7, 1988

5.3.23 88-56: Silicone Fire Barrier Penetration Seals

5.3.24 88-60: Inadequate Design & Installation of Watertight Penetration Seals

5.3.25 88-64: Reporting Fires in Process Systems

5.3.26 89-52: Fire Damper Operational Problems

5.3.27 90-69: Adequacy of Emergency and Essential Lighting, October 31, 1990

5.3.28 91-17: Fire Safety of Temporary Installations

5.3.29 91-18: Resolution of Degraded & Nonconforming Conditions

5.3.30 91-37: Compressed Gas Cylinder Missile Hazards

5.3.31 91-47: Failure of Thermo-Lag

5.3.32 91-53: Failure of Remote Shutdown Instrumentation

5.3.33 91-77: Shift Staffing at Nuclear Power Plants

5.3.34 91-79: Deficiencies in Installing Thermo-Lag

5.3.35 91-79: Supplement 1

5.3.36 92-14: Uranium Oxide Fires

5.3.37 92-18: Loss of Remote Shutdown Capability During a Fire, February 28, 1992

5.3.38 92-28: Inadequate Fire Suppression System Testing

5.3.39 92-46: Thermo-Lag Fire Barrier Special Review Team Final Report

5.3.40 92-55: Thermo-Lag Fire Endurance Test Results

5.3.41 92-82: Thermo-Lag Combustibility Testing

5.3.42 93-40: Thermal Ceramics Fire Endurance Tests

5.3.43 93-41: Fire Endurance Tests - Kaowool, Interam

5.3.44 93-71: Fire at Chernobyl Unit 2

5.3.45 94-12: Resolution of GI 57 Effects of Fire Prot. Sys. Actuation on SR Equipt.

5.3.46 94-22: Thermo-Lag 3-Hour Fire Endurance Tests

5.3.47 94-26: Personnel Hazards From Smoldering Material in the Drywell

5.3.48 94-28: Problems with Fire-Barrier Penetration Seals

5.3.49 94-31: Failure of Wilco Lexan Fire Hose Nozzles

5.3.50 94-34: Thermo-Lag Flexi-Blanket Ampacity Derating Concerns

5.3.51 94-58: Reactor Coolant Pump Lube Oil Fire

5.3.52 94-86: Legal Actions Against Thermal Science Inc.

5.3.53 94-86: Supplement 1

5.3.54 95-27: NRC Review of NEI Thermo-Lag Combustibility Evaluation Methodology

5.3.55 95-32: Thermo-Lag 330-1 Flame Spread Test Results

5.3.56 95-33: Switchgear Fire at Waterford Unit 3

5.3.57 95-36: Problems with Post-Fire Emergency Lighting

5.3.58 95-36: Supplement 1

5.3.59 95-48: Results of Shift Staffing Survey

5.3.60 95-49: Seismic Adequacy of Thermo-Lag Panels

5.3.61 95-49: Supplement 1

5.3.62 95-52: Fire Test Results of 3M Interam Fire Barrier Materials

5.3.63 95-52: Supplement 1

5.3.64 96-23: Fire in Emergency Diesel Generator Exciter

5.3.65 97-01: Improper Electrical Grounding Results in Simultaneous Fires

5.3.66 97-23: Reporting of Fires at Fuel Cycle Facilities

5.3.67 97-37: Main Transformer Fault

5.3.68 97-48: Inadequate Fire Protection Compensatory Measures

5.3.69 97-59: Fire Endurance Tests of Versawrap Fire Barriers

5.3.70 97-70: Problems with Fire Barrier Penetration Seals

5.3.71 97-72: Problems with Omega Sprinkler Heads

5.3.72 97-73: Fire Hazard in the Use of a Leak Sealant

5.3.73 97-82: Inadvertent Control Room Halon Actuation

5.4 OTHER RELATED DOCUMENTS

5.4.1 10 CFR 50.48 Fire Protection (45 FR 76602)

5.4.2 10 CFR 50 Appendix A GDC 3 Fire Protection

5.4.3 10 CFR 50 Appendix R Fire Protection for Operating Nuclear Power Plants

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

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

5.4.6 NUREG-0800 9.5.1 Fire Protection Program

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

5.4.8 NRC Insp. Procedure 64150 Triennial Postfire Safe Shutdown Capability

5.4.9 NRC Insp. Procedure 64704 Fire Protection Program

5.4.10 NUREG/BR-0195 Enforcement Guidance

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

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

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

5.4.14 Reg Guide 1.120 Fire Protection Guidelines for Nuclear Power Plants

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

5.4.16 NUREG-0654 Criteria for Preparation of Emergency Response Plans

5.4.17 Temporary Instruction 2515/XXX Fire Protection Functional Inspection

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

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

5.4.20 SECY-83-269 FP Rule for Future Plants

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

5.4.22 NRC Temp Instruc 2515/62 Inspection of Safe Shutdown Requirements of 10CFR50

5.4.23 NRC Temp Instruc 2515/61 Inspection of Emergency Lighting & Oil Collection Requirements

5.4.24 NUREG-0050, 2/76; Recommendations Related to Bowns Ferry Fire

5.4.25 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.

5.4.26 SECY-93-143 Assessment of Fire Protection Programs

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

5.4.28 SECY-96-134 Fire Protection Regulation Improvement

5.4.29 Appendix S Proposed Rulemaking

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

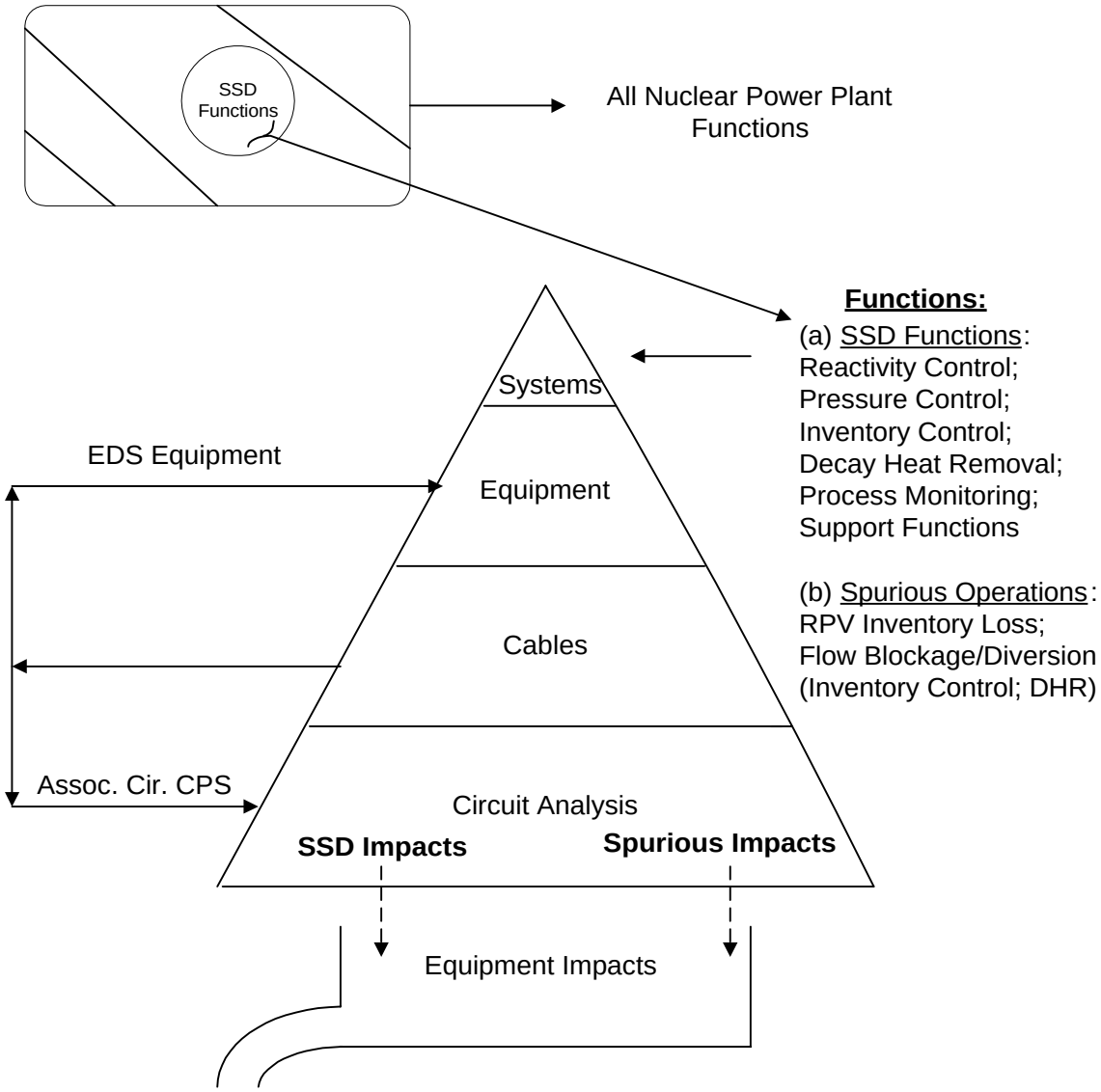
5.4.31 NEI letter to NRC dated May 30, 1997, general subject industry positions on fire-induced circuit failures issues

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

5.5 ADMIN LETTERS

5.5.1 95-06 Relocation of Technical Specification Administrative Controls

Figure 1-1
Post-fire Safe Shutdown Overview



Mitigation Techniques

Reroute Circuit, Wrap Raceway
Manual Action, Repair
Other Equipment
Other Plant Unique Approach

- 86-10 Evaluation
- Exemption
- Deviation

Figure 1-2
Guidance Document Methodology Overview

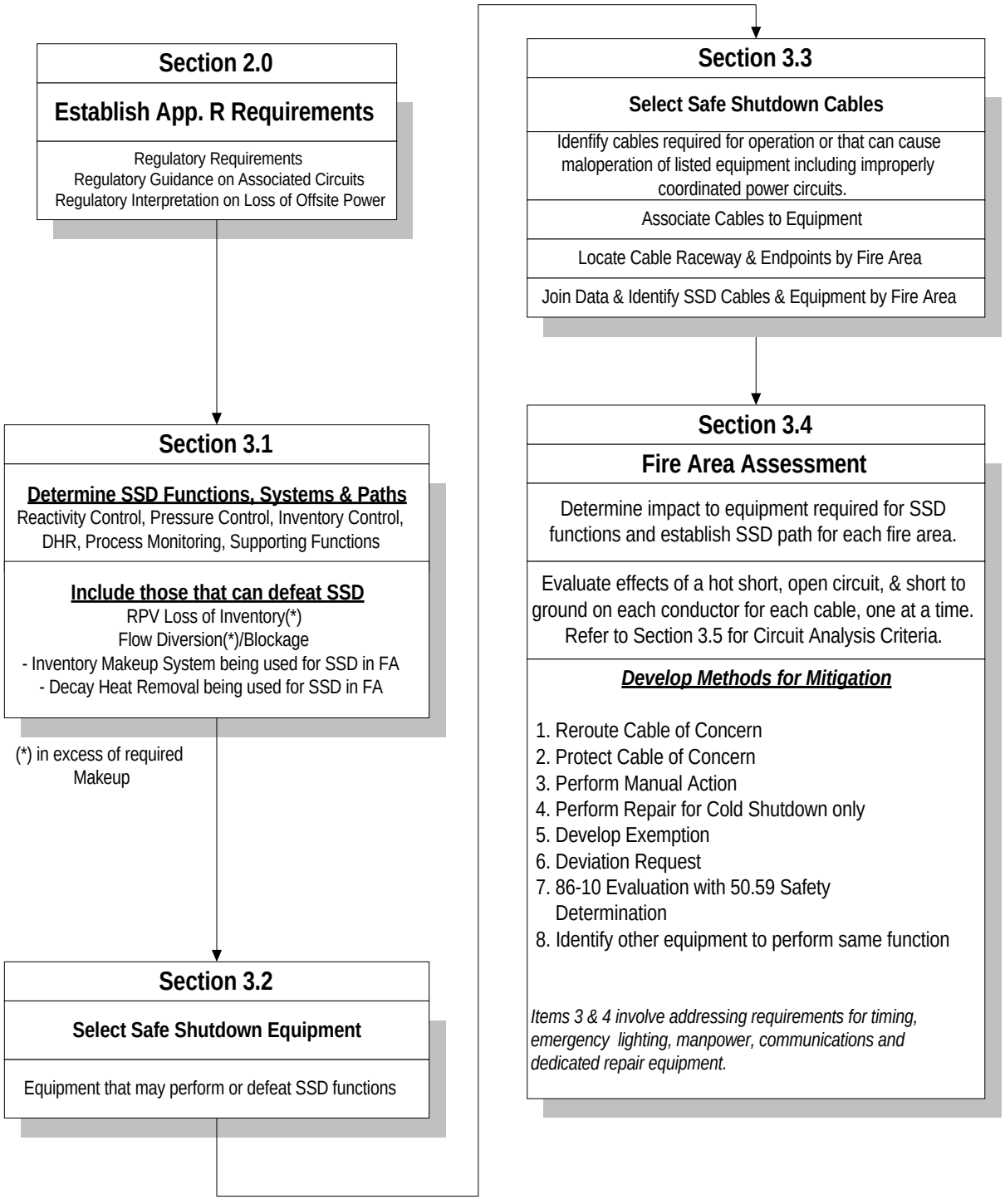
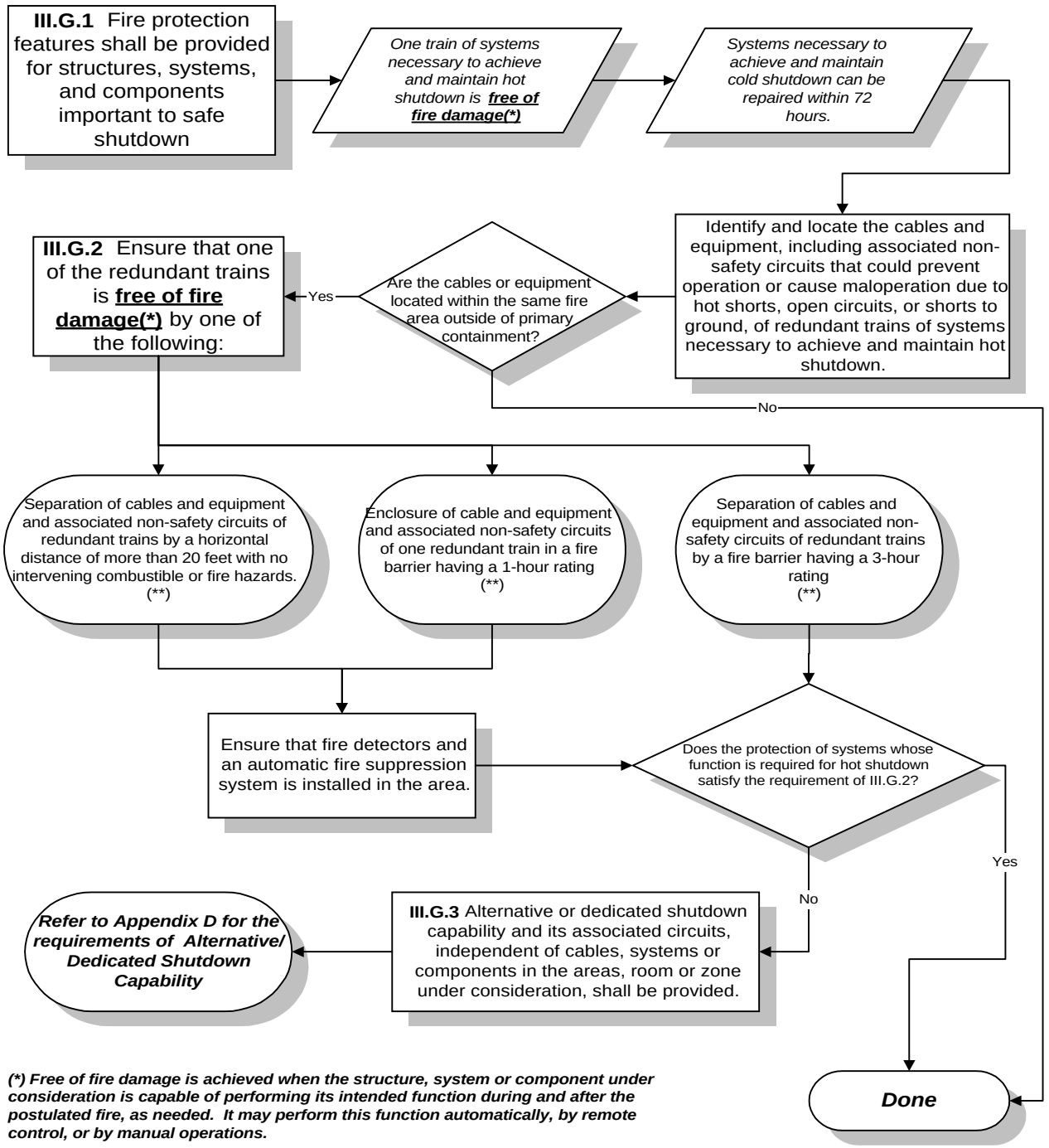


Figure 2-1
Appendix R Requirements Flowchart



(*) 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 or 86-10 Evaluations with 50.59 Safety Determinations may be developed as necessary.

Figure 3-1
Safe Shutdown System Selction and Path Development

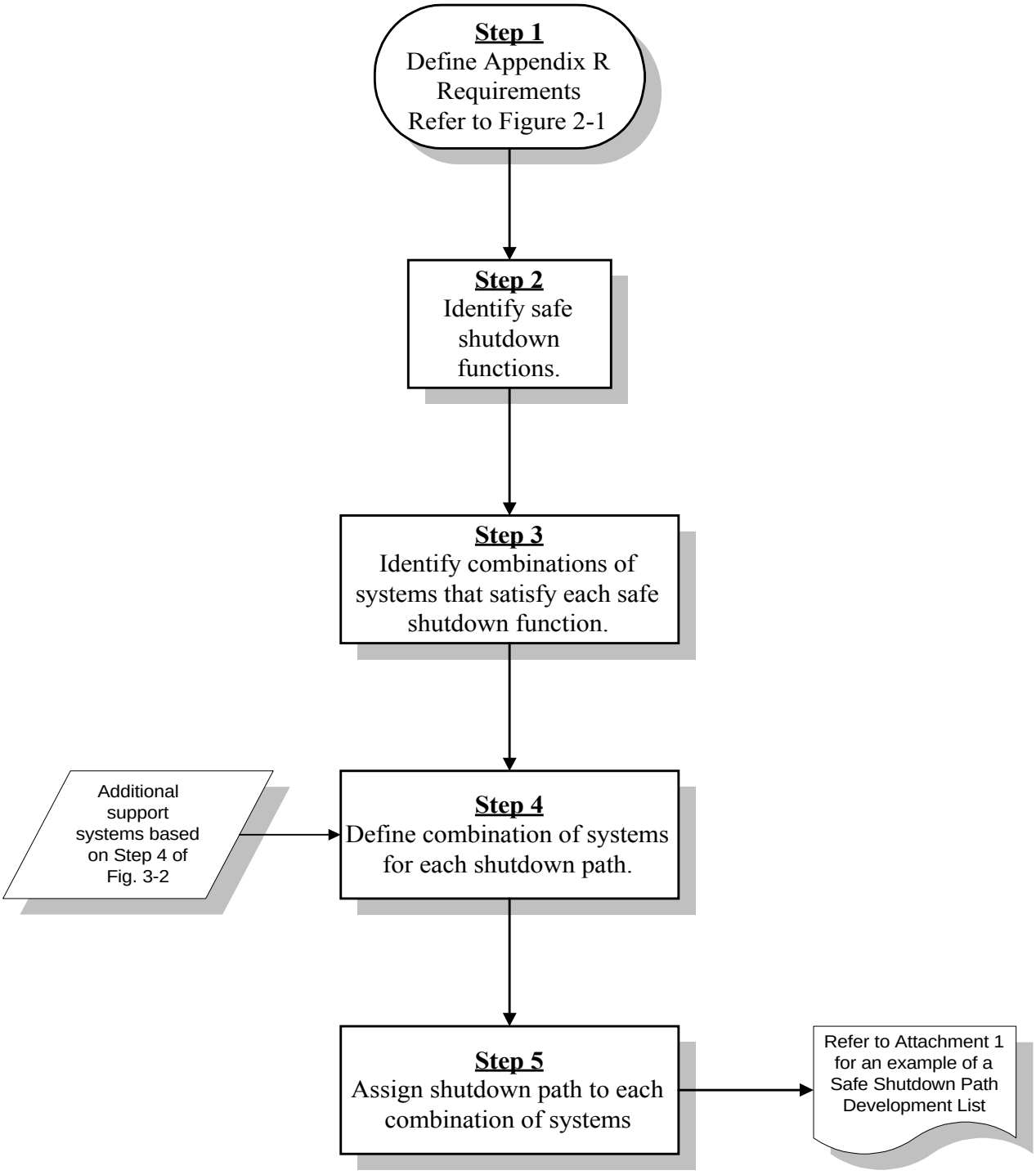


Figure 3-2
Safe Shutdown Equipment Selection

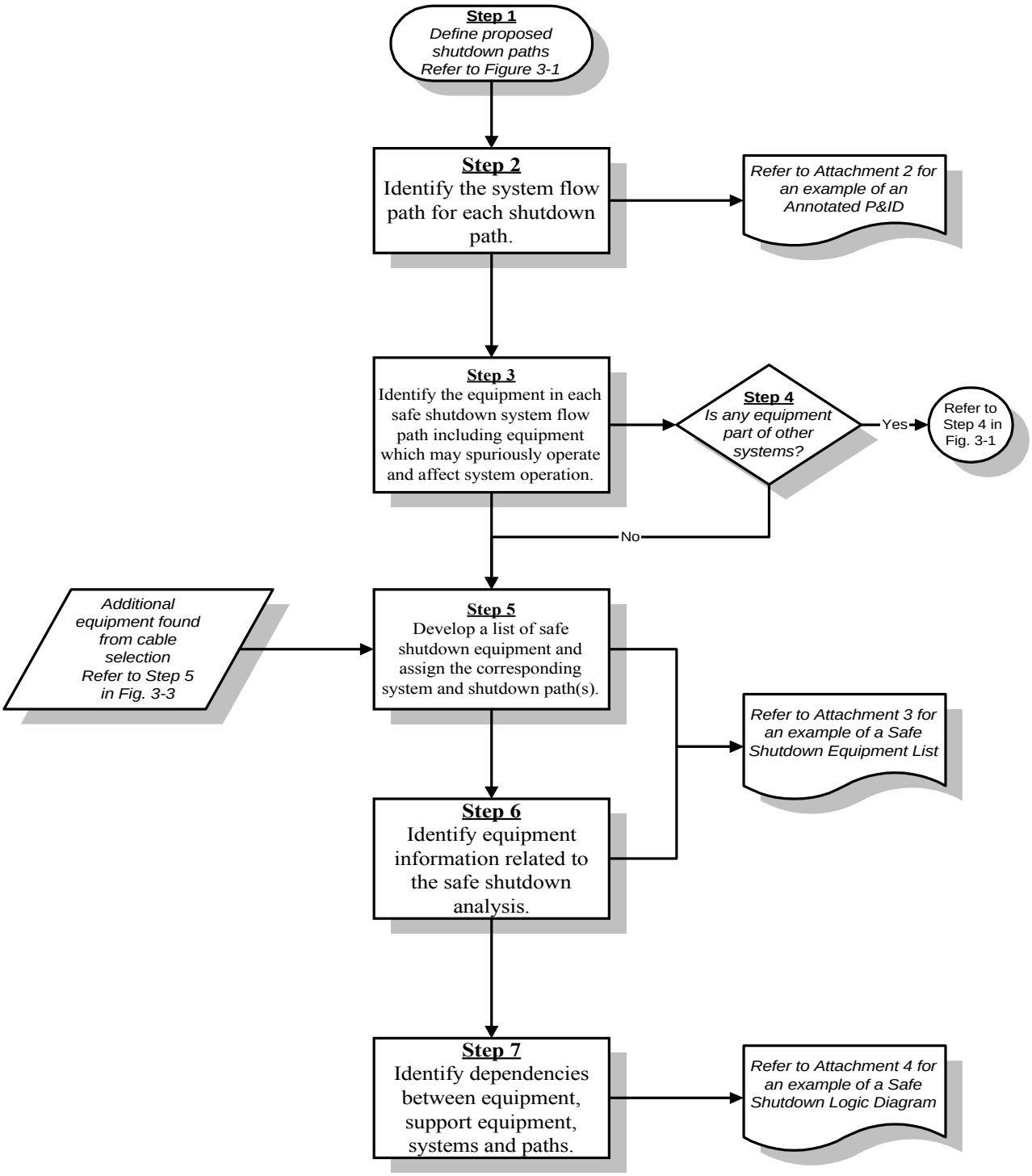
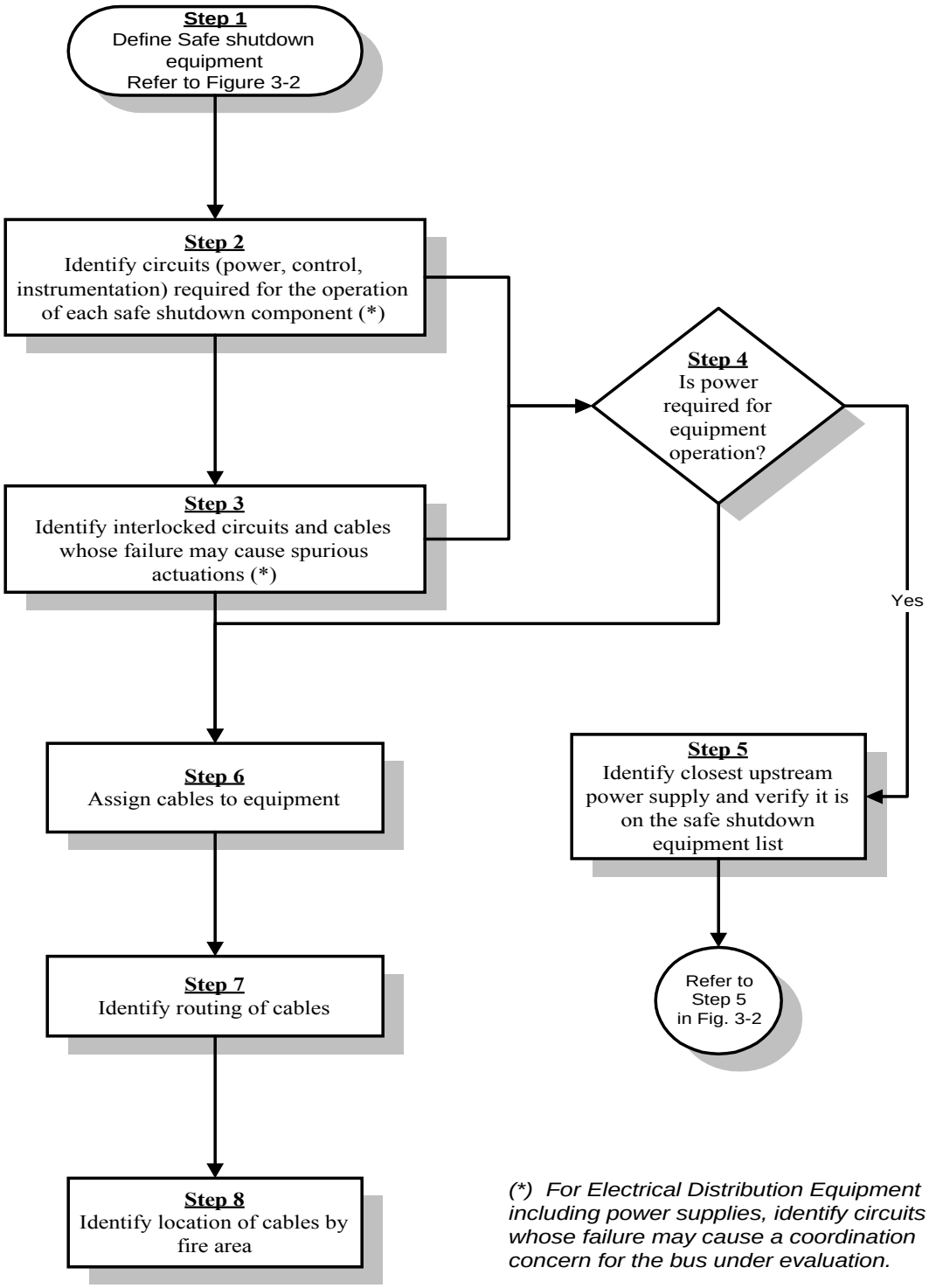
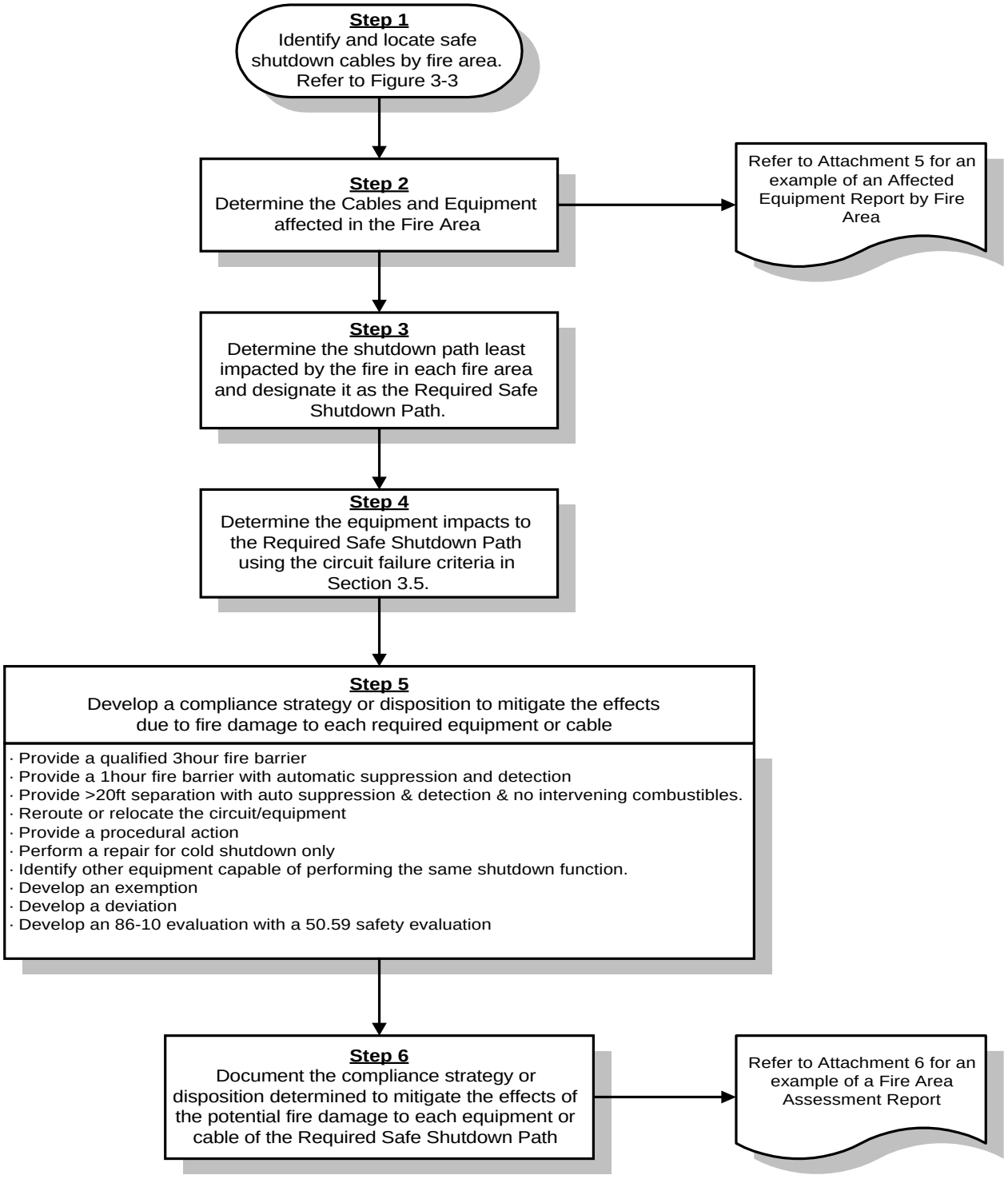


Figure 3-3
Safe Shutdown Cable Selection



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

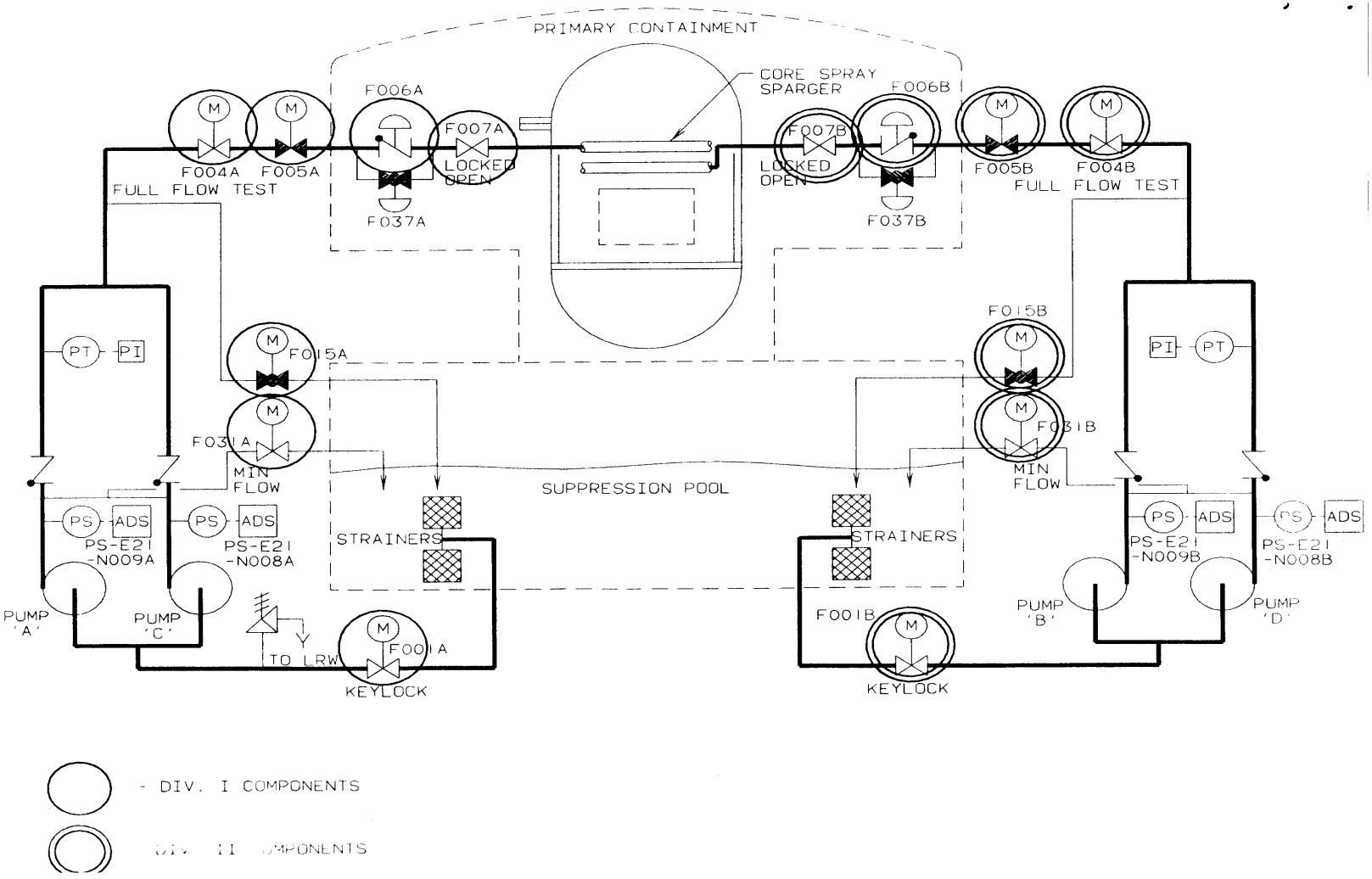
Figure 3-4
Fire Area Assessment Flowchart



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

Attachment 2
Annotated P&ID Illustrating SSD System Paths



Core Spray System

Attachment 3
Safe Shutdown Equipment List
(Sorted by Equipment ID)

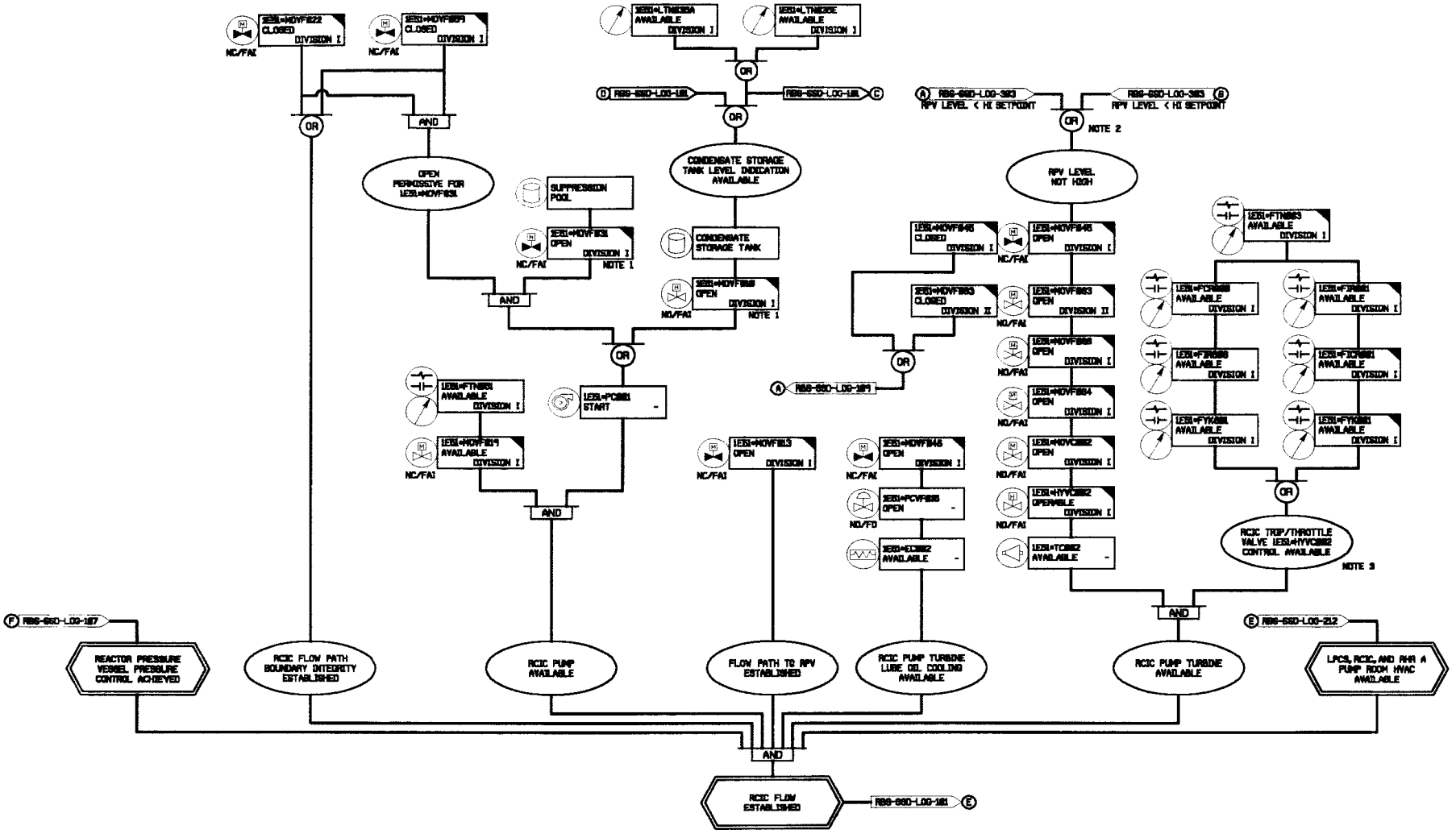
Equipment ID	Logic Diagram	System	Unit	Equipment Type	SSD Path	Equipment Description	Equip FA	Normal Mode	Shutdown Mode(s)	Hi/Lo	Air Fail	Power Fail	Reference

Attachment 3

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 which 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
Safe Shutdown Logic Diagram



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

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 which 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 which 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

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 which 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 which 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 provides a discussion of 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. The components of defense-in-depth built into each licensee's program are: (1) measures to prevent fires from starting; (2) measures to detect a fire upon initiation; (3) measures to mitigate the effects of fire; (4) measures to prevent the spread of fire to adjacent areas; (5) demonstration of the ability to achieve and maintain safe shutdown in the event of a single fire in any plant fire area. This latter component is the domain of the Appendix R Safe Shutdown Analysis. In reality, post-fire safe shutdown is accomplished in conjunction with other defense-in-depth components. The post-fire safe shutdown analysis, however, is performed with the assumption that many of these other components have suffered significant degradation.

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 provide a discussion of the Brown's Ferry fire, the investigation of that fire, the recommendations made to prevent recurrence of such a fire and the improvement made by the U.S. Nuclear Power Industry relative to these recommendations.

A.3.0 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 which 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 which 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 provided recommended improvements in its report, NUREG-0050, "Recommendations Related to Browns Ferry Fire" issued in Feb. 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, the licensees were informed 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 which 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 establish a definitive resolution of these contested subjects in a manner 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. This new rule was described 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 an extremely severe fire. Considerable damage was done to plant cabling and associated equipment affecting vital plant shutdown functions. The fire burned, uncontrolled, while fire fighting efforts, using CO2 and dry chemical extinguishers, continued for approximately 7 hours with little success until water was used to complete the final extinguishing process.

During the 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 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 which were reported and to take appropriate corrective actions.

Use of an open flame from a candle (used to check for air leaks) which 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 which 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. These improvements 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 are 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. Both 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.

1. 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 the necessary assurance that the plant design and operation will be safe from the effects of fire. When these changes are integrated into an approach similar to that outlined in the body of this document for assuring the ability to achieve and maintain post-fire safe shutdown, the result is a significantly enhanced plant

design with emphasis on precluding any unacceptable consequences resulting from plant fires.

A.5.0 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

CONSIDERATION OF NRC IN 92-18

B.1.0 PURPOSE

The purpose of this Appendix is to provide an acceptable means of addressing the issues associated with NRC Information Notice (IN) 92-18, "Potential for Loss of Remote Shutdown Capability During a Control Room Fire." The discussion provided in this Appendix may not be the only means for addressing these issues. It provides an example of an evaluation that adequately addresses the issues raised in IN 92-18.

B.2.0 INTRODUCTION

The U.S. Nuclear Regulatory Commission (NRC) issued IN 92-18, "Potential for Loss of Remote Shutdown Capability During a Control Room Fire," to alert the industry to a condition that could result in the loss of safe shutdown capability in the event of a control room fire. Specifically, in the condition described in IN 92-18, a hot short in the control circuitry of a Motor Operated Valve (MOV) could potentially cause the valve to operate in either the open or closed direction. In the condition described, a hot short may occur such that the torque switch in the MOV control circuitry would be bypassed. Therefore, when the valve reached the end of its travel, it would continue to try to operate resulting in an overtorque condition that could potentially damage the valve. This damage could prevent the valve from performing its post-fire safe shutdown function. This scenario assumed mechanistic fire-induced failures that could potentially challenge the capability to achieve and maintain safe shutdown in the event of a Control Room fire.

This appendix provides an evaluation of the issues involved in IN 92-18 from a regulatory, safety, and risk significance perspective. The risk significance portion of the evaluation is performed for a BWR 6 PGCC designed Control Room, but the method used in the evaluation applies to any operating nuclear facility. In fact, several facilities have used methods similar to this to assess the potential for impact due to this issue and have achieved comparable results. In all of the assessments performed to date, the focus has been on the Control Room, since this is the plant area with the greatest number of circuits from both divisions in the closest proximity to each other.

B.3.0 REGULATORY REVIEW

IN 92-18 addresses a condition that was considered to be of potential safety significance in the unlikely event that a control room fire forced reactor operators to evacuate the control room. Specifically, in the Purpose section of IN 92-18, it states:

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice to alert addressees to conditions found at several reactors that could result in the loss of

capability to maintain the reactor in a safe shutdown condition in the unlikely event that a control room fire forced reactor operators to evacuate the control room. It is expected that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this information notice are not NRC requirements; therefore, no specific action or written response is required.

B.4.0 SAFETY SIGNIFICANCE REVIEW

Before analyzing the safety significance and/or concerns involved in IN 92-18, the scenario itself as it pertains to the Safe Shutdown Analysis will be described. It is as follows:

> A Control Room fire requiring evacuation occurs. The fire produces a "Hot Short" in the control circuitry for an Alternate Shutdown MOV. This hot short is of the specific type that changes the position of the affected valve such that it bypasses the MOV torque and/or limit switches. This MOV overtorques in the undesirable position resulting in damage to the MOV such that it cannot be used for its design safe shutdown purpose when called upon to do so.

The physical fire area of consideration for this scenario is the Main Control Room complex. Since the Control Room is the plant area with the greatest number of circuits from both divisions in close proximity to each other, it is considered to be a bounding case.

Generally, a Control Room design considers divisional separation between panels and cables. Consequently, cables and components are physically separated from their redundant counterparts. Alternate/Remote shutdown capability is provided by transferring and/or isolating the control circuits for at least one division of safe shutdown equipment such that the required systems can operate independently of the control room.

For the scenario described in IN 92-18 to occur and adversely affect safe shutdown, the severity of the Control Room fire must be such that the damage occurs to redundant divisions of safe shutdown equipment. Also, the Control Room environment must be rendered uninhabitable to preclude the use of any other available plant systems to mitigate the effects of the fire to achieve and maintain safe shutdown, or the fire would need to be so severe that these other systems with shutdown capability would be rendered incapable of automatically functioning. Additionally, the damage would have to occur in the first few minutes of the fire during the period between when the control room is evacuated and when transfer is made to the alternative shutdown system. During a Control Room fire, the plant operations staff would perform in accordance with their training and governing procedures and act appropriately to mitigate the effects of any fire damage for the period of time prior to evacuation.

Thus, the scenario would require a fast developing fire of extreme magnitude. Additionally, this fire would have to defeat all extinguishing attempts and affect multiple

divisions of Control Room complex instrumentation and controls. Finally, the fire would have to result in the development of the specific "Hot Shorts" described in IN 92-18. This sequence of events would all have to transpire prior to the isolation of the Alternative Shutdown MOV circuits from the control room. This is highly unlikely for the following reasons:

a) The specific hot short described in IN 92-18 is extremely unlikely even if a fire did occur in the Control Room. While it is generally accepted that a hot short condition is a required analysis assumption, this assumption and any subsequent change of state of the equipment is considered to be a bounding assumption. Although the level of conservatism embedded in this assumption has never been rigorously determined, it is considered to be of a level sufficient to preclude the need to also postulate mechanistic damage to the equipment. The assessment contained in this appendix assumes that mechanistic damage does occur. The results of this assessment can, therefore, be viewed as being very conservative in that they do not include the low likelihood of occurrence of an equipment damaging hot short but, rather, assume this likelihood to be 1.0. For the case of IN 92-18, the following are some of the technical arguments that lead to the general conclusion that designing for a damaging hot short is an overly conservative and unrealistic requirement:

    1) The magnitude of the short circuit current would have to be large enough to energize the MOV contactor. This assumes a "hard" hot short. If the hot short occurs at a point in the circuitry where the combined resistance is too high, the amperage will not be large enough to energize the relay and pull in the contactor.

    2) Other associated cabling and wires could fail which could result in an open circuit or a short to ground that could prevent contactor energization due to loss of control power. A fire that affects the circuitry for the equipment of concern would generally be of such severity that it would also affect other associated cabling and wires of the same circuitry in the general vicinity. If this other cabling and wiring damage resulted in a short to ground, the resulting high amperage would blow the control power fuse resulting in a loss of control power to the circuit. If this were to occur, a subsequent hot short in that circuit would be inconsequential, since there would be no power available because of the blown fuse.

       If an open circuit were to occur in series with the hot short, again, the hot short would be inconsequential, because there would be no power available in that portion of the circuitry.

    3) The hot short must be sustained for a time sufficient to result in unrecoverable damage to the valve motor operator. If the circuit causing the hot short were to progress to a short to ground or an open circuit

during the time required to drive the valve to failure, the potential for equipment damage would be eliminated.

4) The hot short could only be of the type that would fail the valve in its undesirable position. In other words, if the valve were to fail, but the failure were in a position such that the valve would still allow the safe shutdown system to perform its required post-fire safe shutdown function, the hot short would be of no concern.

b) As in all plant areas, plants employ a comprehensive defense-in-depth approach in the Control Room. This approach prevents fires from starting, and even if a fire were to occur, allows for the rapid detection of the fire and limits the development rate and extent of the fire. It also provides a readily available means (personnel and equipment) for performing a rapid suppression of the fire and limiting the damage effects. This defense-in-depth methodology usually consists of, but is not limited to, the following attributes:

1) Strict control of the types and quantities of combustibles, both in-situ and transient, in the Control Room. Fire severity is greatly driven by available combustibles and ignition sources. In the Control Room, combustibles and ignition sources are tightly controlled.

2) Design features such as in-cabinet fire detectors and automatic suppression for concealed spaces

3) Continuous manning of the Control Room by Operations personnel who are currently or having been previously qualified as members of the fire brigade.

4) Fire fighting equipment is readily available in the Control Room.

c) Based upon a realistic Control Room fire event, it is unlikely that the scenario of concern in IN 92-18 would prevent the operator from performing a safe shutdown of the plant. For a control room fire to prevent safe shutdown due to the type of hot shorts described in IN 92-18, the following would have to occur:

1) The control room fire would have to require evacuation of the Control Room which is unlikely based upon the amount of combustibles present. Otherwise, even if an MOV with circuitry in one panel were affected, it is very probable that one or more redundant safe shutdown paths would be able to perform its function, including normally-operating balance of plant (BOP) cooling systems that are in service prior to the fire event. This is primarily because the circuitry and cabling within the Control Room, while not separated in accordance with 10CFR50 Appendix R III.G criteria, are generally separated divisionally between panels or panel sections.

2) If evacuation were required, the hot shorts would have to occur in the short duration from the time that the Control Room is evacuated to the time that the Alternative Shutdown system is isolated from the Control Room. In general, this time does not exceed 10 minutes in duration. While in the Control Room, the operations staff would respond appropriately to any fire-induced damage.

Based upon the above reasoning, the event described in IN 92-18 is highly improbable based on the low credibility of this type of consequential hot short. While it is generally accepted that a hot short condition is a required analysis assumption, this assumption and any subsequent change of state of the equipment is considered to be a sufficiently conservative bounding assumption. Despite this, the risk assessment provided below assumes mechanistic equipment damage results from a hot short. By demonstrating the low safety significance associated with this event, even assuming an equipment damaging hot short, industry believes that the issues raised in IN 92-18 do not need to be included in the design basis for fire-induced circuit failures for consideration in a post-fire safe shutdown analysis.

B.5.0 RISK SIGNIFICANCE REVIEW

For the case of IN 92-18, an evaluation of the frequency of the type of fire that would lead to an IN 92-18 scenario would be useful to determine if this type of hot short should be considered.

Therefore, the following evaluation will evaluate the frequency of a Control Room event that:

- damages Alternative Shutdown MOV circuits prior to their isolation from the Control Room; and
- damages the other division's circuits that could be used to perform a Post-Fire Safe Shutdown.

For the purposes of this evaluation, a typical BWR-6 designed (Power Generation Control Complex (PGCC)) Control Room was used. The PGCC design consists of "a set of floor sections, a set of termination cabinets (one for each floor section), and a set of interpanel cables. The steel floor sections contain raceways to provide routing and separation of all interpanel cabling." (Reference B.6.4). Normally the floor sections are supplied with a gas fire suppression system (Halon 1301). Termination cabinets normally contain divisionally separated control circuitry; however, when multiple division's circuitry are in the same cabinet, metal barriers are provided for separation purposes. Both termination cabinets and floor section ducts have been qualified by fire testing, as described in NEDO-10466-A (NRC approved), and are capable of preventing fire in one compartment from affecting the operation of cables in adjacent compartments/ducts.

For the specific BWR-6 design used in this probabilistic analysis, Safe Shutdown can be achieved using either Division I or Division II. In this assessment, it is assumed that Alternative Shutdown capability for the plant is provided by the Division I Safe Shutdown systems.

While this probabilistic analysis is used here specifically for a BWR-6 designed plant, the same methodology can be used for other plant designs. In fact, the outcome of the risk assessments that have been performed for other design types have demonstrated comparable results.

B.5.1 DISCUSSION

The event selection is based on evaluation of considerations in IN 92-18, as they relate to potential loss of Safe Shutdown capability. This loss is predicated on mechanistic damage to MOVs in the train of components used to perform Post-Fire Safe Shutdown from outside the Control Room, following evacuation. For this evaluation, this represents the ESF Division I compliment of Alternate Shutdown MOVs. The mechanism that damages the MOV is a sustained "Hot short" between certain specific conductors in the MOV circuitry, such that the torque/limit switches do not terminate motor energization at the end of the valve stroke. Thus, the valve actuator may ultimately be damaged to the extent that future use of the valve from the Alternate Shutdown station is precluded. Note that this failure mechanism does not exist following the transfer of controls to the Alternate Shutdown stations. Therefore, the period of interest is the interval from fire initiation until transfer. If transfer occurs prior to MOV damage, the scenario does not adversely impact Post-Fire Safe Shutdown using Division I. The specific subset of cabinets that contain Division I MOV circuits used for Alternate Shutdown and Division II circuits for the plant represented are: P601, P701, and P870. Panels P601 and P870 are benchboard cabinets and panel P701 is a termination cabinet.

The Control Room used for this specific evaluation has a floor area of 8602 ft^2 and a multi-level ceiling. The area above the main control panels (approximately 1275 ft^2) has a ceiling height of 21 ft. and the remaining areas have a suspended ceiling with a height of 8.5 ft. It has three principal sub-compartments, an under floor area containing cable, the normally occupied area containing the controls for the plant and the area above the suspended ceiling. The under floor area is protected by an automatic halon system. The remainder of the control room has detectors in every cabinet except P680, which is the console at which an operator normally sits.

B.5.1.1 Evaluation

Control Room Cabinet Fire Frequency

The base fire initiation frequency for an individual cabinet is determined by the following equation:

$$F_{Cab} = F_{CR} / n_{Total} \qquad Equation\ 1$$

where,

F_{Cab} = *frequency individual cabinent fire*

F_{CR} = *frequency of control room fires*

n_{Total} = *Total number of cabinents in Control Room*

Ignition Frequency Factor

Equation 1 implies that all cabinets are alike. However, some types of cabinets contain less fire initiating components than others. Benchboard cabinets contain fewer relays and circuit cards than control panel cabinets. Termination cabinets contain no relays and circuit cards. Therefore, to accurately represent the individual cabinet fire initiation frequency, it is necessary to develop an ignition frequency factor (IFF).

From Reference B.6.1, the eleven electrical cabinet fires in the EPRI Fire Events Data Base can be categorized as caused by the following:

- relays - 6 incidences
- circuit boards - 3 incidences
- other - 2 incidences

As discussed above and confirmed in walkdowns for the plant used in this evaluation, the principal causes of cabinet fires, relays and circuit cards, do not apply to termination cabinets. A visual inspection of panels containing all three divisions indicated that P601 was lightly loaded with relays and circuit cards and that P680 had no relays but a light to moderate load of circuit cards. Based on this, the control benchboard panels (P601, P864, P870 and P680) were assumed to have a lighter load of circuit cards and relays. The fire ignition frequencies for the three types of cabinets were weighted based on the following assumptions and relationships:

- All fire types apply to control panels ($IFF_{Control\ Panel}$ = control panel ignition frequency factor)
- Only the "other" fires apply to termination cabinets ($IFF_{Term\ Cabinet}$ = 2/11 * $IFF_{Control\ Panel}$, where $IFF_{Term\ Cabinet}$ = termination cabinet ignition frequency factor).
- The relay and circuit card loading of control benchboard panels and therefore the fire initiation frequency is assumed to be 1/4 that of control panel cabinets ($IFF_{Benchboard}$ = 1/4 * $IFF_{Control\ Panel}$, where $IFF_{Benchboard}$ = control benchboard panel ignition frequency factor)

Equation 2a

$$IF_{CR} = n_{total}(IF_{Aver})$$

Equation 2b

$$n_{T\,otal} = n_T\left(IFF_{Term\,Cabinet}\right) + n_P\left(IFF_{TermCabinet}\right) + n_{Bb}\left(IFF_{Benchboard}\right)$$

$$IF_{CR} = n_T\left(IFF_{Term\,Cabinet}\right)\left(IF_{aver}\right) + n_P\left(IFF_{Control\,Panel}\right)\left(IF_{aver}\right) + n_{Bb}\left(IFF_{Benchboard}\right)\left(IF_{aver}\right) = n_{Total}\left(IF_{aver}\right)$$

where:

$\therefore$ $IF_{CR} = frequency\,of\,control\,room\,fires$

$IF_{aver} = average\,CR\,cabinet\,\,frequency$

$n_T = number\,of\,ter\text{mination}\,cabinets\,(15)$

$n_P = number\,of\,\,control\,\,panels\,(39)$

$n_{Bb} = number\,of\,control\,benchboards\,(4)$

$n_{Total} = number\,of\,\,CR\,cabinets\,(58)$

Substituting into Equation 2b and determining the IFF by cabinet type:

$(15 * IFF_{TermCabinet}) + (9 * IFF_{Control\ Panel}) + (4 * IFF_{Benchboard}) = 58$

Substituting $IFF_{Term\ Cabinet} = 2/11 * IFF_{Control\ Panel}$ and $IFF_{Benchboard} = ¼\ IFF_{Control\ Panel}$:

$15(2/11)\ IFF_{Control\ Panel} + 39\ IFF_{Control\ Panel} + 1(1/4)\ IFF_{Control\ Panel} = 58$

Solving for $IFF_{Control\ Panel} = 1.357$

Substituting $IFF_{Term\ Cabinet} = 2/11 * IFF_{Control\ Panel}$

$IFF_{Term\ Cabinet} = 0.247$

Substituting $IFF_{Benchboard} = ¼\ IFF_{Control\ Panel}$

$IFF_{Benchboard} = 0.339$

Severity Factor

In order for the defined scenario to progress, the fire must be of sufficient size so that it affects both divisions within the cabinet. Even though multiple divisions are contained in the cabinets of interest, there are some physical boundaries to the spread of fire within the cabinet. The different divisions within a cabinet are separated by a single interior wall. The walls may or may not contain small openings, but when openings are present, only a few cables pass through the wall.

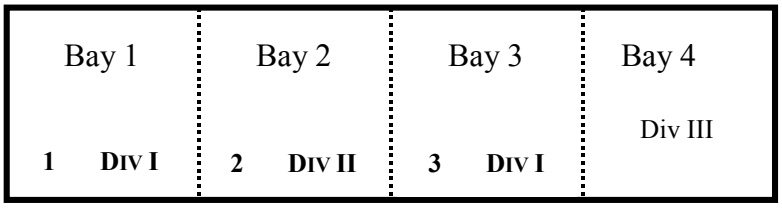
It is apparent that a fire must attain some finite level of severity for it to damage both divisions within a cabinet. Reference B.6.2 provides an estimate for the fraction of control room cabinet fires (from EPRI Fire Event Database) that were severe. The definition of severe fire for this purpose is one that could have caused damage beyond the ignition source, that is, one causing damage to other wiring or adjacent cabinets prior to being extinguished. Based on the review of actual control room fires from the EPRI Fire Events Database, Reference B.6.2 recommends a factor of 0.2 for the fraction of control room cabinet fires that are severe. The remaining fraction of fires (0.8) would be considered non-severe and therefore would only result in the failure of a single division. Therefore, the severity factor, F_{Severe}, is equal to 0.2.

Physical Configuration Factor

As noted in the definition of the scenario of interest, a fire must damage both Divisions I and II. Since the different electrical divisions are primarily segregated into separate bays in the cabinets of interest, this means that once a fire originates in one bay it must progress to another bay so that both Divisions I and II are damaged. Therefore, the physical configuration of the bays within a cabinet has a bearing on whether or not the conditions required for the scenario are possible. This is consistent with the definition of a severe fire from Reference B.6.2. A severe fire can either damage other wiring away from the point of initiation or damage circuits in the adjacent cabinet, or in the case of a GE PGCC cabinet, an adjacent bay. This potential will be characterized through the use of a configuration factor (F_{Config}) for each cabinet.

P601

The physical configuration of benchboard panel 601 is depicted in the following figure. As shown, the panel has four separate bays, two with Division I and one each for Divisions II and III.



P601

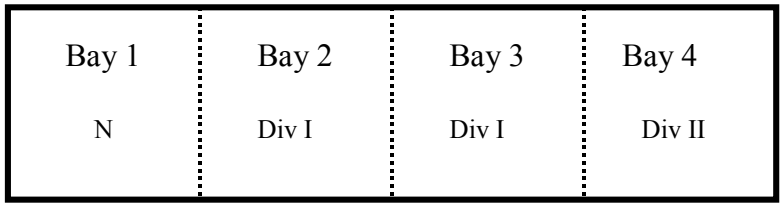
The figure indicates that each bay is primarily a single division. In the case of P601, Bays 1, 2 and 3 also contain circuits from the other division (either I or II). These circuits are contained in totally enclosed raceway and isolation cans specific to their division. No credit will be taken for protection due to these enclosed raceways and isolation cans, and it will be conservatively assumed that a severe fire in one these bays will damage both divisions. The following table identifies all of the potential outcomes of a fire originating in each individual bay.

Fire Originates in Bay	Potential Outcomes	Divisions Affected	Affects Divisions I and II?
1	Fire remains in Bay 1	I & II	**Yes**
	Fire progresses to Bay 2	I & II	**Yes**
2	Fire remains in Bay 2	I & II	**Yes**
	Fire progresses to Bay 1	I & II	**Yes**
	Fire progresses to Bay 3	I & II	**Yes**
	Fire progresses to Bays 1 & 3	I & II	**Yes**
3	Fire remains in Bay 3	I & II	**Yes**
	Fire progresses to Bay 2	I & II	**Yes**
	Fire progresses to Bay 4	I, II & III	**Yes**
	Fire progresses to Bay 2 & 4	I, II& III	**Yes**
4	Fire remains in Bay 4	III	No
	Fire progresses to Bay 3	I, II & III	**Yes**

There are a total of 12 different potential outcomes. Eleven of the outcomes result in damage to both Divisions I and II. Therefore, $F_{Conf\ P601}$ = 11/12 or 0.917.

P701

The physical configuration of termination panel 701 is depicted in the following figure. It has four separate bays, two with Division I and one each for Division II and non-safety related circuits (N).



P701

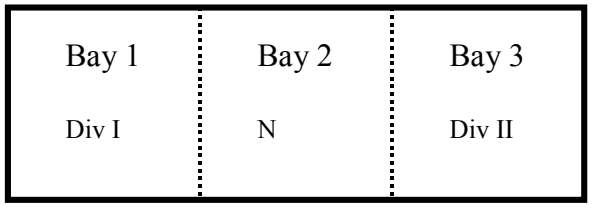
The following table identifies all of the potential outcomes of a fire originating in each individual bay.

Fire Originates in Bay	Potential Outcomes	Divisions Affected	Affects Divisions I and II?
1	Fire remains in Bay 1	N	No
	Fire progresses to Bay 2	N & I	No
2	Fire remains in Bay 2	I	No
	Fire progresses to Bay 1	N & I	No
	Fire progresses to Bay 3	I	No
	Fire progresses to Bays 1 & 3	N & I	No
3	Fire remains in Bay 3	I	No
	Fire progresses to Bay 2	I	No
	Fire progresses to Bay 4	I & II	**Yes**
	Fire progresses to Bay 2 & 4	I & II	**Yes**
4	Fire remains in Bay 4	II	No
	Fire progresses to Bay 3	I & II	**Yes**

There are a total of 12 different potential outcomes. Only 3 of the outcomes result in damage to both Divisions I and II. Therefore, $F_{Conf\ P601} = 3/12$ or 0.25.

P870

The physical configuration of benchboard panel 870 is depicted in the following figure. It has three separate bays, one each for Division I, Division II, and non-safety related circuits (N).



P870

The following table identifies all of the potential outcomes of a fire originating in each individual bay.

Fire Originates in Bay	Potential Outcomes	Divisions Affected	Affects Divisions I and II?
1	Fire remains in Bay 1	I	No
	Fire progresses to Bay 2	N & I	No
2	Fire remains in Bay 2	N	No
	Fire progresses to Bay 1	N & I	No
	Fire progresses to Bay 3	N & II	No
	Fire progresses to Bays 1 & 3	I, II & N	Yes
3	Fire remains in Bay 3	II	No
	Fire progresses to Bay 2	II & N	No

There are a total of 8 different potential outcomes. Only one of the outcomes result in damage to both Divisions I and II. Therefore, $F_{Conf\ P870} = 1/8$ or 0.125.

Probability of Hot Short

One other additional factor must be considered to satisfy the scenario of interest. The fire must cause a sustained hot short in a Division I motor operated valve (MOV) control circuit that causes damage to either the valve or motor operator. Even with a severe control cabinet fire (i.e., one that damages both Division I and II) but with no hot short, safe shutdown capability is maintained because of the ability to transfer control from the Control Room to the Remote Shutdown Panel. Therefore, a hot short is required for the scenario to develop. From NUREG/CR-2258, "Fire Risk Analysis for Nuclear Power Plants" (Reference B.6.3), the conditional probability of a "short" occurring in a multiconductor cable containing both wires of concern given that the cable is fire damaged is estimated as a log-normal distribution with a mean value of 0.068. Therefore, the probability of a hot short, $P_{Hot\ Short,}$ is taken as 0.068. For this scenario, it will be conservatively assumed that it is the probability of a hot short that is sustained long enough to cause damage to an MOV. It is also necessary to assume that this is the

probability of a sustained, hot short that develops before the control room transfer switch is activated. This is considered a conservative value.

Individual Control Cabinet Fire Frequency

Given the above relationships, an individual control cabinet frequency for initiating the defined scenario can be developed. The overall frequency is defined as follows:

$$F_{Cab-IN9218} = IF_{Aver} \times IFF \times F_{Severe} \times F_{Conf\ Cab} \times P_{Hot\ Short} \qquad Equation\ 3$$

The fire ignition frequency for the control room is 9.5E-3/year, which essentially is the frequency of electrical cabinet fires. Therefore, IF_{Aver} is equal to 9.5E-3/year divided by the total number of cabinets (58) or 1.64E-4/year. The frequency for each of the cabinets of concern is developed below.

P601 (Benchboard Cabinet)

$F_{P601\text{-}IN9218}$ = 1.64E-4/year $\times$ 0.339 $\times$ 0.2 $\times$ 0.917 $\times$ 0.068

= 6.93E-7/year

P701 (Termination Cabinet)

$F_{P701\text{-}IN9218}$ = 1.64E-4/year $\times$ 0.247 $\times$ 0.2 $\times$ 0.25 $\times$ 0.068

= 1.38E-7/year

P870 (Benchboard Cabinet)

$F_{P870\text{-}IN9218}$ = 1.64E-4/year $\times$ 0.339 $\times$ 0.2 $\times$ 0.125 $\times$ 0.068

= 9.45E-8/year

Therefore, the total frequency of fires leading to an IN 92-18 scenario is the total of the contribution of these three cabinets. The total is 9.26E-7/year.

B.5.2 CONCLUSION

As indicated above, the frequency of occurrence of the events leading to the scenario of interest described in IN 92-28 is below 1.0E-6/year for each of the potentially affected cabinets in the plant that was analyzed for this study. This study was performed on one representative BWR-6 type plant. Comparable results have been obtained for similar analysis at other types of nuclear plants.

ANS-52.1-1983, "Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants," provides guidance for the identification of events that should be

considered for design. This standard establishes the nuclear safety criteria and functional design requirements of structures, systems, and components of stationary boiling water reactor (BWR) power plants. This standard, in Section 3.2.3, states that "If the frequency of occurrence of an event is shown to be <1.0E-6 reactor year on a best-estimate basis, this event shall not be considered for design."

Additionally, a value of <1.0E-6 per reactor year is consistent with NRC guidance on acceptable risk. Regulatory Guide 1.174, July 1998, which makes use of the NRC's Safety Goal Policy Statement, considers an increase in Core Damage Frequency (CDF) of less than 1.0E-6 per reactor year to be very small. While the results in this analysis consider only the initiation frequency and do not give a CDF result, it is conservative nonetheless, since calculation of CDF would incorporate credit for additional mitigating systems and activities.

Based on the extensive and deliberate consideration given to this issue, the industry has been unable to identify a high safety significance.

B.6.0 REFERENCES

B.6.1 Fire PRA Implementation Guide, Appendix M, Analysis of Control Room Fires, Science Applications International Corporation, EPRI TR-105928, December 1995.

B.6.2 Fire PRA Implementation Guide, Appendix D, Guidance for Estimating Fire Severity, Science Applications International Corporation, EPRI TR-105928, December 1995.

B.6.3 M. Kazarians and G. Apostolakis, "Fire Risk Analysis for Nuclear Power Plants," Washington, DC, United States Nuclear Regulatory Commission, NUREG/CR-2258, September 1981.

B.6.4 GE NEDO-10466-A, "Licensing Topical Report, Power Generation Control Complex, Design Criteria and Safety Evaluation," February 1979.

B.6.5 Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.

B.6.6 NRC Information Notice (IN) 92-18, "Potential for Loss of remote Shutdown Capability During a Control Room Fire."

B.6.7 NRC Inspection Manual, Manual Chapter 06XX – Significance Determination Process

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 which 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 may be more severe than a boil-off condition, 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 is 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:

- RCS to shutdown cooling system (e.g., RHR, DHR, etc.) suction valves.
- RCS letdown isolation valves (e.g., letdown to radwaste, condensate (BWRS), main condenser (BWRs) or volume control system (PWRs).
- 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 Reactor Pressure Vessel 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. 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.4.1 THREE PHASE AC POWER CIRCUIT

However, since GL 86-10 implied a limit on the potential combination of circuit failures for other non-High/Low components, 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 deenergized 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 normally 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.

C.4.2 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 probability of all of these faults occurring, without grounding causing fuses of the aggressor, or victim circuits to blow is highly unlikely. 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.

C.5.0 FIRE AREA ASSESSMENT OF HIGH/LOW PRESSURE INTERFACES:

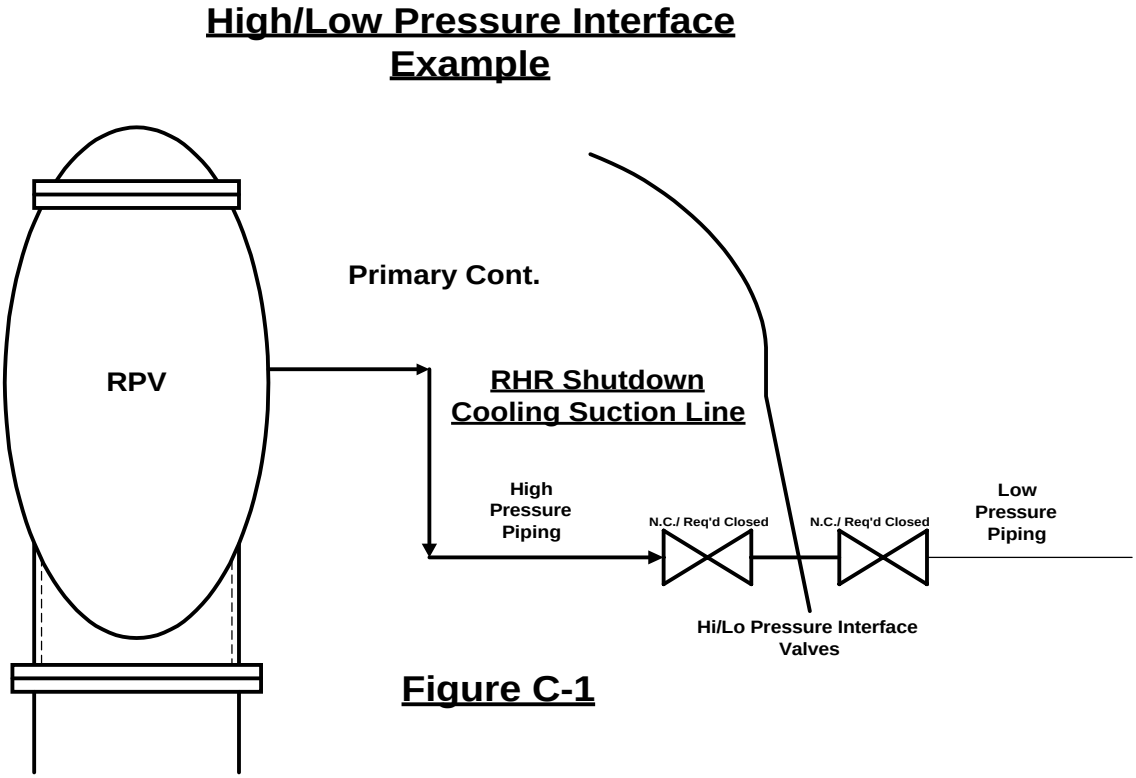


Figure C-1 Discussion for High/Low Pressure Interface Example -

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.

C6.0 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. 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 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.

This appendix provides information on those aspects of the methodology and guidance for Alternative/Dedicated Shutdown that are different form the methodology and guidance applied for redundant post-fire safe shutdown in the body of this document. Section D.3.0 provides an overview of 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 provides a description of the regulatory requirements for Alternative and Dedicated Shutdown. Section D.5.0 provides an itemization of 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 provides a listing of recommended additional operator actions that should be considered for use on a plant unique basis for fires requiring Control Room evacuation.

D.3.0 OVERVIEW

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, a basic assumption of the methodology used in the post-fire safe shutdown analysis for a Control Room fire is to assume that there will be fire damage to all of the systems and equipment located within the Control Room fire area. Additionally, it is assumed 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. Rather, it 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. 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 only conservative 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 reads as follows:

> 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

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. 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, which are not provided with transfer switches, each identified potential and credible spurious operation must be identified to determine if mitigating actions are required. 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, timing, lighting and tenability (accessibility) to ensure that an unrecoverable condition does not occur.

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 section 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 the body 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 the body of this document, depending on a plants licensing basis, Exemption Requests, Deviations Request and GL 86-10 Fire Hazards Evaluations with 50.59 Determinations 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 function 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, then an adequate level of safety is demonstrated 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. Either isolation transfer switches and redundant fusing unaffected by the fire or electrical and physical isolation and manual manipulation of equipment must be provided for all required equipment.

- 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

Industry believes that 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 actions believed to be of benefit. Licensees should be encouraged to identify actions that provide a positive benefit in terms of alternative post-fire safe shutdown and to include these in the governing procedures.

Industry recommends that the following actions 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 the action of performing a reactor scram/trip that is already endorsed for this event.

- Closing the Main Steam Isolation Valves.

- [BWR] Closing the Main Steam Drain Lines.

- Tripping the Feed Pumps and closing the Feed Pump discharge valves.

- [PWR] Closing the letdown isolation valves.

Performing 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, industry considers the following actions to be potentially useful as immediate operator actions for inclusion in the procedures governing shutdown at the emergency control station:

(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, they should be started immediately. In the event of a loss of offsite power, the Emergency Diesel Generators will 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, then the pump should be tripped. Performing this action as an immediate operator action upon arrival at the emergency control station will provide added assurance that these pumps will not be damaged.

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

MULTIPLE HIGH IMPEDANCE FAULTS

E.1.0 PURPOSE

The purpose of this appendix is to evaluate the need to consider multiple high impedance faults as described in Generic Letter 86-10 (Question 5.3.8) as part of post fire safe shutdown analysis. This appendix will be revised when the NEI/EPRI circuit failure characterization activities provide new information to address this issue.

E.2.0 INTRODUCTION

Generic Letter (GL) 86-10 (Question 5.3.8) requires that high impedance faults be considered for all associated circuits connected to safe shutdown power supplies. Simultaneous high impedance faults, as defined by GL 86-10, are fault currents below the trip points for the breakers on each individual circuit. Therefore, high impedance faults by definition do not result in clearing of the fault by the individual feed breaker. The GL requires that such faults be considered for all associated circuits located in the fire zone/area in the evaluation of the safe shutdown capability. The concern is that the summation of fault currents from such faults on both safe shutdown and non-safe shutdown loads could trip the main feed breaker for the affected safe shutdown power supply prior to the individual feed breakers clearing the faults. According to GL 86-10, circuit coordination studies are not required if it is assumed that safe shutdown capability will be disabled by such high impedance faults and appropriate procedures are provided for clearing the faults.

E.3.0 ANALYSIS:

The MHIF (Multiple High Impedance Faults) phenomenon, as postulated by GL 86-10, is based on the occurrence of multiple fire-induced HIFs within a short enough time period to collectively impact the feeder breaker to the bus. The electrical principals involved in this failure phenomenon show that if basic circuit coordination is established, the possibility of multiple high impedance faults is sufficiently low that it need not be postulated.

A fire induced fault occurs when the fire has caused sufficient damage to the cable insulation to allow leakage current to flow. The associated energy causes rapid localized heating, further damaging the insulation and establishing an arc. Due to the amount of energy dissipated to the insulation, the progression from leakage current to arcing fault occurs rapidly (less than 60 sec at 120 VAC levels - Reference E.5.5). The leakage current is extremely small prior to an arc developing. Therefore, the sum of many parallel leakage currents is not a concern. High impedance faults are only of concern when they have progressed to the arcing phase. The arcing fault can either self

extinguish, propagate to a bolted fault, or sustain itself depending on the voltage level and distance between arcing conductors. However, due to the speed with which arcing faults either self-extinguish or clear their breakers as a result of a bolted fault, it is not credible for multiple high impedance faults to occur simultaneously.

Medium Voltage Systems (4 kV and above)

MHIFs are not considered credible for medium voltage buses because at this voltage level postulated arcing faults will clear by one of two mechanisms. The fault current will rapidly propagate into a bolted fault, which will be cleared by the individual feed breaker; or the energy by the postulated fault will be sufficient to vaporize the target and break the fault current path.

Also, at this voltage level, phase-to-phase and three-phase arcing faults approach the magnitude of a three-phase bolted fault. Even if this fault remains an arcing fault, it would be cleared by the protective devices. Minimum arcing ground faults is not a concern at the medium voltage level because the individual feed breakers are provided with ground fault protection. Assuming coordination has already been demonstrated at the medium voltage level, no additional evaluations are required for MHIFs. Therefore, multiple high impedance faults at the 4 kV level and above are not considered credible.

480 Volt System:

High impedance (arcing) faults are credible at the 480 volt level. However, an arbitrary fault current, just below the feed breaker trip setting, is not credible. Research (Reference E.5.1) has shown that the minimum arcing fault, an arcing ground fault, will have a specific behavior. In the case of the arcing ground fault, the probable minimum rms value is 38 of the bolted three-phase fault value. If the fault value is less than 38%, then the fault will self extinguish. If it is greater than 38%, the energy of the fault will cause the fault to go to a condition close to a bolted fault.

Per Reference E.5.1, the minimum line-to-line arcing fault will be 74% of the bolted three-phase fault value, while the minimum three-phase arcing fault will be 89% of the bolted value. Therefore, demonstrating that the feed breakers will clear at 38% of the three-phase bolted fault will confirm that coordination is maintained with high impedance faults and MHIFs are not a concern. The nature of protective devices is such that it is unlikely to have coordination at 100% fault current without having coordination at 38% fault current. Therefore, MHIFs at the 480V level are not considered credible.

208/120 Volt System:

In theory an arcing ground fault cannot be sustained at the 208/120 voltage level. On 120V systems, MHIFs are not considered credible because at this voltage level postulated arcing faults will clear by one of two mechanisms. (1) the fault current will rapidly propagate into a bolted fault, which will be cleared by the individual feed breaker; or (2) the energy by the postulated fault will be sufficient to vaporize the target and break the fault current path. On 208V systems, neither the peak line-to-neutral voltage (1.41 x 120

= 170 V) nor the peak line-to-line voltage (1.41 x 208 = 295 V) exceeds the 375V restrike voltage (Reference E.5.1) required for an arcing fault.

Per Reference E.5.1, the restrike voltage is the voltage at which the spark gap begins to conduct and arcing current begins to build up. In practice however, not all 208V arcing faults are known to have been self-extinguishing; in particular, the three-phase variety. The minimum arcing faults on 208V systems will be 12% of a three-phase bolted fault for three-phase and 2% for line-to-line (Reference E.5.4). These minimum values are low enough to warrant following the guidance provided in Generic Letter (GL) 86-10, Question 5.3.8. However, the probability of having multiple sustained arcing faults without involving ground and without involving an open circuit at the 208V level is sufficiently low that these faults need not be considered. Therefore, MHIFs at the 208/120V level are not considered credible.

250/125 Volt DC System:

The issue of high impedance faults on DC systems is not considered credible because a DC fault will either develop into a full bolted fault or will self-extinguish. In order to establish a fault on a 125 VDC system the two conductors must be less than .075 inches in open air apart (Reference E.5.2). This distance is a safe working distance and would be smaller for an arc to start. Also, this distance would be smaller if there was insulation in the path. A 15 Amp breaker supplying 15A at 125 VDC will cause 1.8 kW to be dissipated at the point of the fault. This amount of energy being consumed in an arc of .075 inches or less will cause the conductor to melt. This will result in a bolted fault that will trip the breaker or will burn the wire open. Similar discussions can be made for the breakers up to 400A. The energy dissipated at the point of the fault is sufficient to melt the conductor. This will result in either a low impedance fault or an open circuit. A similar argument can be made for the 250 VDC system. Therefore, multiple high impedance faults at the 250/125VDC level are not considered credible.

E.4.0 CONCLUSIONS:

The BWROG's conclusions regarding multiple high impedance faults is as follows:

- At various voltage levels, multiple high impedance faults will not occur.
- At those voltage levels where high impedance faults are possible, the magnitude of the fault current is sufficient to operate the associated branch circuit interrupting devices or the probability of the fault is sufficiently low for it to not be of concern.
- In the event that a fire induced sustained arcing fault with insufficient current to actuate the associated circuit interrupting device occurs, the probability of even two such faults is sufficiently low to eliminate the need to evaluate the impact.

E.5.0 REFERENCES

E.5.1. IEEE Transaction on Industry Applications, Vol. 1A-8, No. 3, May/June 1972, "The Effects of Arcing Ground Faults on Low-Voltage System Design" by J. R. Dunki-Jacobs

E.5.2. NEMA ICS-1-1993 Table 7-2 "Clearance and Creepage Distance for Use Where Transient Voltage are Controlled and Known"

E.5.3. Generic Letter (GL) 86-10, "Implementation of Fire Protection Requirements"

E.5.4. "The Impact of Arcing Ground Faults on Low Voltage Power System Design", August 1, 1970, by J. R. Dunki-Jacobs

E.5.5. "Multiple High Impedance Fault Analysis and Resolution for Nuclear Power Facilities" - Proceedings of the American Power Conference, April, 1990, by H. Ovunc and P. Zavadivker

APPENDIX F

MANUAL ACTIONS AND REPAIRS

F.1.0 PURPOSE

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

F.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. To assure that the reliance on manual actions or repairs is appropriate, the following criteria are provided. 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.

F.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.

F.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, since the same considerations apply, whether an action is defined as a manual action or a repair.

F.5.0 DEFINITIONS

Manual Actions include the following:

Local Control: 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 Control: 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.

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

Repair Activity: Those actions required to restore operation to post fire safe shutdown equipment which 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.

F.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.

- 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) do not require outdoor battery backed lights.

- 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. 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 may become apparent that could have a positive benefit by either minimizing the shutdown transient, or by providing a degree of property protection, that are not specifically necessary to demonstrate compliance with Appendix R. It is acceptable to provide this information to the operators. 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 for a primary mitigating technique do not require 8-hour emergency lights, communications or timing considerations.

F.7.0 REFERENCES

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

APPENDIX G

COMBINED EQUIPMENT IMPACTS

G.1.0 OBJECTIVE

The purpose of this appendix is to evaluate the safety margins inherent in the "baseline" methodology described in Section 3.0 of the Generic Guidance for Post-Fire Safe Shutdown Analysis and the risk significance associated with the resolution of the NRC-Industry Issues related to multiple spurious signals and/or spurious operations.

NOTE: Appendix G will be revised to describe a generic screening approach which will be used to identify any additional combined equipment impacts that need to be included into the post-fire safe shutdown analysis (e.g. items similar to hi/lo pressure interface valves). The approach used to accomplish this will be risk-informed and will rely on information compiled in the IPEEE's. Through the application of the information in this appendix, the issue of multiple spurious signals and operations will be resolved either by identifying specific combinations of concern or by demonstrating on a generic basis that there are none with a sufficient likelihood of occurrence that would require their consideration.]

G.2.0 INTRODUCTION

Differences of interpretation have arisen between the NRC and the Industry related to consideration of combined (multiple) spurious signals and/or spurious operations that may adversely impact post-fire safe shutdown. The "baseline" methodology provided in the body of this document does not provide guidance for addressing these issues. It is the position of the industry that the guidance and methodology in the body of this document meets the regulatory requirements, provides an acceptable level of fire risk and results in a safe plant design. The basis for this position is documented in Section G.3.0, Safety Assessment, and Section G.4.0, Risk Insights.

The industry recognizes that the issues described above represent areas of concern to the NRC. In response to this, NEI is providing a discussion of the areas of NRC concern relating to combined failures/events and a generic risk and safety significance evaluation for these areas consistent with the revised Regulatory Oversight Process described in SECY 99-140.

Additionally, Section G.5.0, Regulatory Burden, describes the financial burden to plants should the NRC disagree with the basis outlined in this appendix for resolving these issues.

G.3.0 SAFETY ASSESSMENT

The "baseline" methodology contained in this document uses conservative assumptions relative to all aspects of fire protection defense-in-depth. The "baseline" methodology assumes that the fire occurs irrespective of ignition sources in the area. It assumes that the fire can damage all of the equipment and cables within the fire area irrespective of combustible loading or area geometry. It assumes that every single potential spurious operation or signal that could be induced by the fire occurs (one at a time). It assumes that no detection and suppression activities to limit the effects of the fire occur and that sole reliance is placed on passive barriers to prevent fire spread. Typically, the plant areas where post-fire safe shutdown analysis is performed could not have a fire of this magnitude or damage potential.

In reality, the likelihood of a large fire with the potential to damage plant equipment important to safe plant shutdown is considered to be small. If a fire were to occur, however, it is expected that it would be contained within a single electrical panel or a localized portion of one room or area. 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.

Based on current plant practices for control of combustible materials and ignition sources and the currently installed passive fire protection features, there is a very low probability that a fire would damage any plant equipment. When this fact is considered in conjunction with the current regulatory guidance for electrical separation contained in documents such as Regulatory Guide 1.75, the probability of a single fire damaging redundant safe shutdown equipment is considered to be extremely small.

Regardless of these facts, however, the methodology contained in the body of this document begins with the basic and extremely conservative assumption that any equipment or circuits in a fire area that are not protected from the effects of fire will be damaged and be unavailable to support plant safe shutdown. The methodology progresses by providing guidance on (1) selecting systems and equipment important to post-fire safe shutdown, (2) identifying the circuits of concern relative to these systems and equipment and (3) mitigating each fire-induced effect to these systems, equipment and circuits.

The application of this methodology in its "baseline" form, when considered in conjunction with the facts presented above regarding the potential for plant fires and damage to equipment in redundant divisions, results in a plant design basis that is safe from the adverse effects of fires.

G.4.0 RISK INSIGHTS

The need to consider combined equipment impacts can be assessed by reviewing the risk associated with a generic model depicting a worst-case condition for combined equipment impacts (see Figure G-1 for a pictorial description of the bounding analysis

model). Figure G-1 depicts two cables for two components both within the same cable tray. These two components could be two redundant parallel injection valves, two series flow diversion valves, or some other combined equipment impact configuration. It is postulated in this example that the cabling for these two components has the capability to cause an undesired spurious operation should it experience a hot short.

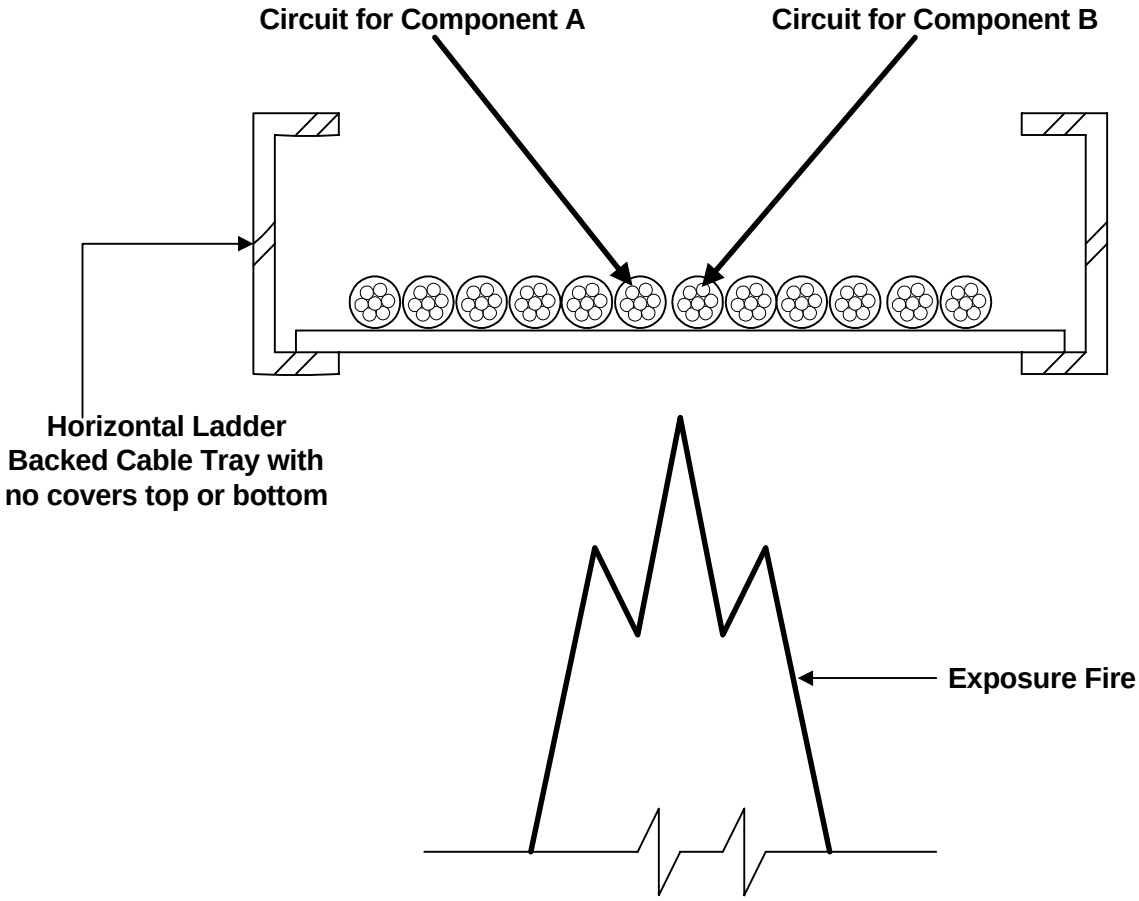


FIGURE G-1

The safety significance of this issue is a function of the likelihood of occurrence of this event and the consequences of the event. When evaluating the cases of a spurious opening of two series flow diversion valves or the spurious closing of two redundant parallel injection valves, it can be readily concluded that there are no adverse consequences associated with these events unless subsequent failures also occur. Therefore, by simply looking at the probability of occurrence of these types of events, a correlation can be made between relative safety significance and probability. Therefore, if the probability of occurrence is low, it can be concluded that the safety significance is not high.

Representative probability estimates for certain things would need to occur for an event such as those described above to take place are presented in Table G-1. The probability values used in this example should not be used as exact values, but rather as order of

magnitude values derived as best estimates using available industry information. Given the conservative model being assessed and the need for additional failures beyond those depicted in this example before adverse consequences would occur, the level of accuracy of these values is considered to be acceptable for the intended purpose of assessing the presence of an event with high safety significance.

Various ranges for fire event occurrence probability are shown in Table G-1. The sources of this information are the Fire Protection SDP, the EPRI FIVE Methodology and other values available in industry documents such as IPEEEs. The values for these occurrences must be multiplied together to represent the likelihood of a fire of sufficient magnitude to develop and involve multiple components or cables.

Similarly, a range of probability of "hot short" occurrence is provided, since this is the mechanism considered most likely to cause spurious signals or operations. Similarly, the probability of the 1st and 2nd hot shorts must be multiplied together to represent the probability of combined events. The value used for the probability of a hot short is currently under evaluation by both Industry and NRC personnel. The value used for the high side of the range is expected to be demonstrated to be quite conservative. This example represents a worst case configuration and bounds most plant applications and therefore, no plant specific evaluation will be necessary.

TABLE G.1

	High	Low
Probability of a fire event	3 E-2/yr	3 E-3/yr
Probability of a damaging fire	3 E-2/occurrence	3 E-3/occurrence
Probability of a "hot short"	6.8 E-2/occurrence	1 E-2/occurrence
Probability of 2nd "hot short"	6.8 E-2/occurrence	1 E-2/occurrence
Fire Brigade Effectiveness	6 E-1/occurrance	3 E-2/occurrance
Likelihood (~) of occurrence	2.5 E-6/yr	2.7 E-11/yr

These results indicate that the likelihood of occurrence of a fire event that damages the appropriate circuits for both components and causes a spurious operation of each is somewhere between 2.5 E-6 and 2.7 E-11 per year. These values represent values for occurrence of the event per year. Therefore, these values represent the point at which the availability of other core damage mitigating systems and actions would need to be evaluated. For the localized fire whose frequency of occurrence is consistent with the values provided on the high side of the range, the potential for damage to additional systems with inventory control capability is estimated to be at least two orders of magnitude lower.

These results fall within the range where a contribution to overall core damage risk is not considered significant. It can also be seen that by requiring even more events to occur in combination, the probability of occurrence becomes increasingly smaller. For areas containing automatic suppression, the values would fall even further. Similarly, routing of conductors in dedicated or even separate raceways would also reduce the likelihood of occurrence. Routing of circuits for these types of equipment in separate raceway separated by physical distance, or even fire zone or room boundaries, is the more likely configuration.

Based on the extensive and deliberate consideration given to this issue, the industry has been unable to identify a high safety significance. The industry, however, will review the output of the Nuclear Energy Institute Circuit Failures Issues Task Force as it relates to this issue and act appropriately regarding the risk significance of this issue. Any subsequent review, however, would be limited to the following combinations:

- Fire induced spurious opening of two series valves in the suction or discharge piping on the required safe shutdown systems being used for inventory control or decay heat removal which result in a flow diversion beyond the make up capability available.

- Fire induced spurious closure of two parallel valves in the suction or discharge piping on the required safe shutdown systems being used for inventory control or decay heat removal which results in a flow blockage beyond that which can be tolerated.

- Fire induced spurious signal to two instruments that directly result in a plant transient with more severe consequences than the fire induced spurious signals identified for the SRV Trip Units at River Bend.

These items were selected based on having the greatest potential to present a condition that impacts the stated goal for post-fire safe shutdown:

> "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."

While there exists an almost unlimited number of combinations of spurious operations that could be postulated, very few have the potential to result in an immediate and unrecoverable condition according to the following reasoning:

- The majority of possible combinations either (a) have no interaction with the safe shutdown capability, and therefore no adverse impact; or (b) are capable of being identified and mitigated before an unrecoverable condition occurs.

- A small number of combinations are associated with the ability to maintain the reactor coolant pressure boundary, and have already been provided with special mitigation criteria as High/Low pressure interfaces, thereby eliminating them from further consideration.

- Based on the discussion provided above, it is the industry's conclusion that any remaining combinations (if they exist) which could be postulated are of minimal safety significance.

G.5.0 REGULATORY BURDEN

The results of this evaluation did not identify a high safety significance for the issues addressed in this appendix. To complete a review of the specific limited combinations described above, expenditures on the order of several hundred thousand dollars could be incurred on an individual plant basis. In addition, an evaluation to address an unlimited and unbounded number of multiple spurious signals and/or spurious operations, would involve expenditures significantly in excess of this. The industry position relative to performing an unlimited unbounded analysis of spurious signals and actuations is as follows:

- Performing such an analysis, addressing all possible permutations and combinations, is probably not possible.

- Assuming that it could be done, the cost to each plant would be in the multi-million dollar range.

- Performing such an exercise would not identify significant contributors to CDF and provide no increase in plant safety.

G.6.0 REFERENCES

G.6.1 NRC Inspection Manual, Chapter 06XX – Significance Determination Process

G.6.2 Fire Induced Vulnerability Evaluation Methodology (FIVE Plant Screening Guide) Enclosure 1 to NUMARC letter from W. Rasin, December 19, 1991.

G.6.3 NRC Regulatory Oversight Process SECY 99-140

G.6.4 NRC Regulatory Guide 1.75.

APPENDIX H

Circuit Failures of Concern

To be supplied from EPRI work

APPENDIX I

PLANT-UNIQUE RISK ASSESSMENT APPROACH

I.1.0 INTRODUCTION

As noted in the introductory section, the specific approach employed in addressing fire-induced circuit failure and the potential spurious actuations varies from licensee-to-licensee. It is likely that a number of licensees have already sufficiently addressed the technical issues described in this document. If so, it makes little sense to perform an additional review. The guidance in Section I.3.1 is intended to assist licensees in determining what, if any, reanalysis should occur.

Difficulties in interpreting NRC requirements and regulatory guidance, along with numerous variations in plant design, have resulted in plant-specific post-fire safe shutdown analysis approaches. Some of these approaches are based on long-held industry interpretations of regulations that differ from the NRC staff interpretations expressed in their letter to NEI of March 11, 1997.

As the industry moves forward, a greater emphasis is being placed on risk-informed methodologies such as those used in the on-line maintenance and outage risk management areas. NRC has indicated its receptivity to a risk-informed industry proposal for resolving the circuit failures issues. Industry is proposing this risk-informed approach for addressing circuit failure issues, which integrates the deterministic approach proposed by the BWR Owner's Group on November 15, 1999, with circuit failure characterization and probabilistic elements developed by the NEI Circuit Failures Issue Task Force.

I.2.0 OBJECTIVE

This document presents a method for licensees to determine the safety significance of concurrent spurious actuations, and potential fire-induced circuit failure modes indicated in Information Notice 92-18. If the user determines that additional measures are needed to prevent or mitigate the consequences of the spurious actuations, this method can also be used to ensure the cost-effectiveness of these measures.

This method, including the documentation of its use and any additional measures taken to address its results, should constitute an acceptable method for resolving these circuit failure issues.

I.3.0 METHOD

I.3.1 NEI 99-05 QUESTIONS TO TRIGGER METHOD USE

- Level 1: Did previous inspections or assessments address NRC concerns related to circuit failure issues, specifically Information Notice 92-18 failure modes and multiple spurious actuations? [If no, consider Level 2 assessment]

- Level 1: If the answer to the previous question is yes, did the inspection or assessment determine that the plant positions on these issues have been reviewed and accepted explicitly by the NRC? [If no, consider Level 2 assessment]

- Level 2: Has the NRC explicitly approved the plant treatment of multiple spurious actuations and IN 92-18 failure modes? [If yes to both, questions D.15 and D.16 are not applicable]

- Level 2: Did the safe shutdown analysis, or subsequent analyses, determine the impact of multiple concurrent spurious actuations, or of IN 92-18 failure modes, for components not related to high/low pressure interfaces? [If no to either, consider use of the forthcoming industry risk-informed method for addressing circuit failures issues]

- Level 2: Would the previous analysis of the impact of multiple concurrent spurious actuations, or of IN 92-18 failure modes, benefit from review using the forthcoming industry risk-informed method for addressing circuit failures issues?

I.3.2 GENERAL DESCRIPTION

This screening method evaluates the likelihood and consequences of concurrent spurious actuations, and IN 92-18-type fire-induced spurious actuations that could result in irrecoverable damage to valves because of bypassing valve motor protective devices. The criteria for determining risk significance are

- Whether the core damage frequency (Δ CDF) for each component (or component pair) for any fire area is less than 1E-7 per reactor year, and

- Whether the Δ CDF for each component (or component pair) is less than the Regulatory Guide 1.174 guideline of 1E-6 per reactor year for the sum of all fire areas where the component or component pair has power, control, or instrument cables

If a component or component pair screens out of a single fire area based on the first criterion, they must still be evaluated for all fire areas where the component or component pair has power, instrument, or control cables. If the component or component pair screens out for some areas but not for the total of all areas, the screened out areas may be dropped from further consideration.

The analysis involves a phased approach that successively multiplies the previously calculated risk factors by new ones at each phase, and compares the Δ CDF against the 1E-7 criterion. This allows the option of stopping the analysis at any phase where the Δ CDF or probabilistic contributors thereto have been determined to be "insignificant" because they are less than 1E-7 per reactor year.

Regulatory Guide 1.174, Figure 3, "Acceptance Guideline for Core Damage Frequency," also illustrates the concept of relative risk measure; that is, the Δ CDF of importance is based on the baseline CDF.

Before any component or component pair is screened out, SM (safety margins) and DID (defense-in-depth) degradations are considered in accordance with Regulatory Guide 1.174. The SM and DID evaluation guidance currently being developed for NFPA 805 may also be useful.

If, when all evaluation phases are completed, the Δ CDF remains greater than or equal to 1E-6 per reactor year, further actions to address the results of the analysis will be evaluated consistent with appropriate regulatory guidance. The complexity of possible corrective measures can be kept to a minimum by defining the additional risk reduction needed to render the Δ CDF less than I E-7 (1E-6) per reactor year. As an example, if a potential spurious actuation has been determined to have a Δ CDF of 1E-5 per reactor year after completing the screening process, a corrective action which applies an additional reduction factor of at least 10 would result in an acceptable configuration.

These screening steps 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.

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

F_f = fire frequency
P_E = fire size parameter
P_{SA} = probability of spurious actuations
P_{AS} = probability automatic suppression will not control the fire
P_{DM} = probability of failure of detection and manual suppression to control the fire
P_{CCD} = conditional probability of core damage given fire-induced spurious actuations

These are generic definitions; a more precise definition is provided at the screening step where each appears.

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 pairs, this calculation is performed for that component pair in each fire area

where power, control, or instrument cables for both components are run, and the results are summed for all such areas.

The initial focus of the assessment methodology contained within this document for IN 92-18 type failures is the Control Room. This is the area of the plant with the largest population of circuits from both divisions in the closest proximity to each other. As such, if this area can be demonstrated to have low safety significance, then the remaining plant areas could be considered to be less of a concern. Additionally, any modifications performed on Control Room circuits to alleviate IN 92-18 issues will not eliminate them, but will rather relocate them to an alternate location in the plant.

Although Control Room fires are the initial focus for IN 92-18 evaluations, it is appropriate to evaluate fires in other locations for IN 92-18 failure modes. Plants should consider the extent to which they perform such evaluations.[a]

I.3.3 STEP-BY-STEP ANALYSIS

I.3.3.1 Selection

This selection process builds on prior deterministic circuit analysis work. Configurations are defined in this selection step for both BWR and PWR plants. Industry expects to provide additional considerations for PWR plants in this guidance document.

1. Select target components (or combinations of two components for multiple spurious actuation evaluations) which could impact safe shutdown to be evaluated. This first step limits consideration of multiple spurious actuation evaluations to pairs with immediate and direct consequences comparable to high/low pressure interface failures. 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.

2. Apply this method to selection of safe shutdown equipment, their associated target cables, and the physical location of target cables. These steps are accomplished by completing steps 3.1.3.1 through 3.4.2.5 of the guidance document for the components and fire areas in question.

3. For IN 92-18 evaluations, determine the type of actuator for these valves. Bistable relays require only a momentary signal to drive the valve open or closed; other types require a sustained signal. If bistable relays are not employed in the control circuitry, determine the length of time it takes for the valve to open or close given an actuation signal.

[a.] At a later date, NEI will provide criteria in this guideline to assist plants in determining whether such evaluations should be considered.

4. If potential circuit failures in any of these target conductors are addressed by the deterministic mitigation techniques in this guidance, then no further analysis is needed.

I.3.3.2 Screen One

The purpose of Screen One is to quickly and qualitatively determine the safety significance of the component failure(s) in question, regardless of the likelihood of occurrence. This significance results from the adverse failure mode of this component(s). The method outlined below is one way to do this.

5. Use Table 1 to qualitatively determine the risk significance of a postulated fire capable of causing these failure modes. The qualitative criteria used for the screening are based on an event tree analysis of bounding quantitative estimates of the parameters in the probabilistic formula above, considering plant specific features. This event tree is provided in Appendix A. The criteria for risk significance are based on Reg Guide 1.174 guidance.

   The numbers in Table 1 represent the number of risk reducing activities (represented by parameters of the probabilistic formula) that would need to be deterministically credited for evaluated components in order to screen out that component(s) from further analysis. The fire frequency ($\mathbf{F_f}$) is defined as "The frequency of fires with a potential to damage critical equipment if left alone." The probability of spurious actuation ($\mathbf{P_{SA}}$) is defined as "The probability of undesirable spurious actuation(s) of the component or component pair. 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 form a momentary spurious signal)."

   Criteria for evaluating high, medium and low for $\mathbf{F_f}$ and $\mathbf{P_{SA}}$ are provided in Table 2. Criteria for crediting detection, suppression, and safe shutdown features are provided in Table 3.

   Several examples:

   a. If for evaluated components $\mathbf{F_f}$ is qualitatively judged to be low and $\mathbf{P_{SA}}$ is judged to be low, no further screening is required. Explained in another way, the combination of a low fire frequency and a low spurious actuation probability given a damaging fire makes it very unlikely that unacceptable consequences (concurrent spurious actuations or IN 92-18 type damage) will result.

   b. If for evaluated components $\mathbf{F_f}$ is qualitatively judged to be medium and $\mathbf{P_{SA}}$ is judged to be medium, the components 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 deterministically as

effective. Explained in another way, a medium fire frequency and a medium spurious actuation probability given a damaging fire will require at least two other mitigating factors (such as automatic detection and suppression, and protected safe shutdown equipment) to be credited deterministically to prevent the unacceptable consequences.

c. If for evaluated components $\mathbf{F_f}$ is qualitatively judged to be high and $\mathbf{P_{SA}}$ is judged to be high, the remainder of this probabilistic screening analysis must proceed at least to Screen Two in order to screen out the component. Explained in another way, if both the fire frequency and the spurious actuation probability given a damaging fire are high, one cannot rule out unacceptable consequences at this stage without detailed probabilistic analysis.

Components or component pairs which do not screen out in Screen One may be addressed in Screen Two.

I.3.3.3 Screen Two

The purpose of Screen Two is to screen out potential spurious actuations based on fire frequency times a spurious actuation conditional probability. The spurious actuation conditional probability will be available from the generic expert panel process described in Appendix B, and assumes a fire size based on a conservatively realistic evaluation of combustibles and initiators (no fire modeling). The spurious actuation probabilities reflect this conservative fire size, which may or may not be large enough to cause significant damage to cable insulation.

6. Using the fire initiator data (to be provided), determine $\mathbf{F_f}$ for each fire area evaluated. The fire size and location assumed in this step is one that results in extensive cable insulation damage and can be located anywhere in the fire areas.

7. Determine the characteristics (combustible types and potential initiators) of the fire areas where the target conductors are located.

8. Using the fire hazards analysis, determine a reasonable and conservative fire size, duration, and energy level (without using detailed fire modeling codes) in the vicinity of the components. This involves consideration of fixed and transient combustibles and ignition sources.[b.]

9. For the fire determined in Step 8, assign a fire size parameter ($\mathbf{P_E}$) based on the results of the generic expert panel process described earlier. $\mathbf{P_E}$ will be developed separately from $\mathbf{P_{SA}}$ during this expert panel process.

[b.] At a later date, NEI will provide criteria in this guideline to assist plants in making this determination.

$\mathbf{P_E}$ effectively revises the frequency of the Step 6 fire (which can occur anywhere in the fire area and be of any size) to the frequency of a Step 8 fire which has a more specific location and realistic energy level. $\mathbf{P_E}$ reflects the facts that (1) the probability of a fire in a specific location is less than the probability of a fire anywhere in the fire area, and (2) below some fire energy threshold the likelihood of insulation damage is very small.[c.]

10. Select the appropriate $\mathbf{P_{SA}}$ value from those developed for several base cases during the expert panel process described earlier. These base cases will reflect the range of possible cable configurations in the plant.

11. If $\mathbf{\Delta\ CDF = F_f\ *\ P_E\ *\ P_{SA}} < 1E\text{-}7$ per reactor year for the component(s) in the fire area, and < 1E-6 for all fire areas, screen this component from further review if SM and DID considerations permit.

I.3.3.4 Screen 3

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

12. Determine whether automatic suppression capabilities available in the area are adequate to restrain the fire ($\mathbf{P_{AS}}$). This evaluation should qualitatively consider the characterization of the area, type of the fire (fire with significant smoke generating capability before generating a lot of heat versus other fires), design features of the detection and suppression equipment available in the area, the design requirements committed to by the licensee, and the time available before fire severity reaches unacceptable levels.

13. Calculate the probability that automatic detection and suppression systems do not prevent undesirable consequences to the cables ($\mathbf{P_{AS}}$), using established fire PSA techniques for automatic detection and suppression systems. These techniques are described in EPRI documents such as NSAC-179L, the FIVE method, and the PRA guide. Quantitatively, the analyst should determine the reliability, unavailability, and effectiveness of the automatic suppression system(s) in the fire area.

    a. Obtain reliability values from NSAC-179L.

    b. Consider 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

[c.] Circuit failure test results will be used to establish thresholds and probabilities.

for the worst of the five years and use that value.

c. Sum the reliability and unavailability figures.

d. The system is considered effective if the criteria in Table 3 for automatic suppression are satisfied. If this is the case, $\mathbf{P_{AS}}$ = the value calculated in Step 12c. If not, $\mathbf{P_{AS}}$ = 1.0.

14. If $\mathbf{\Delta\ CDF = F_f\ *\ P_E\ *\ P_{SA}\ *\ P_{AS}}$ < 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.

I.3.3.5 Screen Four

The purpose of Screen Four is to apply the probability that manual suppression, and detection that supports fire brigade actions, will not control 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 suppressed prior to damage to cables that cause the spurious actuation(s) in question.

15. Calculate the probability that detection and manual suppression fail to extinguish the fire before cable damage thresholds are reached ($\mathbf{P_{DM}}$). This calculation is based on the time available for fire suppression before damage, and the time that is needed to suppress the fire (including fire brigade response time). Standard human reliability models such as HCR/IORE should be used to quantify $\mathbf{P_{DM}}$.

16. If $\mathbf{\Delta\ CDF = F_f\ *\ P_E\ *\ P_{SA}\ *\ P_{AS}\ *\ P_{DM}}$ < 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.

I.3.3.6 Screen Five

When Screen Four is complete, one has calculated the probability of two concurrent spurious actuations, or a single spurious actuation that could result in irrecoverable valve damage. The purpose of Screen Five is to determine the conditional core damage probability given the spurious actuation(s) have occurred.

17. This analysis may be performed using the internal events PSA to determine the CCDP (conditional core damage probability) for all available mitigation

systems, some of which may not have been credited in safe shutdown analyses. 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 4), then further analysis to address the value of potential recovery actions may be useful.

18. Determine whether systems not previously credited, and 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.

19. Using an internal events PSA analysis, determine the CCDP ($\mathbf{P_{CCD}}$) of the failure mode 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 PSA, 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.

20. If $\mathbf{\Delta\ CDF = F_f\ *\ P_E\ *\ P_{SA}\ *\ P_{AS}\ *\ P_{DM}\ *\ P_{CCD}}$ < 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.

I.3.3.7 Screen Six

The purpose of Screen Six is to use fire modeling techniques to recalculate $\boldsymbol{F_f\ *\ P_E}$ *for a realistic fire.*

21. Using accepted fire modeling techniques, determine the probability that a fire size, duration, and location sufficient to cause target conductor insulation damage will not develop.

22. Modify $\mathbf{F_f\ *\ P_E}$ using this probability to calculate a more accurate fire frequency

23. If $\mathbf{F_f\ *\ P_E\ *\ P_{SA}\ *\ P_{AS}\ *\ P_{DM}\ *\ P_{CCD}}$ < 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.

I.3.4 CORRECTIVE ACTION

If, when all evaluation phases are completed, the Δ CDF for a component or component pair remains greater than or equal to 1E-6 per reactor year for all fire areas, further actions to address the results of the analysis will be evaluated. The complexity of

possible corrective measures can be kept to a minimum by defining the additional risk reduction needed to render the Δ CDF less than 1E-7 per reactor year for any fire area. As an example, if a potential spurious actuation has been determined to have a Δ CDF of 1E-5 per reactor year for any fire area after completing the screening process, a corrective action which applies an additional reduction factor of at least 100 would result in an acceptable configuration. Any regulatory reporting should be in accordance with existing regulations.

I.3.5 DOCUMENTATION

The accurate and comprehensive documentation and preservation of documentation of this process is essential to the maintenance of a manageable and auditable Appendix R or BTP 9.5.1 (whichever is applicable) program. Appendix B criteria contained within 10CFR 50 specify the basic documentation requirements while the fire-related regulations contain more detail-specific expectations which will enable the licensee to maintain a compliant program and the NRC inspectors' ability to verify compliance over the life of the nuclear unit.

I.4.0 REFERENCES

I.4.1 Appendix R to 10 CFR 50
I.4.2 Branch Technical Position 9.5.1
I.4.3 NRC Generic Letter 86-10
I.4.4 NRC Information Notice 92-18
I.4.5 GE-NE-T43-0002-00-02, Rev 0 (BWROG Generic Guidance for Post-Fire Safe Shutdown Analysis)
I.4.6 NFPA 805 Draft 7.0
I.4.7 NSAC-179L
I.4.8 EPRI TR-100370, “Fire-Induced Vulnerability Evaluation (FIVE)”

Table 1

Screen One

	Fire Frequency		
Probability of Circuit Failures	**H**	**M**	**L**
H	Analyze	3 AS,DM,CCDP	2 AS,DM,CCDP
M	3 AS,DM,CCDP	2 AS,DM,CCDP	1 AS,DM,CCDP
L	2 AS,DM,CCDP	1 AS,DM,CCDP	OK

Table 2

F_f and P_{SA} Evaluation Criteria

Screen One 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 fires. These sources include: switchgears, ignition sources with liquid combustible or flammable such as larger pumps and compressors, non-dry-type transformers. For Example: • Switchgear room • Control room • ECCS	**Criteria:** The area has limited number of fixed ignition sources that have potential for damaging fires. The area has higher potential for transient fires due to maintenance activities in the area or its adjacent rooms. For Example: • Those cable spreading rooms with few, i.e., one or two electrical cabinets. • Battery room	**Criteria:** No fixed ignition such as pumps, electrical cabinets. Transient combustibles are administratively controlled with provisions for possible staging of combustibles during maintenance. For example • Cable tunnels with no fixed ignition source.
Probability of Spurious Actuation: Probability of undesirable spurious actuation(s) of the pair. Factors to be considered include; circuit design, e.g., normally energized circuits that are required to be de-energized, timing, e.g., a lock-in device that prevents damage from a momentary spurious signal.	**Criteria:** Spurious actuation of the pair requires likely conductor-to-conductor failures considering the factors that affect potential spurious actuation of the pair.	**Criteria:** Spurious actuation of the pair requires conductor-to-conductor failures considering the factors that affect potential spurious actuation of the pair.	**Criteria:** The spurious actuation of the pair requires two or more cable-to-cable hot shorts including 3-phase cables. (To be further clarified)

Bases for these criteria will be provided in a later revision to this document.

Table 3

Credit for Defense-In-Depth Elements

Defense–in-Depth Element for Screen One	Criteria for Crediting
Automatic suppression	Automatic suppression is credited when damage from important ignition sources can be prevented. This may be accomplished by either area-wide or local suppression systems on all important fixed ignition sources. If the cables for the pair are known to be protected by the automatic suppression system, suppression may be credited.
Detection and manual suppression	Manual suppression is credited when it can be demonstrated that all fires from important fixed ignition sources and transients in the area can be suppressed prior to damage to cables that cause spurious actuation of the pair.
Safe shutdown systems	Probability of safe shutdown is credited when it can be demonstrated that, given damage to the pair, equipment is available to prevent core damage. This can be demonstrated by ensuring that at least one division of safe shutdown equipment remains available including manual actions necessary to perform these functions. This may consider ability to restore equipment damaged by spurious actuation(s).

Bases for these criteria will be provided in a later revision to this document.