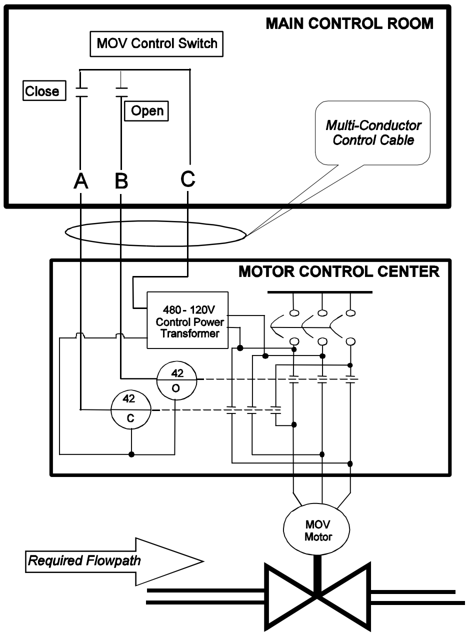
CHAPTER 6. DETERMINISTIC ANALYSIS PROCESS FOR APPENDIX R COMPLIANCE

The Browns Ferry event was of sufficient significance to warrant major changes in fire protection design features of NPPs in the United States. Consequently, the NRC issued its new regulation as 10 CFR 50.48 and Appendix R to 10 CFR Part 50, which became effective on February 17, 1981. One of the key requirements of this regulation was to backfit Section III.G, “Fire Protection of Safe Shutdown Capability,” to all NPPs that were licensed to operate before January 1, 1979. This section establishes the minimum acceptable fire protection design features that are necessary to ensure that licensees can achieve safe-shutdown in the event of fire in any area of the plant. The fundamental objective of Section III.G is to extend the DID concept to fire safety by obtaining reasonable assurance that, in the event a fire were to start (despite the fire prevention program) and continue to propagate (despite fire protection activities), one train of SSCs needed to achieve and maintain safe-shutdown conditions will remain available. Figure 6-1 illustrates how fire damage to circuits and cables may adversely affect the shutdown capability.



For the case shown above, a fire-induced short circuit between conductors “A “and “C” of the multi-conductor cable would have the same effect as placing the MOV control switch to the "Close" position. This would be unacceptable for safe shutdown since this MOV must remain open to allow shutdown system flow. For this circuit this failure mode could occur as a result of fire in the Main Control Room, the fire area where the MCC is located and any fire area between the MCC and Main Control Room where the multi-conductor controlcable may be exposed to fire damage.

Figure 6-1 Potential Effect of a Fire-Induced Circuit Failure

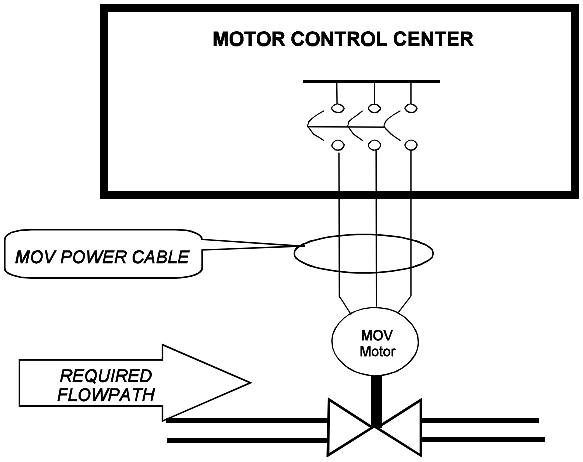
Section III.G required each licensee to perform a comprehensive evaluation of each fire area and demonstrate, through the performance of a deterministic assessment of potential fire damage, that SSCs of which failure (or maloperation) could impact the ability to achieve and maintain safe-shutdown conditions are provided with suitable fire protection features (i.e., as required by Section III.G.2 of Appendix R, or justified in a staff-approved exemption). For locations of the plant where compliance with the the fire protection design features specified in Section III.G.2 may not be feasible because redundant trains of cables and/or equipment are located in close proximity (such as the control room or CSR), Section III.G.3 requires licensees to provide an alternative or dedicated shutdown capability that is independent (both physically and electrically) from the fire area under consideration. In either case, the evaluation of a fire in any area must conclusively demonstrate that one train of equipment that can be used to immediately bring the reactor to hot shutdown conditions remains unaffected by fire.

6.1 Principles of a Deterministic Evaluation of Post-Fire Safe-Shutdown Capability

The SSA for each plant must specifically identify all systems and equipment upon which the licensee will depend to perform essential shutdown functions. It must also include an evaluation of any circuits or cables in the fire area that could (1) adversely affect the operability of identified shutdown systems and equipment or (2) initiate transients that could preclude the successful accomplishment of required shutdown functions by feeding back potentially disabling fault conditions to power supplies, control logic or instrumentation circuits. In addition, the SSA must describe how the licensee will prevent or appropriately mitigate such disabling conditions. Otherwise, the licensee cannot ensure its reliance on the identified safe-shutdown equipment. Because it is not possible to predict the manner in which equipment (cables, circuits or components) may fail, the SSA must assume that the fire will damage any unprotected equipment located in the fire area under evaluation and, unless otherwise demonstrated through the performance of more detailed evaluations, it must be assumed that this damage will fail the affected equipment in a mode that adversely impacts safe-shutdown. In summary, the NRC expects that such evaluations will be based on the following deterministic premise:

> *Cables and components that are exposed to the effects of fire and its related perils (i.e., not provided with fire protection features sufficient to meet Section III.G of Appendix R) will be damaged, and, unless demonstrated otherwise through the performance of suitably comprehensive and conservative engineering evaluations, it is assumed this damage will cause connected equipment to fail or malfunction in an undesired manner for shutdown.*

Not all circuit/cable failures that may occur as a result of fire will necessarily have an adverse impact on the plant's ability to achieve and maintain post-fire safe-shutdown conditions. The electrical distribution, instrumentation, communications, control, and process systems of a commercial NPP are composed of a diverse array of electrical circuits/cables, and fire damage to many (if not most) of these circuits will have no adverse effect on the ability to achieve and maintain safe-shutdown conditions. In certain instances, it may be possible to demonstrate, through the performance of a detailed analysis of the potential effects of fire damage, that even if a fire were to damage certain circuits of required shutdown components, the damage would be acceptable because it will not have any effect on the ability of the component to perform its intended shutdown function. For example, consider the circuit illustrated in Figure 6-2.



For this case, the MOV is "OPEN" during normal plant operations and must be assured to remain "OPEN" for post-fire safe shutdown (to allow fluid to flow in the required shutdown system). Since the MOV will fail in the "as is" position on loss of motive power, fire damage which results in a loss of power to the MOV would not impact the post-fire safe shutdown capability.

Figure 6-2 Fire Damage to Certain Circuits of Required Shutdown Equipment May Not Pose a Threat to the Shutdown Capability

In this case, an MOV is open during normal plant operations. To ensure successful achievement of safe-shutdown conditions, the MOV must remain open to allow fluid to flow through the required flowpath. For this case, the required shutdown component is an MOV which, by design, will fail in the "as-is" (open) position upon a loss of motive power. Therefore, if it can be shown that fire damage to the power cable would only result in a loss of motive power to the MOV, the analysis has demonstrated a level of safety equivalent to that which would be achieved through compliance with Section III.G.2, and the power cable would not require any additional fire protection features. As stated in the staff's clarification of GL 81-12, *"Our interest is only with those circuits (cables) whose fire-induced failure could affect shutdown."*

6.2 Use of "Appendix R" Terminology

Throughout this document, and particularly in this section, reference is made to post-fire safe-shutdown criteria contained in Sections III.G and III.L of Appendix R to 10 CFR Part 50. Since its inception, reference to "III.G.2" has become synonymous with redundant train shutdown capability, and "III.L" is commonly referred to when discussing alternative shutdown capability irrespective of the actual requirements specified in the plant's fire protection licensing basis.

In addition to simplifying the discussion, the use of such "Appendix R terminology" is generally acceptable because the guidelines contained in SRP Section 9.5.1 include the acceptance criteria listed in Appendix R to 10 CFR Part 50 and 10 CFR Part 50.48. It should be noted, however, that the use of this terminology is not intended to imply that Appendix R requirements are applicable to all plants. As described in Section 4, Appendix R is *only* specifically applicable to a limited number of plants that were fully licensed and operating before January 1, 1979. The staff typically reviewed the post-fire safe-shutdown capabilities of plants licensed after this date during the initial licensing process for conformance to guidelines contained in Position C.5.b of SRP Section 9.5.1.

6.3 Overview of the Post-Fire Safe-Shutdown Analysis Process

A comprehensive evaluation of the potential impact of fire damage on the ability to achieve and maintain safe-shutdown conditions within the performance goals and criteria specified in Appendix R to 10 CFR Part 50 is a technically challenging process, involving the expertise of personnel knowledgeable in plant operations and specialists from various engineering disciplines. There are many acceptable methods of performing a fire SSA, and the NRC neither prescribes nor endorses any one approach. The SSA should be a bounding analysis that identifies the range of possible fire impacts within each fire area and ensures that appropriate measures are in place to prevent this damage from affecting the ability to safely shut down the plant. For each fire area, the SSA will define the set of systems necessary to accomplish required shutdown functions in accordance with established performance criteria. The selected systems form the basis for the selection of individual components and cables needed to ensure that each system will be capable of accomplishing its intended shutdown function.

The detailed methods used by a particular plant operating organization will vary with plant-specific conditions, such as design, construction, cable configuration, equipment layout, and operating preferences. Therefore, it is not possible to develop a "one-size-fits-all" procedural process for performing a deterministic analysis sufficient to satisfy Appendix R concerns. However, the *overall approach* for ensuring the availability of at least one shutdown *"success path"* (i.e., the minimum set of SSCs necessary to achieve and maintain safe-shutdown in the event of a fire) for each fire area, is fairly consistent among plants regardless of plant design or vintage. Figure 6-3 illustrates an overview of this approach and provides references to the specific subsection of this chapter that describes each of the steps.

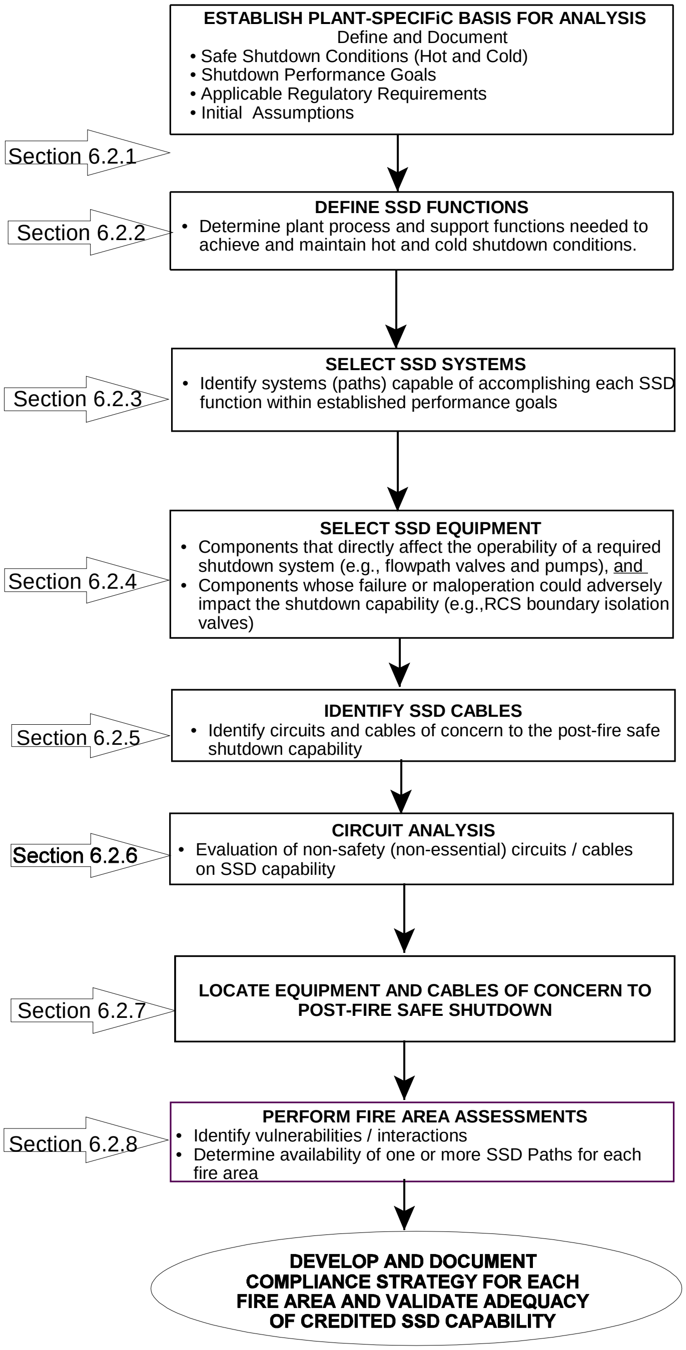

ESTABLISH PLANT-SPECIFiC BASIS FOR ANALYSIS
Define and Document
• Safe Shutdown Conditions (Hot and Cold)
• Shutdown Performance Goals
• Applicable Regulatory Requirements
• Initial Assumptions
Section 6.2.1
DEFINE SSD FUNCTIONS
• Determine plant process and support functions needed to achieve and maintain hot and cold shutdown conditions.
Section 6.2.2
SELECT SSD SYSTEMS
• Identify systems (paths) capable of accomplishing each SSD function within established performance goals
Section 6.2.3
SELECT SSD EQUIPMENT
• Components that directly affect the operability of a required shutdown system (e.g., flowpath valves and pumps), and
• Components whose failure or maloperation could adversely impact the shutdown capability (e.g.,RCS boundary isolation valves)
Section 6.2.4
IDENTIFY SSD CABLES
• Identify circuits and cables of concern to the post-fire safe shutdown capability
Section 6.2.5
CIRCUIT ANALYSIS
• Evaluation of non-safety (non-essential) circuits / cables on SSD capability
Section 6.2.6
LOCATE EQUIPMENT AND CABLES OF CONCERN TO POST-FIRE SAFE SHUTDOWN
Section 6.2.7
PERFORM FIRE AREA ASSESSMENTS
• Identify vulnerabilities / interactions
• Determine availability of one or more SSD Paths for each fire area
Section 6.2.8
DEVELOP AND DOCUMENT COMPLIANCE STRATEGY FOR EACH FIRE AREA AND VALIDATE ADEQUACY OF CREDITED SSD CAPABILITY

Figure 6- 3 Overview of Post-Fire Safe Shutdown Analysis Process

It should be noted that, for the purpose of this discussion, it is assumed that a comprehensive FHA has already been performed by qualified fire protection engineers to divide the plant into separate and distinct fire areas that are separated from other fire areas by rated fire barriers that are adequate for the anticipated fire hazard. As depicted in Figure 6-4, the fire area boundaries represent the extent of fire spread assumed in the SSA.

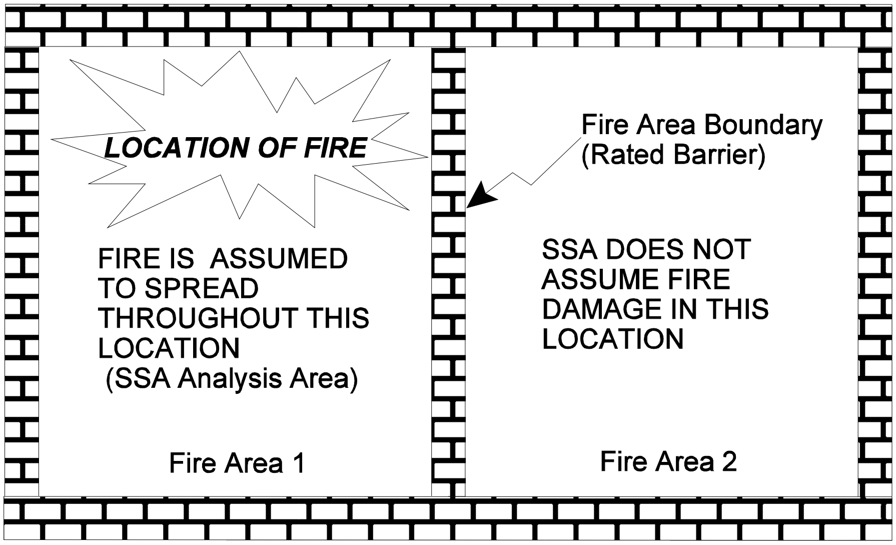

LOCATION OF FIRE
FIRE IS ASSUMED TO SPREAD THROUGHOUT THIS LOCATION (SSA Analysis Area)
Fire Area 1
Fire Area Boundary (Rated Barrier)
SSA DOES NOT ASSUME FIRE DAMAGE IN THIS LOCATION
Fire Area 2

Figure 6-4 Fire-Rated Boundaries Determine Extent of Fire Spread Assumed in SSA

6.4 Methodology

In demonstrating the plant's safe-shutdown capability, the SSA integrates the following evaluations:

(1) **Safe-Shutdown System Selection/Path Development** identifies systems that are capable of accomplishing shutdown safety functions (e.g., reactivity control, reactor coolant makeup, DHR, etc.).

(2) **Plant Configuration** compares equipment locations and cable routing with the fire area boundary information established in the FHA.

(3) **Safe-Shutdown System Performance** demonstrates that, following a fire, sufficient equipment of adequate capacity and capability will remain available to achieve and maintain the reactor in a safe-shutdown condition.

(4) **Associated Circuits Effects** demonstrates that a fire cannot, through its effects on nonessential/nonsafety electrical circuits, prevent safe-shutdown systems and equipment from accomplishing their intended functions or initiate an event that is beyond the capability of the safe-shutdown systems.

6.4.1 Establish the Plant-Specific Technical and Licensing Bases for the Safe-Shutdown Analysis

6.4.1.1 Assemble Plant-Specific Information

The first step in the SSA process is to review available documentation to obtain an understanding of the available plant systems and functions required to achieve and maintain safe-shutdown. The following documentation is typically needed to perform the SSA:

- *Fire Protection Licensing Basis Documents* include the FSAR, plant operating license conditions, TSs, applicable regulatory requirements (Appendix R or SRP Section 9.5.1), and fire protection safety evaluations issued by the staff.
- *Fire Hazards Analysis* identifies the fire areas, characterizes the hazards, and describes the fire protection features within each fire area.
- *Plant System Descriptions* are the detailed descriptions of the functions and capabilities of each plant system, including those systems capable of accomplishing the safe-shutdown functions. They should include both front line and support systems necessary for operation of the system. Support systems do not directly provide safety functions, but are required to ensure that the front line systems can perform the safety functions as required. Examples of support systems include cooling water, electrical power distribution, instrument air, and HVAC.
- *Plant System Design Drawings,* also known as piping and instrumentation diagrams (P&IDs), identify the components that make up a system and the flowpath of that system, and identify any interconnections to other systems that could degrade the system under certain fire damage conditions. Electrical drawings needed for review typically include electrical distribution one-line diagrams, cable block diagrams, logic diagrams, cable and raceway layout drawings, and instrument loop diagrams.
- *Applicable Operating Procedures* document the plant's normal, emergency, and abnormal operating procedures.

6.4.1.2 Define and Document Safe-Shutdown Conditions for the Plant

In order to develop an effective strategy for achieving and maintaining the reactor in a “safe-shutdown” condition, it is first necessary to define the plant-specific parameters that must be satisfied in order to declare that a “safe-shutdown” condition has been achieved. For fire events, safe-shutdown includes both hot shutdown and cold shutdown conditions. The plant’s TSs document the plant-specific parameters for each of these conditions.

6.4.1.3 Define and Document the Safe-Shutdown Performance Goals

Guidance for determining the functional and performance requirements of systems upon which the plant relies to accomplish both redundant (III.G.2) and alternative (III.L) shutdown was initially provided by the NRC in IN 84-09, “Lessons Learned from NRC Inspections of Fire Protection Safe Shutdown Systems.” Specifically, IN 84-09 states that the systems and equipment needed for post-fire safe-shutdown (*both* redundant and alternative) are those systems necessary to perform the safe-shutdown functions defined in Section III.L of Appendix R. Section III.L defines the acceptance criteria for such systems as follows:

- During post-fire safe-shutdown, the reactor coolant system process variables shall be maintained within those predicted for a loss of normal AC power
- 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).

By letter dated December 12, 2000 (Reference: Richards Letter) the staff documented its evaluation of a BWR Owners Group (BWROG) Fire Protection Committee position regarding the use of low-pressure injection systems as “redundant” shutdown systems under Appendix R. The staff position documented in this evaluation clarified the information initially provided in IN 84-09. Specifically, in its review of the applicability of Section III.L requirements, the staff concluded that *“Section III.L performance criteria are applicable only to alternative or dedicated shutdown capability, and need not be met for redundant post-fire safe-shutdown capability.”* As a result of the staff’s clarification of IN 84-09, RG 1.189 now defines performance criteria for shutdown systems as follows:

> **Regulatory Position 5.1 Safe-Shutdown Performance Goals for Redundant Systems**
> *“Ensure that fuel integrity is maintained and that there are no adverse consequences on the reactor pressure vessel integrity or the attached piping. Fuel integrity is maintained provided the fuel design limits are not exceeded*.”
>
> **Regulatory Position 5.2 *Alternative or Dedicated Shutdown Design and Performance Goals***
> ***5.2.1 Alternative or Dedicated Safe-Shutdown System Design Goals***
> *During the post-fire safe-shutdown, the reactor coolant system process variables should be maintained within those predicted for a loss of normal ac power, and the fission product boundary integrity should not be affected (i.e., there should be no fuel clad damage, rupture of any primary coolant boundary, or rupture of the containment boundary).*
>
> *The systems used for alternative or dedicated shutdown need not be designed to (1) seismic Category I criteria, (2) single-failure criteria, or (3) other design-basis accident criteria, except the portions of these systems that interface with or impact existing safety systems.*

> ***5.2.2 Safe-Shutdown Performance Goals for Alternative or Dedicated Systems***
> *The performance goals for the safe-shutdown functions should be:*
>
> - *The reactivity control function should be capable of achieving and maintaining cold shutdown reactivity conditions.*
> - *The reactor coolant makeup function should be capable of maintaining the reactor coolant level above the top of the core for BWRs and within the level indication of the pressurizer for PWRs.*
> - *The reactor heat removal function should be capable of achieving and maintaining DHR.*
> - *The process monitoring function should be capable of providing direct readings of the process variables necessary to perform and control the above functions.*

RG 1.189 further states that the capability of the required shutdown functions should be based on a previous analysis, if possible (e.g., those analyses in the FSAR). The equipment required for alternative or dedicated shutdown should have the same or equivalent capability as that relied on in the above referenced analysis. It should be noted that specific methods for achieving these objectives are left to the individual plants to determine and demonstrate.

6.4.1.4 Define and Document Initial Assumptions

In order to proceed with the analysis, it is necessary to establish a set of initial assumptions or "ground rules" that define the fundamental criteria and conditions under which the evaluation process is to be performed. For compliance with Appendix R, the SSA must be based on the following considerations:

- *Exposure Fire:* The analysis must assume that a single *"exposure fire"* will occur in any fire area. An exposure fire is defined as a fire in a given fire area that involves either in-situ (permanently installed) or transient combustibles, but is external to any SSCs located in (or adjacent to) that same fire area. The effects of such fire (e.g., smoke, heat or ignition) can adversely affect those SSCs 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 fire area. Also, a fire involving combustibles other than the redundant train may constitute an exposure fire to both redundant trains located in the same area

- *Extent of Fire Damage:* For analysis purposes, it is assumed that only a single exposure fire will occur in any fire area at a given time. Since it is not deemed possible to accurately predict the manner in which equipment (cables, circuits or components) may fail, this analysis must assume that the fire will damage any unprotected equipment located in the fire area under evaluation, and, unless demonstrated otherwise through the performance of more detailed evaluations, it must be assumed this damage will cause the affected equipment to fail in an undesired manner for safe-shutdown. The fire area boundaries represent the extent of fire spread assumed in analysis. During the performance of a comprehensive SSA, all areas of the plant will be individually analyzed for an exposure fire.

- *Failures*: The only failures considered are those that are directly attributable to the fire. No other failures or independent events are assumed to occur concurrently with the fire. No other design-basis events or failure consequences need be postulated in conjunction with the exposure fire, except for those caused by the fire itself.

- *Equipment Availability:* At the onset of fire, all safe-shutdown systems are assumed to be operable and available for post-fire safe-shutdown.

- *Availability of Offsite Power:* For fires not requiring implementation of an alternative or dedicated shutdown capability, offsite power is assumed to remain available unless fire can result in its loss. In the absence of an evaluation of the impact of fire on the availability of the offsite power sources, the analysis should demonstrate the capability of achieving shutdown conditions where offsite power is available and where offsite power is not available for up to 72 hours. For fire areas requiring an alternative or dedicated shutdown capability, the analysis should demonstrate the capability of achieving shutdown conditions where offsite power is available and where offsite power is not available for up to 72 hours. After 72 hours, offsite power can be assumed restored.

- *Automatic Equipment Operation*: Automatic equipment operation may or may not occur during a fire. For fire in areas requiring an alternative or dedicated shutdown capability, a loss of automatic functions must be assumed. For example, in the event of a loss of offsite power (LOOP) the EDGs will normally start automatically on undervoltage. However, in developing the alternative shutdown capability operation of this automatic start feature cannot be assumed. For other fire areas, automatic operation of components and logic circuits may be credited in the analysis, but only if the circuitry associated with the automatic operation is known to be unaffected by the postulated fire (i.e., satisfy separation requirements of Section III.G.2 of Appendix R). If the automatic actuation of equipment will be lost as a result of fire in these areas, manual initiation of systems required to achieve and maintain safe-shutdown, via manipulation of controls located in the main control room, is acceptable if it can be demonstrated that reliance on such operator actions will provide an equivalent level of safety to that which would be achieved by performance of the automatic functions.

- *Plant Status*: The plant is operating at 100-percent power upon the occurrence of the fire.

- *Equipment Status:* Components are in their normal operating position or status at the time of the fire. All relay, position switch, an control switch contacts are in the position or status that corresponds to the normal operation of the device. Test and transfer switches in control circuits are in their normal position.

- *Use of Repair Activities*: Repair activities, (which are generally defined as any activity requiring the use of tools such as wiring changes, installation of electrical or pneumatic jumpers, and fuse replacements) are not permitted for systems required to achieve and maintain hot shutdown conditions. Modifications and repairs are permitted for cold shutdown systems as described below.

- *Multi-Unit Sites*: Where a single fire can impact more than one unit, the ability to achieve and maintain safe-shutdown for each affected unit must be demonstrated.

- *Passive Components:* The operation of passive components that are not electrically controlled or operated, such as manually actuated valves and check valves, is not assumed to be affected by fire damage.

- *Time Constraints and Limitations of Fire Damage*

  Hot Shutdown Systems (All Areas)
  When considering the consequences of fire in a given fire area, it must be conclusively demonstrated that one success path of equipment, that can be used immediately to bring the reactor to *hot shutdown* conditions, remains unaffected by fire.

  Cold Shutdown Systems (Areas not Requiring an Alternative Shutdown Capability)
  For areas of the plant not requiring an alternative or dedicated shutdown capability, it must be demonstrated that fire damage to one success path of equipment needed for achieving cold shutdown will be limited so that equipment can be returned to an operating condition within 72 hours.

  Cold Shutdown (Areas Requiring an Alternative or Dedicated Shutdown Capability)
  For areas requiring an alternative or dedicated shutdown capability, it must be demonstrated that cold shutdown capability can be restored *and cold shutdown conditions achieved* within 72 hours.

6.4.2 Define Required Safe-Shutdown (SSD) Functions

Required shutdown functions are those plant process and support functions that must be accomplished and controlled to ensure that the reactor is brought to and maintained in a safe-shutdown condition without exceeding the shutdown performance goals described above. (See Section 6.4.1.3.) Successful accomplishment of each of the following shutdown functions is necessary to preclude the occurrence of an unrecoverable plant condition (e.g., uncontrolled primary depressurization, loss of DHR capability or breach of the RCS boundaries):

- *Reactivity Control*
  This function is necessary to decrease the power output of the reactor core to the decay heat level. The reactivity control function must be capable of achieving and maintaining reactor shutdown from the initial scram shutdown to cold shutdown conditions. This function must be capable of compensating for any positive reactivity increases as a result of Xenon-135 decay, reactor coolant temperature decreases occurring during cooldown, and RCS dilution. The safe-shutdown performance and design requirements for the reactivity control function can be met without automatic scram/trip capability. The SSA must only provide the capability to manually scram/trip the reactor. For PWR the analysis must demonstrate that a method for ensuring that adequate shutdown margin is maintained. This is typically accomplished by ensuring an adequate concentration of borated water is utilized during RCS makeup/charging.

- *Reactor Coolant Makeup Control*
  The reactor coolant makeup control function must be capable of ensuring that sufficient makeup inventory is provided to compensate for reactor coolant system fluid shrinkage during cooldown and to replace any coolant that may leak from the system. Maintenance of adequate inventory prevents overheating of the reactor fuel, which could lead to core damage.

Systems performing this function must be capable of maintaining reactor coolant level above the top of the core for BWRs[25] and within the level indication of the pressurizer for PWRs.

- *Reactor Coolant Pressure Control*
  Pressure control is required to ensure that the RCS is operated within prescribed pressure-temperature limits, to prevent RCS peak pressure limitations from being exceeded and (for PWRs) to minimize void formation within the reactor vessel during natural circulation cooldown.

- *Decay Heat Removal*
  The DHR function must be capable of removing both decay and latent energy from the reactor core and primary systems at a rate such that overall system temperatures can be maintained within acceptable limits. This function shall also be capable of achieving cold shutdown conditions and maintaining cold shutdown thereafter.

- *Process Monitoring*
  To adequately change system alignments, control safe-shutdown equipment, and ensure the shutdown process remains within acceptable performance criteria, operators must be provided with sufficient instrumentation to monitor the status of process system variables. Direct readings of the variables used to control the shutdown process are required.

  In GL 81-12, “Fire Protection Rule,” and IN 84-09, “Lessons Learned form NRC Inspections of Fire Protection Safe Shutdown Systems” the NRC provides guidance regarding the minimum set of instrumentation deemed necessary for *alternative* or *dedicated* shutdown capabilities. The minimum process monitoring capability described in these documents includes the following instruments:

  Instrumentation Needed for Alternative or Dedicated Shutdown of a BWR:
  a. Reactor water level and pressure.
  b. Suppression pool level and temperature.
  c. Emergency or isolation condenser level.
  d. Diagnostic instrumentation for shutdown systems. (See Note 1.)
  e. Level indication for all tanks used.

  Instrumentation Needed for Alternative or Dedicated Shutdown of a PWR:
  a. Pressurizer pressure and level.
  b. Reactor coolant hot leg temperature or core exit thermocouples, and cold leg temperature.
  c. Steam generator pressure and level (wide range).
  d. Source range neutron flux. (See Note 2.)
  e. Diagnostic instrumentation for shutdown systems. (See Note 1.)
  f. Level indication for all tanks used [e.g., condensate storage tank (CST)].

  Note 1 Diagnostic instrumentation is instrumentation, beyond that identified above, that is needed to ensure the proper actuation and functioning of safe-shutdown equipment and associated support equipment (e.g., flow rate, pump discharge

[25] Short-term core uncovery may be permissible when using low-pressure injection systems at BWRs (see Richards Letter to BWROG, December 2000).

pressure). The diagnostic instrumentation needed is plant-specific and should be based on the design of the alternative shutdown capability (GL 86-10). Sufficient instrumentation must be ensured to remain available (unaffected by fire) to allow operators to detect malfunctions that may occur, take appropriate corrective actions without resorting to potentially complex troubleshooting activities, and ensure activity was successfully accomplished.

Note 2 In a letter dated September 10, 1985, the NRC Committee for Review Generic Requirements (CRGR) instructed the Office of Nuclear Reactor Regulation (NRR) to eliminate the staff position for a source range neutron flux monitor as part of the Appendix R alternative shutdown instrumentation in PWRs.

Enclosure 1 of GL 86-10, “Implementation of Fire Protection Requirements” states that the instrumentation listed above provides an acceptable method for compliance with the *alternative shutdown* requirements of the regulation (i.e., Section III.L.2.d of Appendix R). This list, however, does not exclude other alternative methods of compliance. 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.

Instrumentation Needed for Redundant Shutdown Capabilities:

For redundant shutdown capabilities, where shutdown activities are controlled from within the main control room, one train of systems needed to achieve and maintain hot shutdown conditions must remain free of fire damage. (Section III.G of Appendix R) As a result, additional specific guidance, such as that discussed above for alternative shutdown capabilities is not necessary. For these areas, the determination of required process and diagnostic instrumentation should to be based on the plant-specific operating procedures (including normal, abnormal, and EOPs) that would be used to shutdown the reactor in the event of an unmitigated fire. Since the same shutdown functions are generally required to be performed for both alternative and redundant shutdown, this monitoring capability is expected to be fairly consistent with the instrumentation listed above.

Sufficient instrumentation must be ensured to remain available to implement the shutdown methodology described in the SSA and applicable procedures. For shutdown strategies that rely on operator actions as a means of mitigating equipment maloperations that may occur as a result of fire damage, sufficient diagnostic instrumentation must be available for operators to detect the maloperations and initiate appropriate responses in a timely manner, without resorting to complex and potentially hazardous troubleshooting activities.

When sufficient diagnostic instrumentation is not ensured to remain unaffected by fire, reliance on the operators ability to detect fire-induced maloperations that may occur and perform activities needed to defeat them before an unrecoverable condition is achieved cannot be ensured. For example, during a fire an operator observes the ensured method of monitoring pressurizer level to be decreasing. Since many possible maloperations of plant equipment are capable of causing this indication (e.g., spurious closure of a makeup flowpath valve, loss of a makeup pump, open bypass valve, open PORV or open head vent) without the benefit of additional diagnostic instrumentation, the operator’s ability to determine the cause of this indication (pressurizer level decreasing) may be significantly compromised.

It should be noted that the use of operator actions as an immediate response to a confirmed fire has been shown to reduce the need for diagnostic instrumentation. An example of this approach would be a shutdown procedure that, immediately upon confirmation of fire, directs operators to close the MSIVs in the control room as a means of preventing their undesired operation (failure to close) as a result of potential fire damage to their control circuits.

For this case, an immediate action is taken to prevent a possible undesired outcome. Since no reliance is placed on the operators ability to detect a possible failure, the need for some diagnostic instrumentation may be eliminated.

- *Supporting Functions*
  To ensure the successful accomplishment of the above shutdown functions, several support systems and equipment are necessary. The supporting functions shall be capable of providing the process cooling, lubrication, etc., necessary to permit the operation of equipment used to accomplish the above shutdown functions. The specific support systems needed will vary with the shutdown methodology developed by the plant. Typical examples include electrical distribution systems, HVAC and essential room cooling, component cooling water, essential service water, and communications capability (e.g., portable radios, sound powered phones).

6.4.3 Select Shutdown Systems

The next step in the process is to identify a system or combination of systems capable of accomplishing each of the required shutdown functions described above (Section 6.4.2). This may be accomplished by a review the design documentation, such as system descriptions, system drawings, and plant procedures, described in Section 6.4.1.1. Once identified, these systems can be combined into safe-shutdown success paths and given a unique designation (e.g., SSD Path 1, SSD Path 2, etc.). A description of each path should then be documented. For example, shutdown paths for a BWR may be described as follows:

Path 1 Control Rod Drive System; Division I train of ADS, Division I CS in Alternative Shutdown Cooling and Division I of RHR in Suppression Pool Cooling Mode

Path 2 Control Rod Drive System; Division II train of ADS, Division II CS in Alternative Shutdown Cooling and Division II RHR in Suppression Pool Cooling Mode

In addition, systems necessary to support the operation of the above “front line” systems should also be identified as safe-shutdown systems (e.g., electrical distribution systems, instrumentation, cooling water systems and HVAC). A summary of the post-fire safe-shutdown analysis process to this point is illustrated in Figure 6-4a.

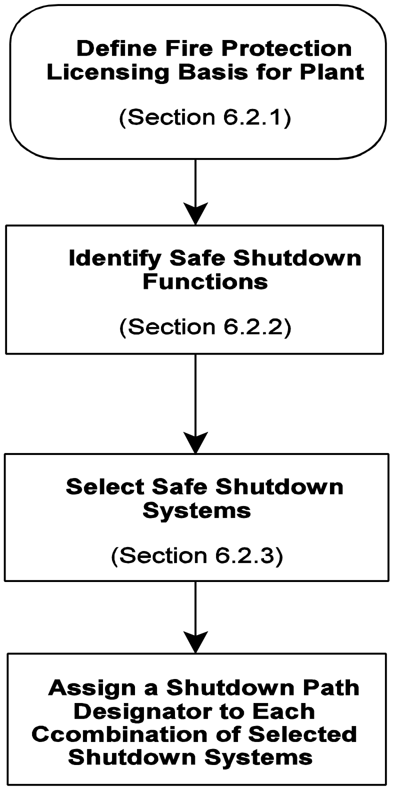

Define Fire Protection Licensing Basis for Plant
(Section 6.2.1)
Identify Safe Shutdown Functions
(Section 6.2.2)
Select Safe Shutdown Systems
(Section 6.2.3)
Assign a Shutdown Path Designator to Each Ccombination of Selected Shutdown Systems

Figure 6.4a Safe Shutdown System Selection and Path Development

6.4.4 Select and Locate Required Shutdown Equipment

The systems identified above form the basis for the selection of safe-shutdown components. The next step in the process is to identify the specific equipment necessary for the identified systems to perform their shutdown function. This process is illustrated in Figure 6-4b.

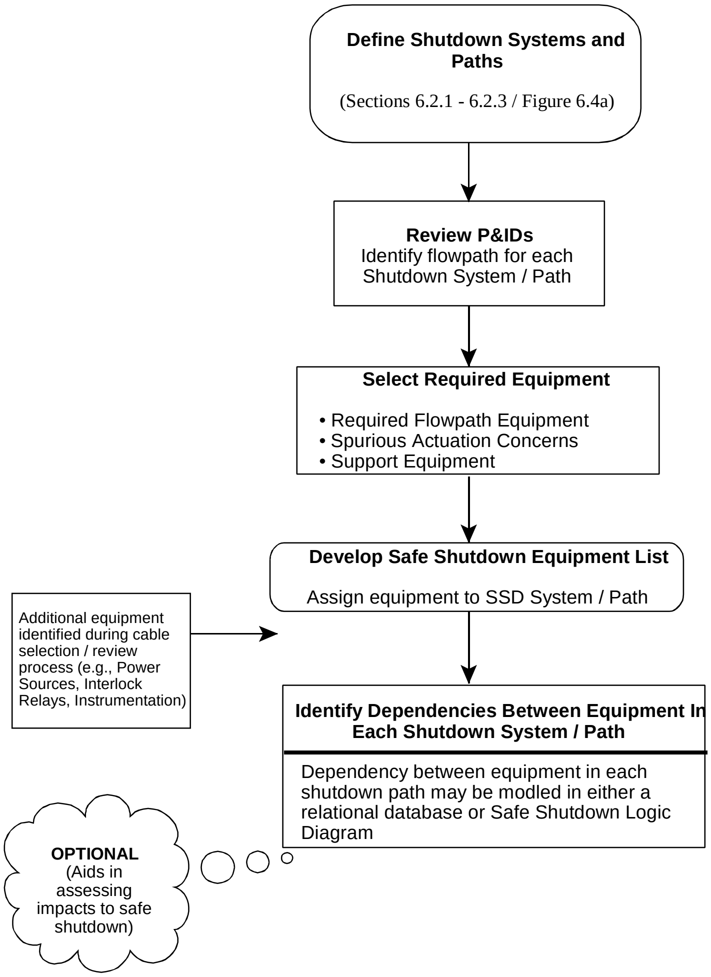

Define Shutdown Systems and Paths
(Sections 6.2.1 - 6.2.3 / Figure 6.4a)
Review P&IDs
Identify flowpath for each Shutdown System / Path
Select Required Equipment
• Required Flowpath Equipment
• Spurious Actuation Concerns
• Support Equipment
Develop Safe Shutdown Equipment List
Assign equipment to SSD System / Path
Additional equipment identified during cable selection / review process (e.g., Power Sources, Interlock Relays, Instrumentation)
Identify Dependencies Between Equipment In Each Shutdown System / Path
Dependency between equipment in each shutdown path may be modled in either a relational database or Safe Shutdown Logic Diagram
OPTIONAL
(Aids in assessing impacts to safe shutdown)

Figure 6.4b Safe Shutdown Equipment Selection

Using piping and instrumentation drawings (P&IDs) for the systems comprising each safe-shutdown path, the mechanical equipment required for the operation of each system may be identified. The selected equipment should be related back to the safe-shutdown systems it supports and be assigned to the same safe-shutdown path as that system. Equipment that could spuriously operate and impact the safe-shutdown capability may also be identified during the review of the P&IDs. This equipment should be related to the particular safe-shutdown path that it can affect. Equipment that can result in a loss of reactor inventory in excess of the available make up capability (i.e., initiate a fire-induced LOCA) should also be identified by a review of P&IDs for systems physically connected to the reactor vessel. The following criteria and assumptions are applicable to the selection of safe-shutdown equipment:

- Exposure fire damage to manual valves and piping is not assumed to adversely impact their ability to perform their safe-shutdown function.
- Manual valves are assumed to be in their normal position as shown on P&IDs.
- 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.
- The effects of fire on instrument tubing must be considered. Heat generated by the fire may cause subsequent effects on instrument readings and/or signals. The fire area location of the instrument tubing should be determined and the effects of fire damage to it should be considered when evaluating the effects of a postulated fire in the area. In addition, the effects of fire on heat sensitive components such as copper sweated fittings should also be considered.

As a result of this review process, a list of “safe-shutdown components” also called “required components” will be generated for each system. This list should include: (1) components that are required to operate in order to ensure the proper operation of systems credited in the analysis (e.g., SSA) for achieving and maintaining post-fire safe-shutdown conditions; *and* (2) components of which inadvertent actuation or maloperation could significantly degrade the capability of these credited systems to perform their intended shutdown function. The following examples represent the typical required components:

(1) Components that must start and/or continue to operate on demand such as required pumps, fans, air compressors and motors.

(2) Electrically actuated or controlled components that must change operating status or position, such as a normally closed valves located in a required flowpath.

(3) Electrically actuated or controlled components that must *not* change position or operating mode. Examples include a normally closed valves that constitute a system boundary or diversion flowpath and normally open valves located in a required flowpath.

(4) Components needed to ensure the proper operation of shutdown equipment and systems. Examples include: Power supplies (EDGs, battery banks, inverters, battery chargers, SWGRs, MCCs, load centers, and distribution panels) room coolers and air bottles.

(5) Components that can cause equipment and systems to automatically actuate and/or change operating state in an undesired manner for safe-shutdown. Examples include interlock circuits, pressure switches, temperature switches, solid-state control systems, and various instrumentation devices.

The resulting list of equipment SSEL establishes the basis for identifying *required circuits and cables* (i.e., circuits and cables needed to support operation of the identified shutdown paths) ***as well as*** *associated nonsafety circuits* for which damage attributable to fire could impact (adversely affect) the achievement of safe-shutdown conditions.

Illustration of Equipment Selection Process

The following are *guidelines* regarding which components to include on the SSEL for each system evaluated. (Refer to Figure 6-5.)

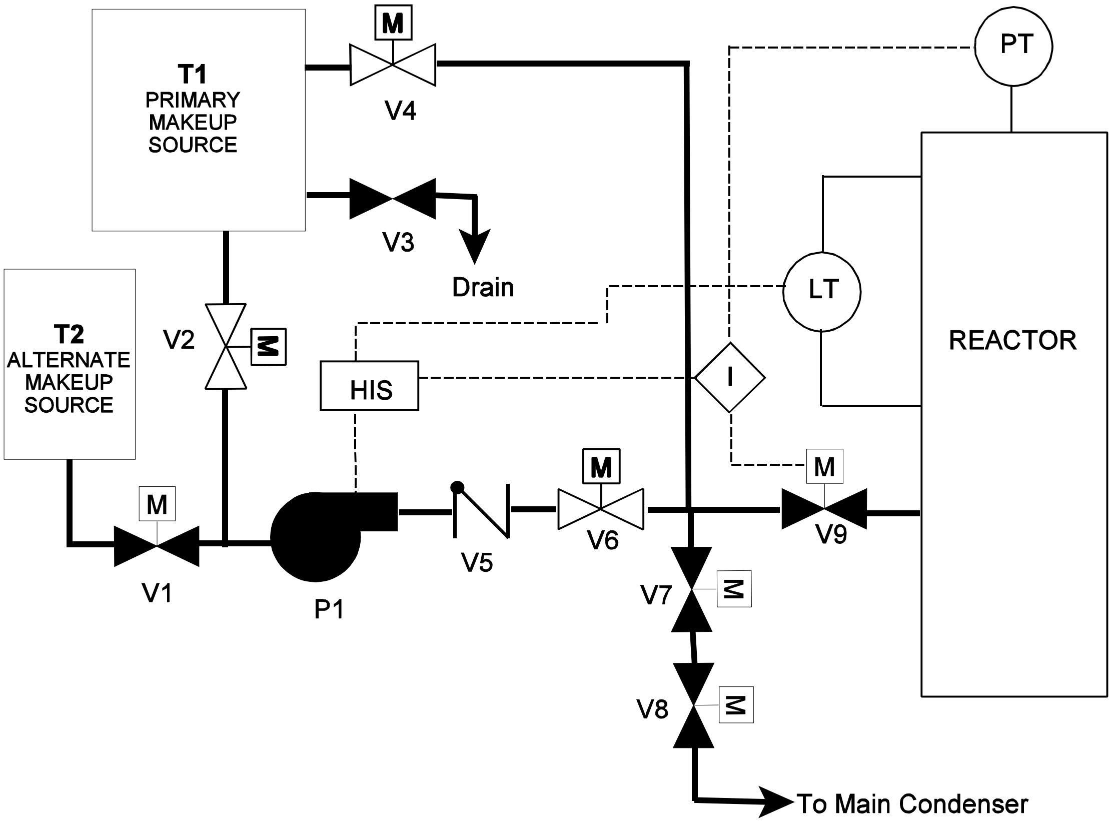


Figure 6-5 Example System

Components of interest are those needed to ensure the successful accomplishment of a required shutdown functions. This includes components that are needed to ensure the proper functioning of required shutdown systems (e.g., pumps and valves located in a required flowpath) as well as components of which maloperation attributable to fire could impact the shutdown capability (e.g., pressurizer PORVs, ADS valves, instrumentation). The following examples represent the typical components to be included in the SSEL:

- *Valves and HVAC dampers that constitute system boundaries* should be included if fire-induced faults could cause them to change position *and* their maloperation (e.g., inadvertent/spurious opening) would significantly impact the capability of the system to perform its intended shutdown function (e.g., by creating a flow leakage/diversion path that cannot be adequately compensated for by the system). Valves V7 and V8 in Figure 6-5 fall into this category.
- *Valves and dampers (e.g., HVAC dampers) in the flow path* that are power operated should be included. Associated valve operators should also be included as part of the valve/damper. These components should be included whether or not they are required to change position during shutdown if a fire-induced fault could cause them to change position. These components ensure that the process flow path is maintained. [Valves V1, V2, P1, V4 and V9 in Figure 6-5) fall into this category.]
- *For tanks*, all inlets and outlet lines should be evaluated for their functional requirements and isolation. For lines that are not required to be functional, a means of isolation should be included when necessary to prevent unnecessary drawdown of the tank. Tank inventory must be evaluated to ensure that it is always sufficient to support the system requirements. Tanks T1 and T2 in Figure 6-5 are an example of this category.
- *Interlock circuitry* between safe-shutdown components and safe-shutdown/non-safe shutdown components should be reviewed to determine if additional components require inclusion. This is to ensure that a failure of a non-safe-shutdown component would not prevent the safe-shutdown system from operating as required. (In Figure 6-5, the interlocks between the reactor level and the pump and the reactor pressure and valve V9 and the pump are examples of this category.)
- *All necessary process and diagnostic instrumentation* (e.g., process flow, pressure, temperature, level, indicators and recorders)
- *Power supplies* or other electrical components that support operation of required shutdown components should be included (SWGR, EDGs, MCCs, load centers, inverters, batteries, relays, control switches, flow switches, pressure switches, level switches, transmitters, controllers, transducers, and signal conditioners).

6.4.5 Identify Required Circuits and Cables

As discussed above, to achieve safe-shutdown conditions certain *shutdown functions* (e.g., reactivity control, DHR, reactor coolant inventory and pressure control, etc.) must be accomplished and controlled to ensure that the reactor is brought to and maintained in a safe-shutdown condition within design parameters established in the applicable licensing basis documents. The systems identified as being needed to accomplish these functions are classified as *"required shutdown systems."* Similarly, the equipment that must operate or be prevented from mal-operating in order for the required shutdown systems to accomplish their intended shutdown functions, are considered *"required equipment" or "required components."* Once identified, required components are listed on the SSEL. The SSEL establishes a starting point for identifying *required circuits and cables* (i.e., circuits and cables needed to support operation of the identified/credited shutdown paths) ***as well as*** the *associated nonsafety circuits* for which damage attributable to fire could impact (adversely affect) the achievement of safe-shutdown conditions by initiating an event that exceeds the design capability of the credited/required shutdown systems.

After the listing of required components is developed SSEL for each shutdown path, the circuits/cables needed to support the operation of this equipment are identified and evaluated. For each required component, all circuits (cables) that: (a) are needed to ensure proper operation, or (b) could cause maloperation/undesired actuation must be identified.
A circuit/cable is considered to be *required for safe-shutdown* if it is connected to or associated with the operation of a required shutdown component *and* fire damage to the circuit/cable can cause the component to fail in an undesired manner for post-fire safe-shutdown. In addition to the set of circuits/cables needed to ensure the acceptable operation of required shutdown components, *associated circuits of concern to post-fire safe-shutdown* must also be identified and analyzed. As discussed below, these circuits have one of the following:

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

(2) A *common enclosure* (e.g., raceway, panel, junction box) with shutdown cables and a) are not electrically protected by suitably sized circuit breakers, fuses or similar devices, or b) will allow fire to propagate into the common enclosure

(3) *A connection to equipment of which spurious operation or maloperation may adversely affect the shutdown capability* (Note: As discussed in Section 6.4.4 above, the identification of "spurious operation components" is typically performed as part of the review of P&IDs to identify required shutdown equipment)

The following paragraphs provide criteria and guidance for selecting safe-shutdown cables and determining their potential impact to equipment required for achieving and maintaining safe shutdown for the condition of an exposure fire. The objective of the cable selection criteria is to ensure that circuits and cables of required shutdown equipment are identified and that these cables are properly related to equipment with functionality they could affect. Through this cable-to-equipment relationship, cables become associated with the same safe-shutdown path as the equipment affected by the cable.

6.4.5.1 Cable Identification

- *Scope:* The list of cables of which failure could impact the operation of a piece of safe shutdown equipment includes more than those cables that are directly connected to the equipment. The relationship between cable and affected equipment should be based on a review of electrical or elementary wiring diagrams. In addition to the cables that are physically connected to the equipment, the list of required cables will include any cables interlocked to the primary electrical schematic through secondary schematics. To ensure that all cables that could affect the operation of the safe shutdown equipment are identified, the power, control, instrumentation, interlock, and equipment status indications should be investigated. Schematic diagrams should be reviewed to identify additional circuits and cables for interlocked circuits that also need to be considered for their impact on the ability of the equipment to operate as required in support of post-fire safe-shutdown.
- *Cable/Component Associations:* Each cable should be related back to the same shutdown path as the equipment it supports. In cases where the failure of a single cable could impact more than one piece of shutdown equipment, the cable should be associated with each piece of shutdown equipment.
- *Isolation Devices:* Electrical devices such as relays, switches, and signal resistor units (SRUs) are considered to be acceptable isolation devices. In the case of instrument loops, the isolation capabilities of the devices in the loop should be evaluated to determine that an acceptable isolation device has been installed at each point where the loop must be isolated so that a fault would not impact the performance of the instrument function.
- *Screening:* Circuits that do not impact the desired safe-shutdown performance or expected operation of a component, such as those illustrated in Figure 6-2 above, may be screened from further evaluation unless some reliance on these circuits is necessary. However, these circuits must be ensured to be isolated from the component's control scheme in such a way that a cable fault would not impact the performance of the circuit.
- *Power Cables:* Electrical distribution system (EDS) equipment needed to provide power to shutdown equipment may be identified from a review of the electrical schematics associated with the shutdown equipment. For each component requiring electric power to perform its safe-shutdown function, the cable that supplies power to the component should be identified. Initially, only the power cables from the immediate upstream power source are identified for these interlocked circuits and components. 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 EDGs to the safe-shutdown equipment. This equipment should then be added to the SSEL. This information will be needed to support the *Associated Circuits — Common Power Source Analysis* described in Section 6.4.5.2.
- *Automatic Initiation Logic:* The automatic initiation logic 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 be verified to not adversely affect any post-fire safe-shutdown system function. Otherwise it would need to be included in the SSEL.

6.4.5.2 Identification of Associated Circuits

The overall objective of the SSA, is to demonstrate that in the event of an exposure fire in any single area of the plant, SSCs important to safe-shutdown will remain available to accomplish required shutdown functions (e.g., reactivity control, reactor coolant makeup, and pressure control, DHR) as needed. Because circuits and cables of the required shutdown systems frequently share certain physical or electrical configurations with cables of nonessential systems and equipment (i.e., not required for post-fire safe-shutdown) it is not sufficient to only consider the effects of fire damage to cables of required components. For example, consider the cable configuration shown in Figure 6-6. In this case, the cable that supplies power to a nonessential load is powered from the same power supply as equipment relied on for safe-shutdown. While a fire that causes a loss of the nonessential load may not directly impact the shutdown capability, a fire that damages the power cable of the nonessential load could significantly impact the shutdown capability if damage to this cable resulted in a loss of the required (Train B) power supply. Because fire damage to certain nonessential equipment and cables may adversely affect the operability of required shutdown systems, in performing the SSA the analyst must consider the effect of fire on both the primary, or "front-line" shutdown equipment and any nonessential equipment and cabling that may affect the ability of required shutdown systems to accomplish their intended shutdown function if they are damaged by fire. That is, the scope of the evaluation must extend beyond the limited set of equipment that comprises the defined shutdown paths. A suitably comprehensive evaluation will address the potential impact of fire damage to any circuit/cable located within the fire area that could adversely affect the post-fire safe-shutdown capability.

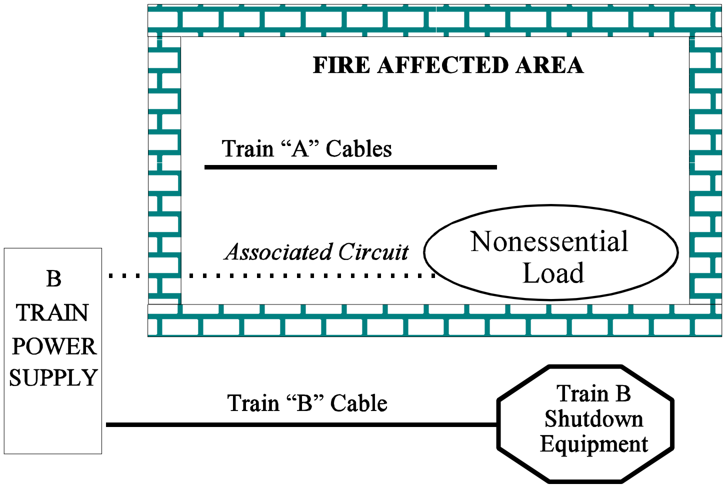


Figure 6-6 Associated Circuit

6.4.5.2.1 Associated Circuit Configurations of Concern to Post-Fire Safe Shutdown

Section III.G.2 of Appendix R to 10 CFR Part 50 requires that separation features be provided for equipment and cables, including associated nonsafety circuits that could prevent the operation or cause the maloperation (attributable to hot shorts, open circuits, or shorts to ground) of redundant trains of systems necessary to achieve and maintain hot shutdown conditions. An *associated circuit of concern* to post-fire safe-shutdown may include any circuit or cable that, while not needed to support the proper operation of required shutdown equipment (i.e., a nonessential/nonsafety circuit), could adversely affect the plant's ability to achieve and maintain safe-shutdown conditions. Associated circuits of concern may be found to be associated with circuits of required systems through any of the following configurations:

- Circuits that share a **common power source** (e.g., SWGR, MCCs, fuse panel) with circuits of equipment required to achieve safe-shutdown
- Circuits that share a **common enclosure**, (e.g., raceway, conduit, junction box, etc.) with cables of equipment required to achieve safe-shutdown
- Circuits of equipment of which **spurious operation** or maloperation may adversely affect the shutdown capability

Methods for identifying each type of associated circuit defined above are discussed in the following sections.

Circuits Associated by Common Power Source

The electrical distribution system is one of the most important support systems of any installation. Electrical power supplies (e.g., SWGRs, MCCs, fuse and circuit breaker panels) required to power shutdown equipment in the event of fire are identified during the selection of required shutdown equipment (Section 6.4.4). Once identified, the analyst must then ensure that in the event of fire, the required power supplies will remain available, as needed to ensure the continuity of service to essential shutdown loads. In the event of an electrical fault condition, a properly engineered system will allow only the protective device nearest the fault to open while not disturbing the remainder of the system.

In many cases, relatively few of the components that are normally powered from a specific power supply are needed to accomplish required shutdown functions. While providing power to the remaining "nonessential" loads (equipment) may not be necessary to accomplish safe-shutdown, it must be ensured that fire initiated faults on the power cables to this equipment will not affect the shutdown capability by causing a trip of the protective devices (e.g., circuit breaker, fuse, or relay) located upstream of the required supply. To address this concern, the SSA must be extended to consider the effects of fire-induced faults on all circuits of required power supplies identified in Section 6.4.4. To ensure that fire-induced faults on these circuits will not affect the capability of achieving safe-shutdown conditions, this analysis must ensure that circuits which share a common power source with circuits of required equipment are provided with: (a) fire protection features sufficient to satisfy Section III.G.2, or (b) suitably coordinated electrical protective devices.

The common power source associated circuit concern is illustrated in Figure 6-7a. In this case, in the event of fire in Fire Area II, Train A safe-shutdown equipment (Pump A) located in Fire

Area I and powered by safe-shutdown Bus A, is relied on to accomplish safe-shutdown. Although the Train A pump is located in a separate fire area, it may be vulnerable to loss as a result of fire in Fire Area II. This is because, as shown in Figure 6-7a, a Train A *associated circuit power cable* is also located in Fire Area II. Although this cable and its connected load (Pump X) are not needed to perform a shutdown function, the absence of suitable *coordination of electrical protective devices*, a fire-induced electrical fault on the this cable could cause the upstream feeder breaker of Bus A (Breaker 1) to trip before the individual branch breaker (Breaker 2). Because this would result in a loss of electrical power to all shutdown equipment powered from safe-shutdown Bus A, failures of this type are unacceptable.

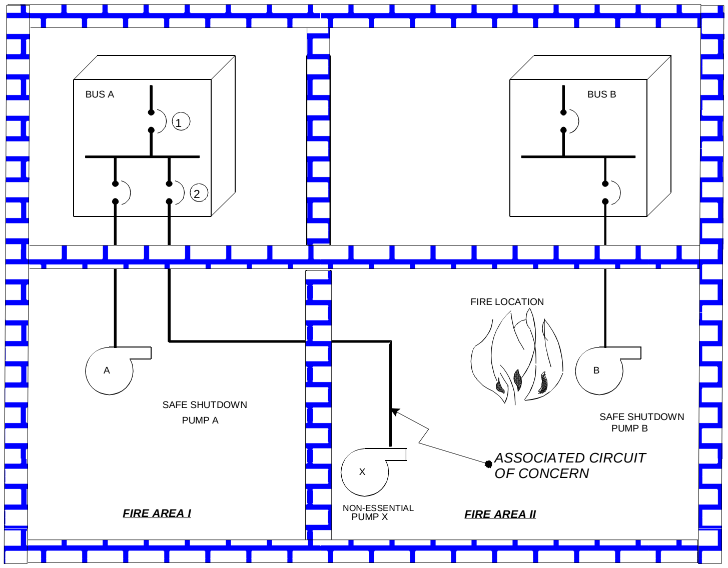


Figure 6-7a Common Power Source Associated Circuit

The common power source associated circuit concern consists of two items:

(1) coordination of electrical protective devices (circuit breakers, relays, fuses, etc.)
(2) multiple high impedance faults (MHIFs)

Coordination of Electrical Protective Devices

To minimize the effect of an electrical fault on system operation, the tripping characteristics of electrical protective devices (fuses, circuit breakers and relays) should be sufficiently coordinated so that electrical faults will be rapidly isolated by the protective device located nearest the fault. Although the term “coordination” is often used, “selectivity” or “selective tripping” more precisely describes post-fire safe-shutdown concerns. Selectivity means positive coordination over the entire range of possible fault currents, ensuring that the faulted circuit is cleared and that other parts of the system are not affected. Examples of both a non-selective system and a system that is provided with fully selective protective devices are illustrated in Figures 6-7b and 6-7c. In the non-selective system shown in Figure 6-7b, a branch circuit fault would cause fuses D, C and B to open, resulting in a loss of power to all loads supplied from the system. In the fully selective system shown in Figure 6-7c, the fault is isolated by fuse D and the remainder of the system remains undisturbed.

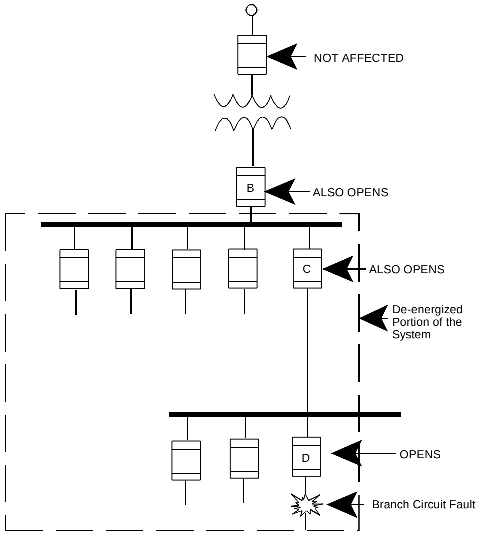


Figure 6.7b - Non-Selective Coordination

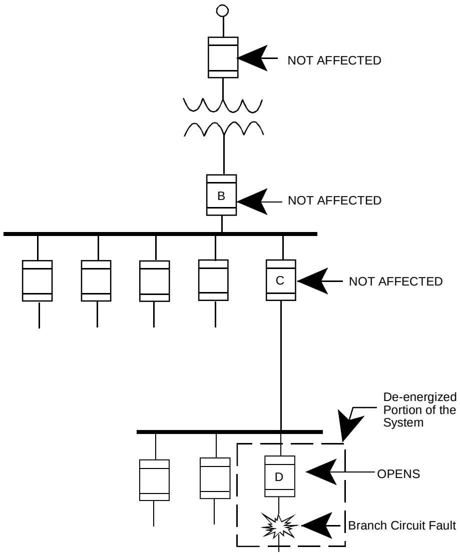


Figure 6.7c - Selective Coordination

Depending on their design and/or individual trip settings, fault protective devices of the same type (e.g., fuse or circuit breaker) and rating (20 amp, 30 amp etc.) may have significantly different tripping characteristics. A coordination study consists of the selection or setting of all series protective devices from the load upstream to the power supply. In selecting or setting these protective devices, a comparison is made of the operating times of all the devices in response to various levels of overcurrent. The objective, of course, is to design a selectively coordinated electrical power system. The operating response of a specific protective device is graphically represented by time-current characteristic curves. Time-current characteristic curves are presented on a log-log graph where the ordinate (y-axis) represents a time range from 0.01 to 1,000 seconds, and the abscissa (x-axis) represents the current level. By overlaying the time-current curves of two protective devices or comparing them in some other manner, their selectivity may be quickly determined. If the curves of the two devices intersect, for example, the intersection area indicates conditions under which both devices may trip. If such a pair of circuit breakers were used in an electrical distribution system, those conditions could result in both devices tripping. On the other hand, if the curves of the circuit breakers are distinctly separate and do not intersect, the circuit breakers are said to be coordinated.

A new or revised coordination study should be made when the available short-circuit current from the power supply is increased; when new large loads are added or existing equipment is replaced with larger equipment; or when protective devices are upgraded.

Multiple High-Impedance Faults

In the previous paragraphs, the need for circuit protective device "selectivity" was discussed. The evaluation of selectivity typically considers "worst-case" fault conditions initiated by "bolted faults." A "bolted fault" develops when the conductor of a faulted cable is in firm contact with a conductor that is at a different potential, such as a cable tray (phase to ground fault). Since this fault condition offers little, if any, impedance (resistance) to the flow of fault current, it will result in a maximum value of fault current being drawn from the affected power source. In a properly coordinated (selective) system, this high value of fault current will be rapidly interrupted and cleared by the circuit protective device closest to the fault. Under certain conditions, however, insulation degradation resulting from fire damage may cause a different kind of fault condition known as an "HIF." In almost every case, this type of fault occurs between one phase and ground. However, instead of establishing direct contact to ground potential (as for a "bolted fault"condition) the faulted conductor is not mechanically firm or is erratic. As a result an arc develops in the air gap between the faulted conductor and ground. This arc introduces an element of resistance to the flow of fault current that is not present in a bolted fault. As a result, the magnitude of high-impedance fault currents are relatively low (in comparison to a bolted fault) and in many cases, the arcing fault will be of such a low value that it is less than the continuous current rating of the overcurrent protective for the circuit involved.

In the majority of cases, an arcing fault starts as a small breakdown in insulation. Ionization of the atmosphere and destruction of insulation cause the fault to develop into a self-sustaining arcing fault. In a 480-V system, tests and calculations have indicated that this sustained current can be as low as 20-percent of the available bolted three-phase current[26]. Although the individual faults are not of sufficient magnitude to cause a trip of the individual load breakers, a coordination problem could exist if the cumulative effect of these faults were to cause the upstream feeder breaker of a required power source to trip. To fully demonstrate that a required power source will not be impacted by fire damage to its connected cabling, the potential impact of HIFs should be considered. This evaluation involves determining the effect of such faults on all cables of a required power supply that may exposed to fire damage. (See Figure 6-8.)

For the purpose of performing this analysis, the following assumptions are applicable:

- The HIF current of each cable that may be exposed to fire damage is postulated to be a value that is just below the trip point setting of the individual protective device for the load.
- All unprotected load cables of the power supply being evaluated, that are located within the zone of influence of the fire (e.g., located in the same fire area/zone), are assumed to simultaneously fault to the HIF condition.
- The total load current to be considered is the sum of all high-impedance faults *plus* the normal operating load current on the bus.

[26] "Good Design Prevents High-Impedance Fault," *Actual Specifying Engineer*, Vol. 17, No.4, Medalist Publications, Inc., Chicago, IL, 1967.

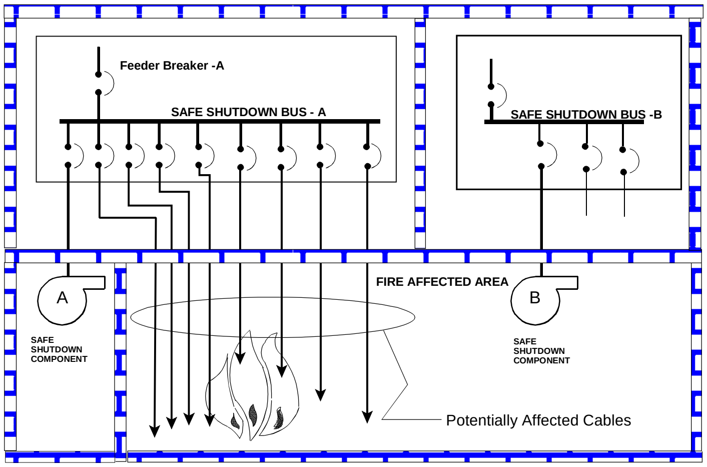


Figure 6-8 Illustration of Multiple HIF Concern

Circuits Associated by Common Enclosure

Cables that are not needed to perform a shutdown function (nonessential cables) frequently share a common enclosure (e.g., cable tray, conduit, junction box, panel, etc) with cables of shutdown equipment. Since the routing of these nonessential cables is generally unknown, they may be damaged by fire in any area of the plant. In the absence of suitably sized electrical protection devices (fuse or circuit breaker) and/or fire protection features, damage to these cables could also damage the required cables located within the common enclosure. In addition, if fire were to spread along these cables into an adjacent fire area due to inadequate cable penetration seals, the safe shutdown equipment or cables located in the adjacent fire area could also be impacted. This condition would exceed the criteria and assumptions of this methodology (i.e., multiple fires and fire spread beyond area under consideration).

Circuits that share enclosures with safe-shutdown circuits must be analyzed to determine the potential effect that fire damage to these circuits (cables) may have on the safe-shutdown capability. This concern consists of two issues:

(1) *Cable ignition*: Fire-initiated electrical faults on inadequately protected cables could cause an over current condition, resulting in secondary ignition.

(2) *Fire propagation*: The effects of the fire may extend outside of the immediate area or into the common enclosure by means of fire propagation.

As described in the following paragraphs, either of these cases could result in damage that could disable redundant trains of required shutdown equipment.

Case 1: Common Enclosure — Cable Ignition

Cables of nonessential equipment may share a common enclosure (e.g., raceway, conduit, or panel) with cables of equipment required for safe-shutdown. In the absence of adequate electrical protection (i.e., properly sized fuses and circuit breakers), heat generated by fire-induced faults on the nonessential cables may cause a secondary fire to occur within the common enclosure, thereby damaging required cables.

Figure 6-9 illustrates the common enclosure concern associated with “cable ignition.” As shown in this diagram, a fire occurs in fire area II and causes a fault on an associated circuit cable that is not properly protected by a suitably sized fuse. As a result of this condition, the fault current will propagate along the entire length of the affected cable, into an adjacent fire area (Fire Area I). If the value of fault current exceeds the current carrying capacity of the cable, a secondary fire may be initiated in Fire Area I, resulting in the loss of redundant trains of shutdown equipment (Instruments A and B).

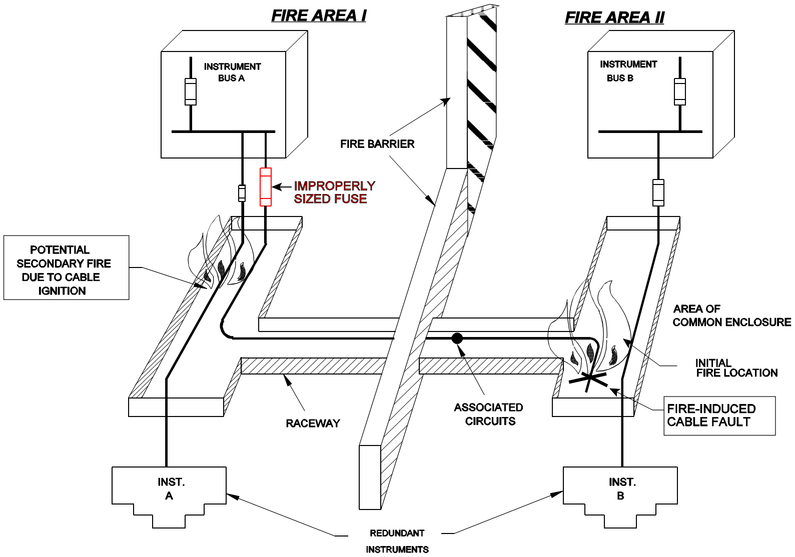


Figure 6-9 Common Enclosure - Case 1: Cable Ignition

Case 2 Common Enclosure — Fire Propagation

Cables of equipment that is not needed for safe-shutdown may traverse fire areas containing redundant trains of shutdown equipment. When fire protection features, such as fire stops and penetration seals are not provided, there is a potential for a cable to serve as a pathway for fire to propagate (travel) into adjacent fire areas. This concern is illustrated in Figure 6-10. In the example shown, the initial fire in Fire Area II will render instrument "B" inoperable. Since the cable tray is not provided with suitable protection features (e.g., penetration seals or fire stops), a fire that affects Instrument "B"cables could also propagate along the associated circuit cables and impact the redundant Instrument "A"cables located in the adjacent fire area.

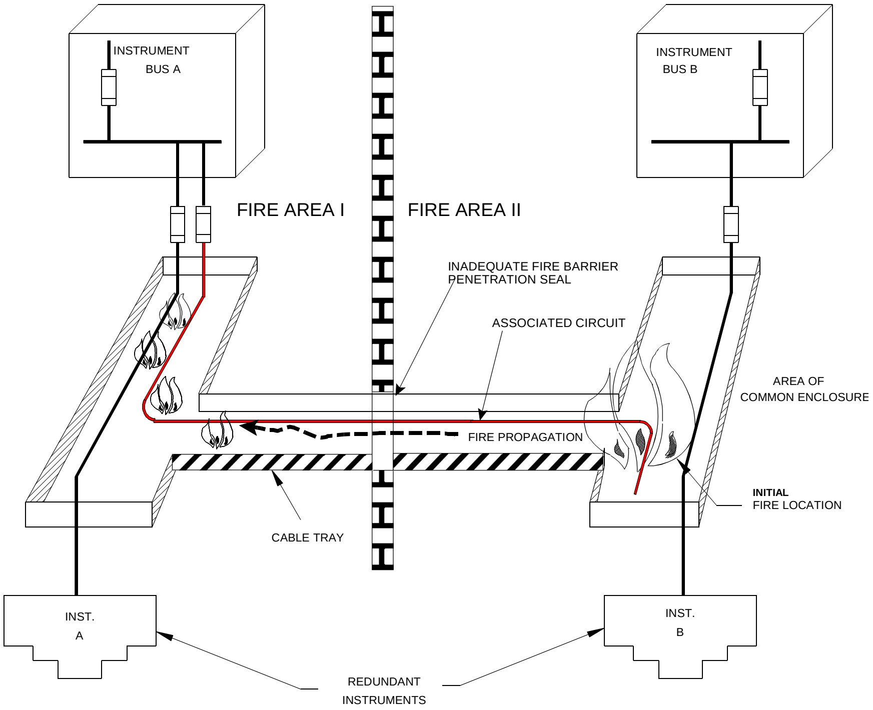


Figure 6-10 Common Enclosure Associated Circuit Case 2: Fire Propagation

Spurious Actuations and Signals

Cable damage attributable to fire or its related perils (e.g., firefighting and fire-suppression activities) can cause connected equipment to operate in an undesirable and/or unexpected manner. For example, a fire-induced short circuit on control wiring of a normally open MOV, could cause the valve to inadvertently close, thereby blocking a required flow path. Conversely, the spurious opening of a normally closed valve could divert flow from a required flow path. Additional examples include false instrument indications, the spurious starting or stopping of electrically powered equipment, such as pumps and motors, and the initiation of false control and interlock signals.

The achievement of safe-shutdown is dependent on the active control of some components and preventing the maloperation of other components. The circuits of both categories of components have the potential for being associated circuits of concern by spurious operation. Components which must actively operate (change position or operating status) at some point in the safe-shutdown sequence must be analyzed to identify circuits (cables) which if damaged could prevent the desired component operation; likewise, passive components, such as a normally closed MOV that is required to remain closed for safe shutdown, must be analyzed to ensure that fire-induced cable faults cannot cause the spurious maloperation of the component.

An example of how fire-initiated spurious actuations of equipment may impact the shutdown capability is illustrated in Figure 6-11. For this case, MOV-1, located in Fire Area IV, is normally closed during plant operation and is required to remain closed for safe-shutdown. As depicted in the illustration, MOV-1 could spuriously actuate (open) as a result of fire in Fire Area I. Specifically, if fire damage to relay “R” control circuits in this area were to initiate a false “auto-open” signal, relay “R” would actuate, closing contact RC1. Since actuation of contact RC1 has the same effect as closing the “open” contact of the MOV control switch (CS-O), motor-contactor solenoid 42-O would energize, resulting in the inadvertent actuation (undesired opening) of MOV-1.

Circuits that could cause undesirable spurious equipment operations must be identified and evaluated for their effect on safe-shutdown capability. The specific method used to prevent or control spurious equipment operations must be consistent with the potential severity of the spurious actuation. For example, since their inadvertent operation may place the plant in a potentially unrecoverable condition [loss of coolant accident (LOCA)], the spurious opening of valves which form a high/low pressure interface boundary would have a high consequence on the shutdown capability. As discussed in Section 6.3, given the severe consequences associated with this event, high/low-pressure interface boundaries are subject to more stringent analysis criteria. For example, the analysis must consider multiple, simultaneous, hot shorts of the required polarity and sequence as a credible event.

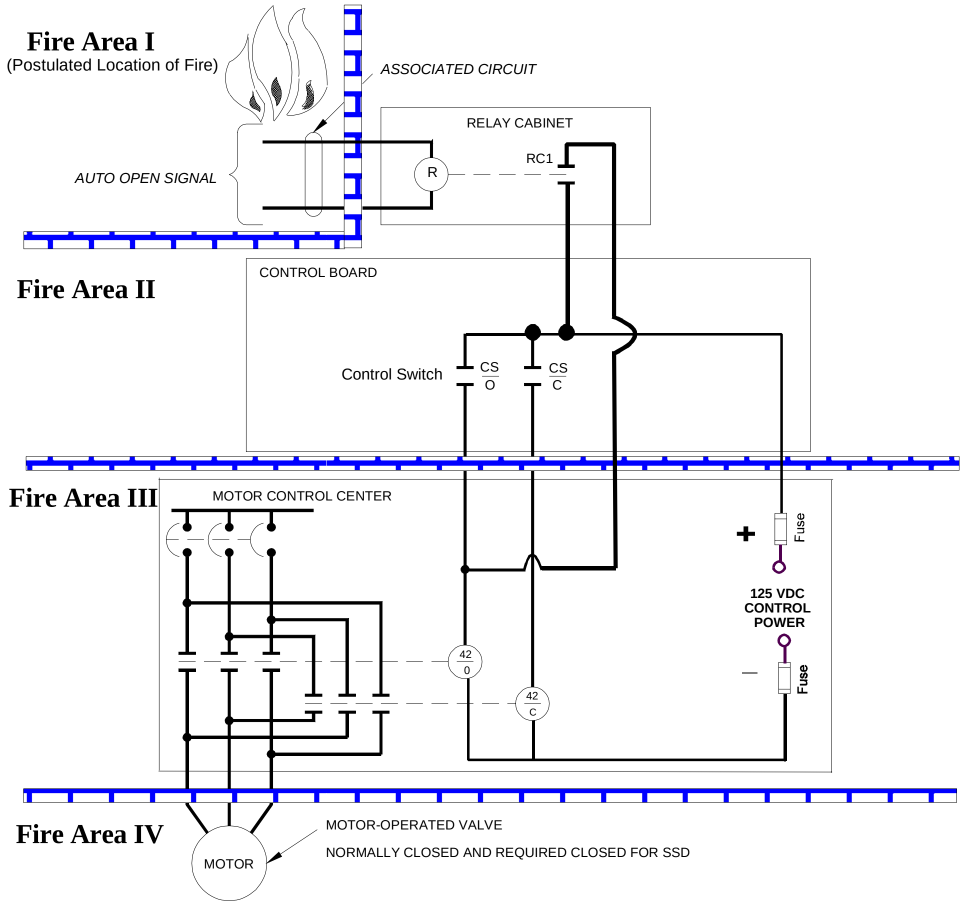


Figure 6-11 Example of the Spurious Actuation Associated Circuit Concern

While the spurious actuation of components having a high consequence on the ability to achieve safe-shutdown conditions must be precluded, other spurious equipment operations may not require this level of protection, provided it can be demonstrated that their inadvertent or “spurious” actuation would not impact on the safe-shutdown capability of the plant. A specific example of this case is a spurious actuation which causes the loss of ventilation in an area containing safe-shutdown equipment. If it can be demonstrated that the required equipment will remain operable (i.e., capable of performing its intended function) for a sufficient length of time without ventilation, plant modifications necessary to preclude the spurious operation may not be necessary.

As described in Section 6.4.4, potential spurious components of concern may be identified from a review of system design documents (e.g., flow diagrams, electrical schematics, etc.). During this review, components of which inadvertent operation could prevent the system from performing its intended shutdown function are identified and included in the SSEL. This list should include components of nonessential systems of which spurious operation could affect the shutdown capability. Once identified, appropriate methods of control can be planned. However, it is imperative that the safe-shutdown analysis include a thorough evaluation of all plant systems so that potential spurious equipment operations of concern can be properly identified for each fire area.

6.4.6 Circuit Analysis

> *"The need to evaluate the effects of fire on circuits associated with the safe-shutdown systems was not explicitly stated in Appendix A to BTP APCSB 9.5-1. It is explicitly required in Appendix R."* (Reference: SECY-80-438A, "Commission Approval of the Final Rule on Fire Protection Program," September 30,1980.)

6.4.6.1 Background/Objective

The evaluation of the consequences of fire in a given fire area must conclusively demonstrate that one train of equipment that can be used immediately to bring the reactor to hot shutdown conditions remains unaffected by fire. The systems and equipment that will be depended upon to perform essential shutdown functions must be identified in the FHA and/or the SSA for the plant. It follows that any circuits or cables in the fire area that could (1) adversely affect the operability of identified shutdown equipment and systems or (2) initiate plant transients that could preclude the successful accomplishment of required shutdown functions, by feeding back potentially disabling fault conditions to power supplies, control logic or instrumentation circuits, must be evaluated and such disabling conditions prevented or appropriately mitigated. Otherwise, reliance on the identified safe-shutdown equipment cannot be ensured.

In addition to establishing protection requirements for redundant trains of systems necessary to achieve and maintain hot-shutdown conditions (i.e., the set of "required" shutdown equipment identified in Section 6.4.4 above), Section III.G.2 of Appendix R further specifies that the ability to achieve and maintain hot shutdown conditions must not be impacted by fire which damages nonsafety circuits that are associated with the required shutdown systems. Additionally, with regard to alternative or dedicated shutdown capabilities, Sections III.L.3 and III.L.7 of Appendix R require the shutdown capability to be independent (physically and electrically) of the specific fire area(s) under consideration and isolated from associated nonsafety circuits such that a postulated fire involving associated circuits will not prevent safe-shutdown.

Associated circuits of concern are defined as cables (circuits) that may affect the safe-shutdown capability and/or prevent the achievement of post-fire safe-shutdown conditions if they are damaged by fire. Associated circuits may be safety-related or nonsafety-related. These circuits are a concern as long as their failure could impact the defined method of achieving and maintaining post-fire safe-shutdown conditions (i.e., the method credited in the plant's SSA). Specific associated circuit configurations of concern to post-fire safe-shutdown include circuits that share a common enclosure or power source with shutdown circuits and circuits that could cause equipment to spuriously actuate in an undesired manner for safe-shutdown. Each of these configurations is described above in Section 6.4.5.

6.4.6.2 Circuit Analysis Criteria and Assumptions

The fire protection design options delineated in Section III.G.2 of Appendix R provide assurance that cables and equipment located in a specific fire area under consideration will remain free of fire damage. It is not deemed possible to accurately predict the manner in which cables or circuits which lack such protection may fail when subjected to fire and its related perils (e.g., fire-suppression system actuation and physical insults resulting from fire-damaged equipment and firefighting activities). Therefore, analytical approaches used to demonstrate an equivalent level of fire safety to that which would be achieved through compliance with the regulation, are expected to assume that the exposed cables (circuits) will be damaged and then evaluate the possible consequences of this damage on the ability to achieve and maintain safe-shutdown conditions. Such an evaluation would require consideration of one or more (i.e., combination) of the following failure modes:

(1) Open circuits resulting in a loss of electrical continuity (see Section 6.4.6)

(2) Short circuits between individual conductors of a multi-conductor cable (see Section 6.4.6).

(3) Short circuits between conductors of different cables (see Section 6.4.6)

(4) "Hot shorts" where un-energized circuits are inadvertently energized by fire damage which causes conductors of different potential to establish electrical contact (short). A "hot-short" may be compared to the actuation of a light switch. Prior to actuation of the switch, the light is off because its conductors are not energized. Following actuation of the switch (or in our case, development of a hot short) a pathway for current flow is completed between the energized conductors and the formally de-energized conductors and the light illuminates (see Section 6.4.6)

(5) Short circuits between conductors of logic circuits located in equipment and cabinets that are exposed to fire damage (e.g., MCCs, control boards, instrument panels).

(6) Direct or "bolted" low-impedance short circuits of energized conductors to grounded reference potentials. (see Section 6.4.5)

(7) Arcing (high impedance) short circuits of energized conductors. (see Section 6.4.5)

Criteria/Assumptions

For the purpose of performing an evaluation of fire-induced circuit failures, the following criteria and assumptions are applicable:

- The fire is assumed to occur anywhere in the fire area and to extend throughout the fire area under consideration. Unless provided with suitable fire protection features (per Section III.G.2 of Appendix R) the fire must be assumed to impact the performance of all equipment and cables located in the fire area.
- Credit cannot be taken for the proper function of any electrical circuit that has not been fully analyzed.
- Credit may be taken for automatic actuation signals to position equipment to the desired shutdown condition but only if it can be demonstrated that the fire will not affect the proper operation of the circuits and equipment that generate the automatic signals. Credit cannot be taken for automatic signals if the equipment or circuits that generate the automatic signals are exposed to fire damage.
- It cannot be assumed that fire will affect any electrical circuit in such a way as to cause equipment to fail in its desired safe-shutdown position.
- There is no limit on the number of circuit/cable faults that may occur as a result of fire damage in a given fire area. Any circuit/cable located in the fire area of consideration that lacks suitable fire protection features (per Section III.G.2) must be assumed to be damaged by the effects of fire and/or its related perils.

- In determining the potential for fire to cause undesired spurious equipment actuations, components other than high/low pressure interface valves, need only consider the effect of a single hot short. However, this single fault (hot short) must be considered to occur in combination with other possible circuit failure modes (open circuits, shorts to ground).
- If it is determined that more than one hot short is required to cause a component to spuriously actuate and the component is not a high/low pressure interface valve *and* the conductors of concern are not located in a single (multi-conductor) cable, then spurious operation of the component is not considered credible. (See Figure 6-11a.)

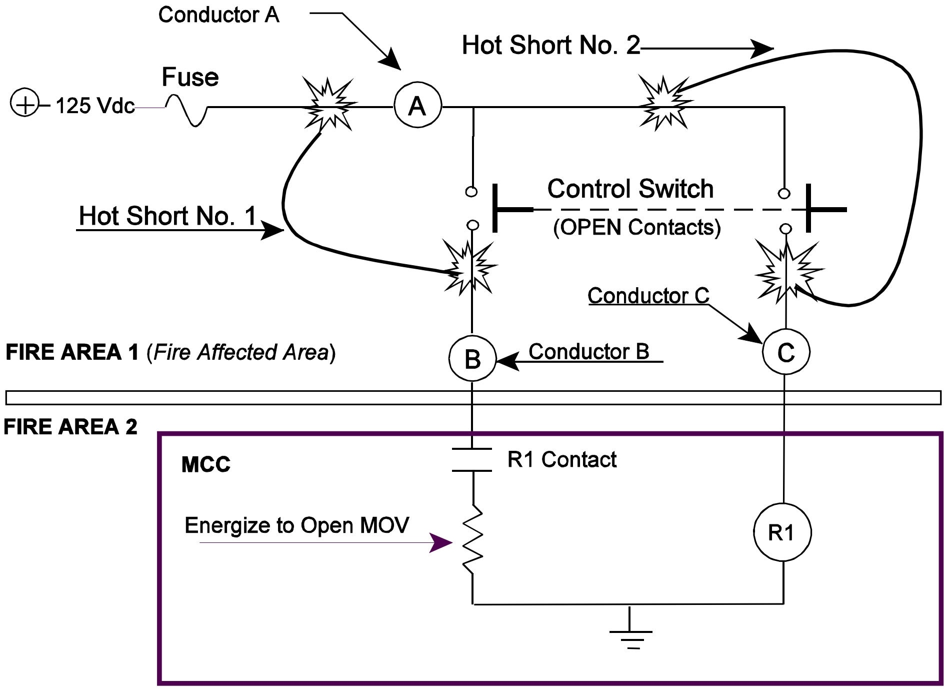


Figure 6.11a Consideration of Multiple Hot-Shorts

For fire in Fire Area 1 Both Hot Short No. 1 [Conductor A to B] and Hot Short No. 2 [Conductor A t o C must occur to cause the spurious opening of the MOV. With the following two exceptions, multiple hot shorts of this nature are not considered credible:

1. For High / Low Pressure interface valves, each valve having exposed circuits in the fire affected area would need to consider the occurrence of multiple hot shorts as a credible event. OR
2. IF: Conductors necessary to cause a spurious actuation (e.g., A, B, and C)are all located in same multi-conductor cable and the cable is not adequately protected from fire damage (per III.G.2)
   THEN : Spurious operation of the component must be considered as a credible event , whether or not the component is part of a High / Low Pressure interface.

- The evaluation of high/low pressure interface components must consider the occurrence of multiple, simultaneous, hot shorts of the required polarity and sequence as a credible event. Given the unacceptable consequences associated with this event, the analysis must consider the occurrence of hot shorts on all three phases of the components power cable in the proper sequence (i.e., Phase A to Phase A; Phase B to Phase B and Phase C to Phase C) as a credible event.
- Multiple conductor-to-conductor hot shorts in cables containing more than a single conductor (i.e., multi-conductor cables) are credible and must be evaluated. It is not sufficient to only consider the effect of a single fault on each conductor on a one at a time basis (see Figure 6-11a).
- “Hot shorts” may result from a fire-induced insulation breakdown between conductors of the same cable (circuit), a different cable (circuit), or from some other external source resulting in an undesired impressed voltage or signal on specific conductors.
- Circuit failures resulting in spurious actuations of equipment must be assumed to exist until action is taken to isolate the affected circuit from the fire area or other actions are taken, as appropriate, to negate the effects of the faulted condition that is causing the spurious actuation. It cannot be assumed that the fire would eventually clear the circuit faults.
- “Open circuits” may result from a fire-induced break in conductors resulting in the loss of circuit continuity.
- “Shorts to ground” may result from a fire-induced breakdown of cable (circuit) insulation, resulting in the conductor being applied to ground potential.
- Where a single fire can impact cables that can cause the spurious opening of high/low pressure interface isolation valves, it must be assumed that all of the affected valves will spuriously actuate *simultaneously*.
- For each fire area all potential spurious operations that may occur as a result of a postulated fire should be identified and evaluated for their impact on the safe shutdown capability. With the exception of components comprising a high/low pressure interface boundary, spurious actuations having the potential to impact the shutdown capability must either be prevented or the effects of each actuation must be appropriately mitigated on a one-at-time basis. That is, the analyst must assume that “any and all” spurious actuations that could occur, will occur, but on a sequential, one-at-a-time, basis. It is not assumed that all spurious actuations that could occur as a result of fire damage will occur instantaneously at the onset of the fire. However, the analyst must consider the possibility for each spurious actuation to occur sequentially, as the fire progresses, on a one-at-a-time basis. In the absence of suitable fire protection features, the potential for such sequential failures to result in the concurrent failure of two or more devices must be considered. Analysis approaches that arbitrarily limit the number of spurious actuations that may occur (such as assuming that only one spurious actuation will occur for each fire event) as a result of fire damage are inconsistent with regulatory requirements. GL 86-10 Question and Answer Section 5.3 provides additional guidance.

- Analysis methodologies that attempt to predict the number of circuit faults and/or spurious equipment actuations that may occur as a result of fire damage to exposed circuits and cables may lack sufficient technical basis may not be valid. For example, without additional justification it is not acceptable to assume that only one spurious actuation or one hot short would occur as a result of fire in any fire area, unless it has been reviewed by the staff for a specific licensee's application.
- All cables, regardless of type or manufacture, including IEEE-383 qualified cables, will support combustion. No credit may be taken for the ability of cables to "self-extinguish".
- For fires requiring implementation of an alternative or dedicated shutdown capability, it is necessary to identify all potential spurious operations that may result from the fire and evaluate the impact of each on the ability to achieve and maintain safe shutdown. Spurious operations could occur on a circuit that is isolated from the fire area under consideration during the time it takes the operator to evacuate the MCR and assume control of the plant at a remote location (e.g., RSP, therefore, spurious operations must be postulated on circuits that can be isolated as well as circuits that cannot be isolated from the fire area under consideration. That is, the potential for spurious operations of equipment to occur prior to actuation of isolation devices (e.g., isolation/transfer switches) must be considered. If the actuation can be appropriately controlled or mitigated by actuation of the isolation/transfer switch, actuation of the transfer switch is considered to be an adequate mitigating action. For those circuits that are not capable of being isolated from the fire area under consideration, it must be assumed that they will spuriously actuate as a result of fire damage on a one-at-a-time, sequential basis.
- A "hot short" between conductors of different cables does not need to be postulated to occur on a safe-shutdown cable that is routed individually (by itself) in a metallic conduit or in a metallic conduit that does not contain other energized circuits (conductors). If this justification is used provisions must be made to ensure that future circuit changes or cable routing modifications do not alter this condition.
- Fire is not expected to damage cables that are routed in "embedded" conduits (i.e., conduits that are located within the confines of a structural concrete floor, wall or ceiling).
- All components are assumed to be in their normal position as shown on the P&IDs.
- Circuit contacts are assumed to be positioned (i.e., open or closed) consistent with the normal mode of the component as shown on the schematic drawings.
- Unless demonstrated otherwise, the effect of fire damage to instrumentation circuits cannot be predicted. That is, the instrument may fail full scale high, full scale low or at some intermediate point. It cannot be assumed that fire damage would always cause an instrument to fail at some pre-determined point (e.g., full downscale, mid-range or full upscale).
- The evaluation of the potential impact of fire-induced spurious actuations on safe shutdown capability must consider all possible failure modes of the equipment or components under consideration. This includes, for example, the potential for fire-induced circuit/cable damage to cause mechanical failure of MOVs as described in IN 92-18.

6.4.6.3 Types of Circuit Failures

Sections III.G.2 and III.L.7 of Appendix R delineate the cable and circuit failure modes that must be considered in the evaluation of post-fire safe-shutdown capability as open circuits, shorts to ground and hot shorts. This section provides specific examples of each of these types of circuit failure conditions.

6.4.6.3.1 Open Circuits

An open circuit is a fire-induced break in a conductor resulting in a loss of circuit continuity. An open circuit will prevent the ability to control or power the affected equipment. Deterioration of fiber optic cables leads to a loss of signal and has a similar effect.

Potential consequences of open circuits on the safe-shutdown capability include, but are not limited to the following:

- a loss of power to required shutdown equipment
- an inability to control essential shutdown equipment
- a loss of power to an interlocked relay or other device that may change the state of the equipment (e.g., a solenoid that is required to remain energized for safe shutdown becomes de-energized)
- an open circuit on the secondary winding of certain types of current transformers may result in initiation of secondary fires at the location of the current transformer. The potential for this occurrence is largely dependent on the rating, type and design of current transformers used and, therefore, must be evaluated on a case-by-case basis

The condition of an open circuit on a grounded control circuit is illustrated in Figure 6-12. In the circuit illustrated an open circuit at location No. 1 is equivalent to a blown fuse — equipment operation will not be possible. An open circuit at location No. 2 will prevent opening or starting of the equipment but will not impact the ability to close or stop the equipment.

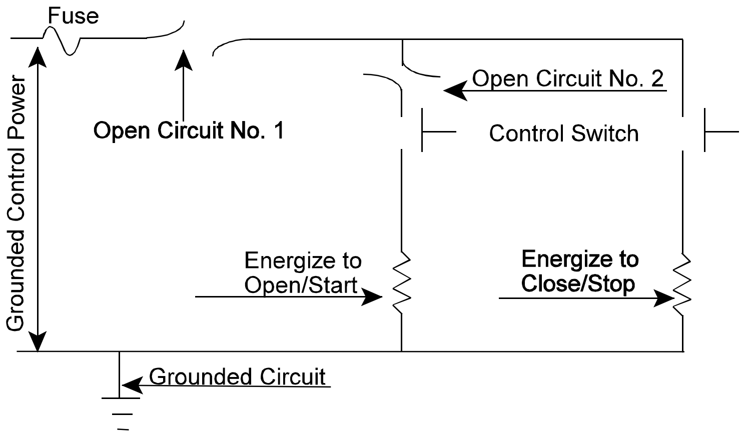


Figure 6-12 Open Circuit Example

6.4.6.3.2 Shorts to Ground: Grounded Circuits

A short to ground results from a degradation (breakdown) of cable/conductor insulation. This fault condition results in a ground potential on the affected conductor. A short to ground can have all of the same effects as an open circuit and, in addition, a short to ground can also impact the control circuit or power train of which it is a part. In the case of a grounded circuit illustrated in Figure 6-13, a short on any part of the circuit would present a concern for tripping the isolation device (i.e., fuse) thereby causing a loss of control power. For the circuit illustrated a short to ground at location No. 1 will result in the control power fuse blowing and a loss of power to the control circuit. This will result in an inability to operate the equipment using the control switch. As discussed in Section 6.4.5.2.1, depending on the coordination characteristics (selectivity) between the fuse and its upstream protective devices (fuses, circuit breakers that provide power to the fuse in this circuit) the power to other circuits could also be affected. This failure mechanism should be evaluated as part of the associated circuits common power source analysis. A short to ground at location No.2 will have no effect on equipment operation until the close/stop control switch is closed. Should this occur the effect will be identical to the short to ground at location No.1. A short to ground at this location would not affect the ability to open/start the equipment until the close/stop control switch is placed in the closed position.

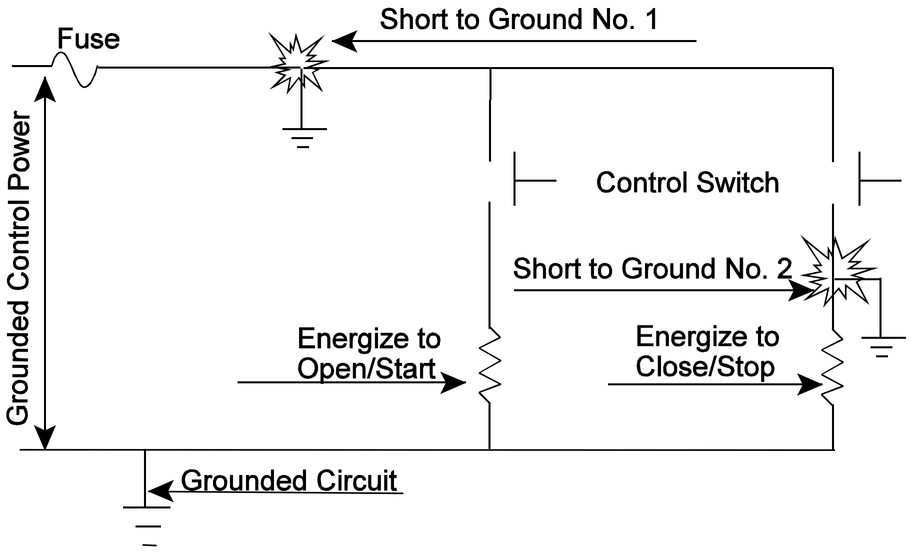


Figure 6-13 Shorts to Ground (Gounded Circuit)

6.4.6.3.3 Shorts to Ground: Ungrounded Circuits

In the case of an ungrounded circuit (such as most 125 VDC control power schemes) a single short to an external ground reference (e.g., cable tray, conduit or metallic enclosure) on any part of the circuit may not cause the circuit isolation device to trip. To illustrate this concept consider the simple light circuit illustrated in Figure 6-14. In this case a battery is being used to supply power to the lamp and there is no reference to any external grounded reference potential, such as a metal cable tray. This is a simple example of an ungrounded circuit. For a circuit such as this, connecting a single wire (to simulate a short) from the positive (+) side of the battery to a grounded cable tray will not have any effect on the operation of the lamp since there is no complete path for fault current to flow back to the battery. However, the occurrence of an additional (second) short on the negative (-) side of the circuit will provide a complete path for current to flow, causing the fuse to blow and resulting in an inability to illuminate the lamp.
It should be noted that the second ground fault may occur as a result of fire damage to this circuit or any other circuit that is also fed from the same ungrounded power source (e.g., battery). Therefore, the potential for an ungrounded circuit to become grounded as a result of fire damage must be considered.

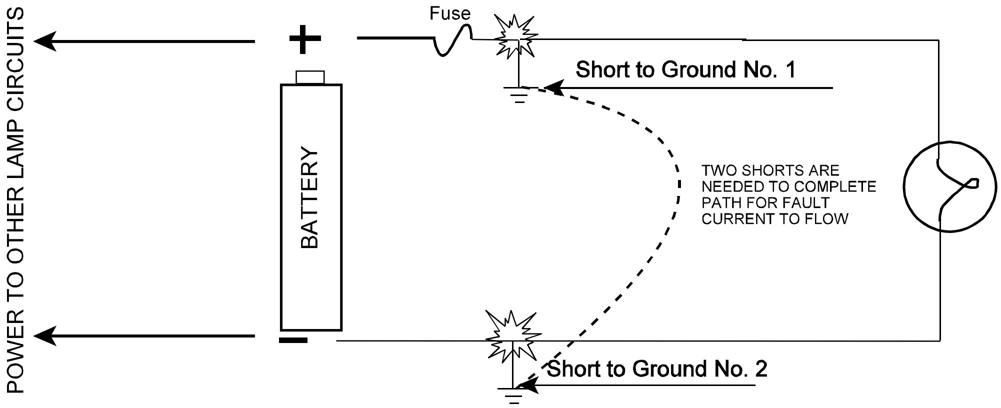

POWER TO OTHER LAMP CIRCUITS
+
BATTERY
−
Fuse
Short to Ground No. 1
TWO SHORTS ARE NEEDED TO COMPLETE PATH FOR FAULT CURRENT TO FLOW
Short to Ground No. 2

Figure 6-14 Ungrounded Circuit Illustration

6.4.6.3.4 Hot Shorts

In a “hot short” fault condition an energized conductor comes in electrical contact with other un-energized conductors. As a result of this fault, (short circuit between conductors) an undesired voltage or signal is impressed on conductors that were previously un-energized. A hot short fault condition may occur between conductors of the same cable, a different cable, or some other external source. An example of a hot short fault condition is illustrated in Figure 6-15. For the circuit illustrated in Figure 6-15, a hot short at location no.1 would energize the open/start relay and result in the undesired (spurious) opening or starting of the equipment being controlled by this circuit. This condition would be unacceptable for safe-shutdown if the desired operating mode of the affected equipment were closed or stop. A hot short at location No.2 would energize the close/stop relay and result in the undesired (spurious) closure or stopping of the equipment being controlled by this circuit. This condition would be unacceptable for safe-shutdown if the desired operating mode of the affected equipment were open/start.

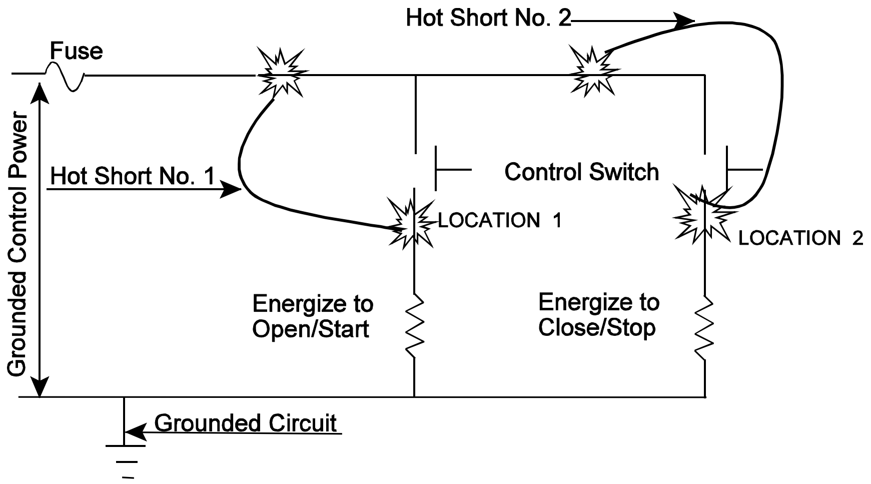


Figure 6-15 Hot Short Example

The hot shorts illustrated in Figure 6-15 are derived from energized conductors in the same circuit. However, it should be noted that the same hot short fault conditions could also be established as a result of electrical contact (short) between locations 1 and 2 and conductors connected to any other energized source, including those that may be external to this circuit.

In the case of an ungrounded circuit, a single hot short may be sufficient to cause a spurious actuation. A single hot short can cause a spurious actuation 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 actuation. In reviewing these cases, the “common denominator” is that in every case, the conductor in the circuit between the control switch and the control coils (open/start or close/stop) must be involved.

Given the possibility of a short to ground being caused by the fire, it should be assumed that a spurious operation will result whenever the fire affects the conductor between the control switch and the control coils. Since a hot short from the same source or grounding of ungrounded circuits cannot be ruled out, it should be assumed that ungrounded circuits will behave the same as grounded circuits in their response to hot shorts.

6.4.7 Locate Equipment, Cables, and Circuits of Concern to Post-Fire Safe Shutdown

At this point in the analysis process, plant process and support *functions* that must be accomplished to achieve and maintain hot and cold shutdown conditions have been defined (Section 6.4.2), *shutdown systems* (redundant and/or alternative) capable of accomplishing each of the required shutdown functions have been determined and assigned a unique safe-shutdown path designation (Section 6.4.3). With the shutdown paths defined, the equipment needed to ensure the proper operation of each path is identified and documented in the SSEL (See Sections 6.4.4). The SSEL establishes a starting point for identifying *required circuits and cables* (i.e., circuits and cables needed to support operation of the identified shutdown paths) ***as well as*** *associated nonsafety circuits* that could impact (adversely affect) the achievement of safe-shutdown conditions if they are damaged by fire. (See Section 6.4.5.) Following their identification, associated circuits of concern are then evaluated to assess the potential impact of fire and related perils (e.g., fire suppression activities) on the shutdown capability of the plant. (See Section 6.4.6.)

As discussed in Section 6.1, the post-fire safe-shutdown analysis is performed on a fire area basis. With the equipment, circuits and cables of concern to post-fire safe-shutdown identified, their physical location in the plant is then determined. The specific fire area where each piece of shutdown equipment is located may be determined from a comparison of plant design documents (e.g., equipment layout drawings) to the fire area delineations identified in the FHA. The location of this equipment (i.e., fire area) should then be verified as necessary by field walkdowns and entered into the SSEL.

The routing of cables, including all raceway and cable endpoints, may be determined from a review of plant design drawings (e.g., conduit and cable raceway drawings) and/or cable installation data (e.g., cable pull tags). In certain cases, cable routing information may be obtained by joining the list of safe-shutdown cables with an existing cable and raceway database. For either case, field walkdowns should be performed as necessary to confirm the accuracy of the design information used in the evaluation.

To understand the potential impact of an exposure fire within each fire area, the results of the preceding evaluations should be tabulated in a report that includes such information as:

- fire area designation, location, and description
- shutdown path/systems relied on to achieve SSD [required path(s)]
- potentially affected unit(s)
- potentially affected shutdown path/system
- potentially affected cables [identify function (power, control, instrument) and whether damage can result in a spurious actuation, SSD path/system, affected equipment]
- potentially affected equipment (ID, type, description, SSD path, location, normal operating mode, required operating mode/position for SSD, etc.)

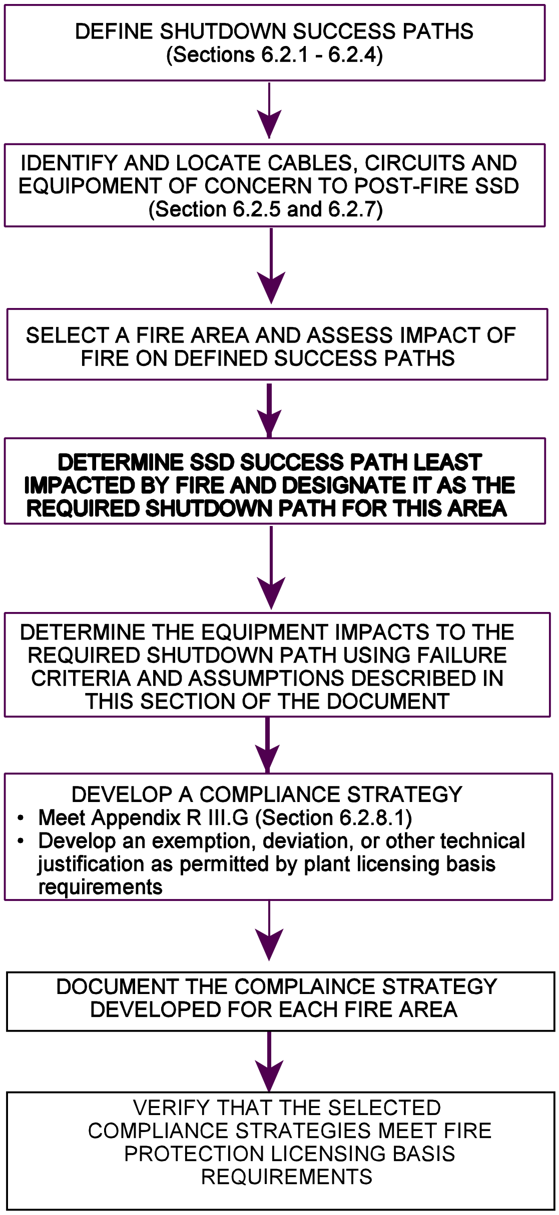
6.4.8 Perform Fire Area Assessments

For each fire area the evaluation of the consequences of fire must conclusively demonstrate that one train of equipment that can be used immediately to bring the reactor to hot shutdown conditions remains unaffected by fire. Systems needed to achieve and maintain cold shutdown may be damaged by fire but the extent of damage to these systems must be limited so that any necessary repairs can be implemented and shutdown conditions achieved within the time constraints described in Section 6.4.1.4.

There are many acceptable approaches to achieve the above objectives and the NRC does not prescribe or endorse any one specific approach. The approach presented in this document starts by defining safe-shutdown success paths (See Section 6.4.1–Section 6.4.5) and then each fire area is evaluated to determine the affected equipment in each fire area. From the resulting list of affected equipment, the impact of fire on the ability to achieve and maintain safe-shutdown conditions can be determined for each area. The various steps involved in this approach are illustrated in Figure 6-16. Another approach may start with the fire area and identify the redundant divisions (trains) of equipment and cables that are located in the fire area. From this information a shutdown success path that relies on the use of equipment associated with the "least affected" division could be developed. With the shutdown success path determined for the area, the impact of any interactions between cables and equipment in the area can then be assessed.

Regardless of the approach used, the SSA should be a bounding analysis which identifies the range of possible fire impacts within each fire area and ensures that appropriate measures are in place to prevent this damage from affecting the ability to safely shutdown the plant. For each fire area, the SSA must define a set of systems and equipment that are capable of accomplishing the required shutdown functions in accordance with established performance criteria.

The degree of physical separation provided for redundant trains of shutdown systems may vary widely among plants. Later generation plants that were designed and/or constructed after the Browns Ferry fire, tend to have a greater amount of physical separation inherent in their design. Older plants, however, (typically those receiving an operating license prior to the promulgation of Appendix R) typically were not designed with this concept in mind. Regardless of plant vintage however, the evaluation of a specific fire area may find at least one shutdown success path to be completely independent (both physically and electrically) of the fire area under evaluation. For these cases, the method(s) [e.g., SSD success path(s)] available to achieve safe-shutdown in the event of fire in the area is documented and no further evaluation is necessary. In other cases, however, an adequate level of separation may not already exist (i.e., at least one train of shutdown equipment/shutdown path is *not* independent of the fire area). For these cases, at least one shutdown success path must be identified and provided with suitable fire protection features as described below.


DEFINE SHUTDOWN SUCCESS PATHS
(Sections 6.2.1 - 6.2.4)
IDENTIFY AND LOCATE CABLES, CIRCUITS AND EQUIPOMENT OF CONCERN TO POST-FIRE SSD
(Section 6.2.5 and 6.2.7)
SELECT A FIRE AREA AND ASSESS IMPACT OF FIRE ON DEFINED SUCCESS PATHS
DETERMINE SSD SUCCESS PATH LEAST IMPACTED BY FIRE AND DESIGNATE IT AS THE REQUIRED SHUTDOWN PATH FOR THIS AREA
DETERMINE THE EQUIPMENT IMPACTS TO THE REQUIRED SHUTDOWN PATH USING FAILURE CRITERIA AND ASSUMPTIONS DESCRIBED IN THIS SECTION OF THE DOCUMENT
DEVELOP A COMPLIANCE STRATEGY
• Meet Appendix R III.G (Section 6.2.8.1)
• Develop an exemption, deviation, or other technical justification as permitted by plant licensing basis requirements
DOCUMENT THE COMPLAINCE STRATEGY DEVELOPED FOR EACH FIRE AREA
VERIFY THAT THE SELECTED COMPLIANCE STRATEGIES MEET FIRE PROTECTION LICENSING BASIS REQUIREMENTS

igure 6.16 Fire Area Assessment Flowchart

One train of systems necessary to achieve and maintain hot shutdown conditions must be free of fire damage (Appendix R Section III.G.1.a). For cases where adequate fire area separation does not exist (i.e., redundant trains of shutdown systems are located in the same fire area), Section III.G of Appendix R provides several options for ensuring that the hot shutdown capability is protected from fires. The first three options, as defined in Section III.G.2, provide the following methods for protecting redundant trains of equipment located in fire areas that are *outside* of non-inerted containments:

- Enclose one of the redundant systems, including cables, equipment and associated nonsafety circuits, in a 3-hour fire-rated barrier. (III.G.2.a)
- Separate redundant systems, including cables, equipment and associated nonsafety circuits, by a horizontal distance of more than 6.08 m (20 ft) with no intervening combustibles or fire hazards. In addition, fire detection and an automatic fire-suppression system are required. (III.G.2.b)
- Enclose redundant systems (including cables, equipment and associated nonsafety circuits) in a 1-hour fire-rated barrier. In addition, fire detection and an automatic fire-suppression system are required. (III.G.2.c).

The next three options, as defined in Section III.G.2, provide methods for protecting redundant trains of equipment located in fire areas that are *inside* non-inerted containments:

- Separate redundant systems, including cables, equipment and associated nonsafety circuits, by a horizontal distance of more than 6.08 m (20 ft) with no intervening combustibles or fire hazards. (III.G.2.d)
- Install fire detection and an automatic fire suppression systems. (III.G.2.e)
- Separate redundant systems (including cables, equipment and associated nonsafety circuits) by a noncombustible radiant energy shield. (III.G.2.f)

The last option, as defined by Section III.G.3, provides an alternative or dedicated shutdown capability to the redundant trains damaged by a fire:

- Ensure that alternative (or dedicated) shutdown equipment are independent (both physically and electrically) of the cables, equipment, and associated nonsafety circuits of the redundant systems damaged by the fire.

CHAPTER 7. MAINTAINING POST-FIRE SAFE-SHUTDOWN:
Configuration Management for Post-Fire Safe-Shutdown Analysis

A post-fire safe-shutdown analysis is based on a “snapshot” of the configuration of plant SSCs and cable routing information that existed at the time the analysis was performed. However, the plant design features and operating practices that form the basis of the analysis are rarely static. Over its operating life, a plant may make modifications to improve its safety, reliability, and efficiency. If not properly evaluated, plant modifications can significantly compromise the results presented in the SSA and, in certain instances, may threaten the plant’s ability to achieve and maintain safe-shutdown conditions in the event of fire. Effective maintenance of the plant’s post-fire safe-shutdown capability, as described in the SSA and its supporting calculations and procedures, requires that all proposed changes to the plant design and operations, whether permanent or temporary, must be evaluated for their impact on the shutdown capability.

Figure 7-1 illustrates how even a seemingly straightforward modification involving the installation of nonsafety-related equipment can impact the shutdown capability. In this case, the licensee is making a modification to provide a more efficient means of transferring water between two nonsafety-related tanks. Key components being added as part of this modification include a pump (Pump X), piping, a nonsafety-related SWGR (SWGR 1A-1), motor-operated pump suction and discharge valves, and related controls and instrumentation. The pump is to be located in a fire area where the SSA credits the use of Division B equipment and is to be powered from a new Division A power source (SWGR 1A-1).

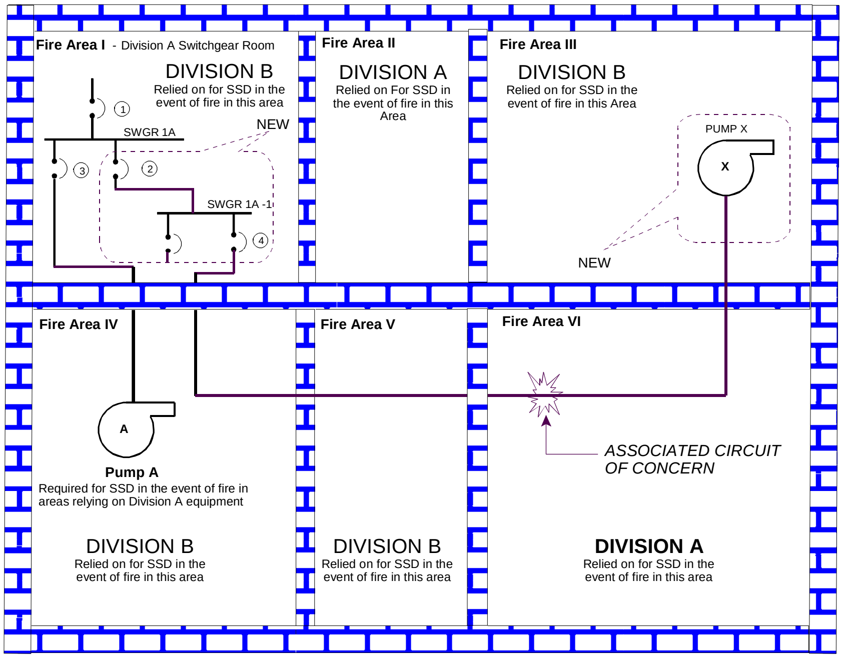

Fire Area I - Division A Switchgear Room
DIVISION B
Relied on for SSD in the event of fire in this area
1
SWGR 1A
NEW
3
2
SWGR 1A -1
4
Fire Area II
DIVISION A
Relied on For SSD in the event of fire in this Area
Fire Area III
DIVISION B
Relied on for SSD in the event of fire in this Area
PUMP X
X
NEW
Fire Area IV
A
Pump A
Required for SSD in the event of fire in areas relying on Division A equipment
DIVISION B
Relied on for SSD in the event of fire in this area
Fire Area V
DIVISION B
Relied on for SSD in the event of fire in this area
Fire Area VI
ASSOCIATED CIRCUIT OF CONCERN
DIVISION A
Relied on for SSD in the event of fire in this area

Figure 7-1 Modification Impacting the SSD Capability

The proposed design also includes the following attributes:

- The pump and the entire system in which it is located will not need to remain operational to accomplish required shutdown functions.
- Maloperation of the pump (e.g., an unintended start or stop) would have no impact on the shutdown capability of the plant.
- The pump is powered from a nonsafety-related power source (SWGR 1-1A) that does not power any safe-shutdown components. A fire-induced loss of SWGR 1-1A would not impact safe-shutdown.
- The power source (SWGR 1-1A) is physically located in a fire area where equipment from the redundant division (Division B) is relied on to accomplish post-fire safe-shutdown.
- Before installing this modification, the SSA demonstrated an acceptable level of coordination between load and feeder breakers of SWGR 1A.

While these considerations may suggest that the planned modification would not impact the plant's post-fire safe-shutdown capability, a potential vulnerability still exists. Specifically, as shown in Figure 7-1, the cable that provides power to Pump X traverses several fire areas. Note that this routing includes an area (Fire Area VI) where Division A equipment (including required SSD Pump A powered from SWGR 1A) is relied on for post-fire safe-shutdown. Because the cable has not been provided with fire protection features (e.g., rated barrier wrap), it is susceptible to fire damage. If this modification were to be installed without ensuring that the new circuit breakers installed in SWGR1A (Breaker 4) and SWGR 1A-1 (Breaker 2) properly coordinate with the upstream feeder breaker (Breaker 1), a fire in Fire Area VI could cause Breaker 1 to trip and, thereby, result in the loss of equipment (Pump A) that is relied on to accomplish essential shutdown functions in the event of fire in Fire Area VI. (Refer to Section 6.4.5.2.1 for a more detailed discussion of circuit breaker coordination.)

Other examples of plant changes that may affect the shutdown capability include replacing a passive component (e.g., a manual valve) with an electrically controlled device (e.g., an MOV), rerouting cables, replacingf circuit protective devices (fuses, circuit breakers, relays), installing or removing interlocks, modifying control circuits (e.g., changing from manual to automatic control), making temporary modifications to facilitate plant maintenance activities (e.g., welding), and changing the plant's operating procedures (normal, abnormal or emergency).

Requirements governing the fire protection of safe-shutdown capability must be maintained over the life of the plant. This capability is provided through the establishment of administrative control procedures, which specify that changes in plant design and operations (both permanent and temporary) must be subjected to an appropriate level of review. This assessment must be performed by qualified personnel knowledgeable of the plant's post-fire safe-shutdown analysis. These procedures must address the following specific configuration control issues:

- **Modifications:** All modifications (i.e., permanent or temporary additions, deletions, or changes) to plant SSCs must be reviewed for their potential impact on the plant's post-fire safe-shutdown capability (as documented in the SSA, its supporting calculations, and procedures).
- **Fuse Replacement and Changes in Circuit Breaker or Relay Settings:** Ensure that fuses, circuit breakers, and relays having ratings or settings other than those selected to ensure proper coordination for post-fire safe-shutdown are not accidentally used. To ensure that future plant changes will not compromise circuit breaker and fuse coordination studies referenced in the SSA, the replacement of fuses in power sources required for post-fire safe-shutdown should be performed in accordance with approved procedures. In addition, the coordination study should be maintained current with the most recent modification.
- **Procedure Changes**: The review of permanent and/or temporary procedure changes should consider the following factors:
  (a) the effects of the change on the plant's capability to achieve and maintain post-fire safe-shutdown
  (b) changes to responsibilities and tasks assigned to fire brigade members
  (c) changes to responsibilities and tasks assigned to operations staff members who are responsible for achieving and maintaining safe-shutdown from inside the control room and from alternative shutdown location(s)

This page intentionally left blank.

CHAPTER 8. INTEGRATION OF DETERMINISTIC CRITERIA AND RISK-INFORMED INFORMATION

8.1 Overview of a Risk-Informed Approach

It is NRC policy to increase the use of risk information in the regulatory decisionmaking process (Reference Final Policy Statement, 1995). Risk combines two factors, including (1) the likelihood (or frequency) that an event will occur and lead to undesired consequences and (2) the severity of those undesired consequences. In this chapter, the event of interest is a fire that challenges nuclear safety. The potential undesired consequence of such an event is an offsite release of radioactive materials. For the commercial nuclear power industry, the severity of the release consequences is measured by the potential impact on public health.

In practice, risk is usually quantified using probabilistic risk assessment (PRA). PRA results are most often expressed using two intermediate risk measures; namely, CDF and large-early release frequency (LERF)[27]. CDF reflects the frequency (in events per reactor year) with which a given plant might expect to experience an accident leading to core damage. LERF reflects the frequency with which one might expect an accident to occur and lead to a large release of radioactive materials relatively early in the accident sequence. In this context, the term “early” is measured in relation to population evacuation times. Both CDF and LERF are considered indirect measures of risk because they do not directly quantify the public health consequences of potential plant accidents. CDF and LERF are used as risk measures because they are generally indicative of the potential that public health consequences might occur.

The NRC’s risk-informed policy, as embodied in RG 1.174, weighs regulatory compliance issues against both CDF and LERF criteria. To date, the NRC has not formally risk-informed the fire protection portions of the regulatory requirements (e.g., Appendix R to 10 CFR Part 50). However, aspects of the fire protection regulatory process have begun to incorporate risk information. For example, the NRC staff is currently engaged in a rulemaking activity related to the recently adopted 2001 Edition of the National Fire Protection Association Standard 805 (NFPA 805), “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plant.” NFPA 805 utilizes risk information in evaluating the acceptability of proposed plant changes that impact fire protection. A second example is the significance determination process (SDP) and, in particular, the fire protection SDP, which assesses fire-related inspection findings based on risk measures.

The current discussion is intended to provide risk-informed perspectives on the post-fire safe shutdown circuit analysis issues for use by the NRC staff and, in particular, those staff members responsible for plant inspection activities. The discussion does not establish any new requirements or regulatory compliance criteria. Rather, the discussion is intended to assist the NRC staff in understanding, and potentially assessing, the risk-significance of the fire-related safe-shutdown circuit analysis issue.

[27] Note that the calculation of CDF is also known as the Level 1 analysis. Level 2 refers to the containment performance analysis (e.g., LERF), and Level 3 refers to the analysis of offsite release and public health consequences.

It should be noted that fire-induced circuit failure modes and effects risk analysis is an area of ongoing technical discussion and development. Some aspects of the problem are in their first stages of application, and quantification methods have not yet been fully developed or demonstrated. Hence, this discussion is preliminary and subject to change as additional insights develop. Efforts to further develop risk analysis methods for fire-induced circuit faults is ongoing through the NRC's Office of Nuclear Regulatory Research (RES). More detailed discussions on this topic can, for example, be found in LaChance, et al., 2000.

8.2 Fire Risk Analysis Overview

For the purposes of this chapter, risk insights will be discussed in the context of CDF as the primary risk measure of interest. It should be recognized that the success criteria assumed in a typical fire PRA are not the same as those applied in a regulatory fire protection framework. In the regulatory context, the fire safe-shutdown analysis considers the ability to achieve both hot and cold shutdown. Hot shutdown must be possible within 24 hours, and the regulations do not allow for hot shutdown repair actions. Cold shutdown has a longer mission time, 72 hours, and, within certain limits, repair actions are allowed. In contrast, a typical PRA considers success to be achieving and maintaining a stable hot shutdown condition such that core damage is prevented. In a typical PRA, scenarios are analyzed until a safe and stable plant condition is achieved, but generally only out to 24 hours. (Note that the potential for core damage accidents that occur beyond this period should not be dismissed out of hand.) PRAs do not generally consider cold shutdown. Hence, the PRA/CDF success criteria align most closely with the regulatory hot shutdown requirements. The only correspondence to the regulatory cold shutdown requirements would be found in a low power and shutdown fire risk analysis and very few of these have been performed to date. This section provides an overview of current fire CDF quantification practice. This overview provides a convenient framework for our discussion of risk perspectives on post-fire safe-shutdown circuit analysis.

Both regulatory requirements and fire PRAs focus first and foremost on the fire hazard, or risk, associated with fires that impact some bounded region of the plant. However, how these bounded regions are defined in the regulatory context often differs from the definitions used in a fire PRA. In the regulatory context plants are partitioned into fire areas; that is, physical regions that are bounded on all sides by fire-rated boundary elements sufficient to contain the fire hazards(RG 1.189). Fire PRAs are generally based on fire compartments[28], a less rigorously defined subdivision of the plant. In a fire PRA, a given fire area may be retained in whole as a fire PRA compartment, or the fire area may be partitioned into two or more fire compartments. Defining fire PRA compartments involves the application of analyst judgment. Fire PRA compartments may credit features that would not be credited in defining fire areas in the regulatory context. This may include non-fire-rated partitions, partitions with unsealed penetrations, active partitions (e.g., heat activated roll-up doors), water curtains, and even extended spatial separation. In most fire PRAs, each fire compartment represents a region wherein, based on the judgement of the analyst, the damaging effects of the majority of fires are expected to be confined.

[28] Note that the terminology applied varies between analyses. Some analysts may refer to fire zones, analysis zones, rooms, or other designations to describe the physical analysis boundaries drawn to support the fire PRA. The concept remains the same.

The CDF analysis systematically considers risk contributions arising from fires in each fire compartment. The risk quantification results may be reported at a fire scenario level (e.g., for a given fire ignition source), but are more typically reported at a compartment level. Hence, PRAs will often cite a CDF contribution for each individual fire compartment (e.g., the Cable Spreading Room). An explicit analysis is also conducted to assess the risk contribution of fires that might impact multiple fire compartments. The results for the multi-compartment (or room-to-room) fire scenarios are often reported separately. It is also common to report a total fire-induced CDF for the plant as a whole (i.e., the sum of the individual compartment and multi-compartment contributors).

In the most general terms, the likelihood that a fire might initiate a core damage accident is assessed on the basis of the following three-factor formula:

$$CDF = \sum_{i} f_{i} \left(\sum_{j} P_{cd,j|i} \left(\sum_{k} P_{CD:k|i,j} \right) \right)$$

The first term (f_i) on the right-hand side represents the fire occurrence frequency. The summation over the index “I” implies that the plant-wide fire-induced CDF is based on the sum of contributions from many individual fires involving a number of fire compartments. Fire frequency includes consideration of both fixed (e.g., fixed electrical and mechanical equipment; fixed components that might experience a leak of lubricating oil or flammable gases including hydrogen; semi-permanent storage items; etc.) and transient fire ignition sources (e.g., maintenance materials staged in anticipation of an outage, inservice maintenance support materials, welding and cutting operations, refuse, etc.).

Consistent with the fire PRA plant partitioning practices as described previously, fire frequency may be quantified at a compartment level reflecting all possible fire ignition sources in a given fire compartment (e.g., a battery room). However, fire frequency may also be quantified at a more detailed level. For example, fire frequency may be expressed for a particular fire ignition source (e.g., a motor or pump), or for a specific group of fire ignition sources (e.g., a bank of SWGR or general transient fuel sources). Fire frequency is usually based on statistical analysis of the evidence provided by past fire events; i.e., a fire event database. A number of such databases are available from both public and private sources. (Reference NUREG/CR-4586 and EPRI TR-1000894.)

The second term ($P_{cd,j|I}$) reflects the conditional probability that, given a particular fire (I), a particular physical damage state (j) will be induced. The physical damage state is defined by the plant equipment, components, and/or electrical cables damaged by the fire. Note that the nomenclature P_{cd} implies the **p**robability of either “component damage” or “critical damage,” depending on the analysts’ use of terminology. The second summation implies that a given fire might lead to more than one physical damage state depending, for example, on the duration of the fire and, by implication, the physical extent of fire damage. Calculation of the component damage term typically involves the analysis of fire growth behavior, component thermal response and damage, and fire detection and suppression. It is in this part of the analysis that fire models, for example, are applied.

Given the first and second terms, the analyst is postulating that a fire has occurred and has damaged some set of plant components. The loss of some plant components implies that some subset of the plant systems and/or functions are damaged and/or rendered inoperable. The third and final term ($P_{CD,k|i,j}$) reflects the conditional probability that given the physical damage state (j) resulting from the fire (I), operators will fail to achieve safe-shutdown and **c**ore **d**amage will result. Summation over the index (k) implies that for a given physical damage state, the plant will still have available various options (or paths) for achieving safe-shutdown. Each safe-shutdown path will have a unique likelihood of success/failure. The calculation of P_{CD} includes consideration of system faulting behaviors given the fire damage, operator performance, and random equipment failures independent of the fire. The summation of the contributions from each failure path leading to core damage is often referred to as the conditional core damage probability (CCDP) associated with a given physical plant damage state.

The risk importance of any given fire compartment can be weighed in terms of the absolute CDF contribution and based on the relative contribution of a given fire compartment to the overall fire CDF. For example, even if a plant has a total fire CDF that is considered low, the fire PRA will still typically identify and analyze in detail the risk-dominant fire compartments; that is, those compartments that contribute most to fire risk. Typically, on the order of two-to-ten fire compartments are found to dominate the plant fire risk estimates. The risk-dominant fire compartments often include areas such as the main control room, cable spreading room, auxiliary electrical equipment or relay rooms, and emergency SWGR areas. Other compartments may be risk important on a plant-specific basis.

One of the most significant factors in determining which compartments are fire risk dominant is the routing of important power, control, and instrument cables through the plant. Fire risk is often dominated by fires leading to the failure of electrical cables. Hence, fire compartments through which important electrical cables pass tend to be fire risk-dominant. A second significant factor is the presence, or absence, of significant fire ignition sources in a fire compartment. For example, even a fire compartment such as the cable spreading room may be found to have a relatively low fire risk if it lacks significant fire ignition sources.

Many fire compartments will ultimately be found to contribute little to plant risk. In a fire PRA, a formal process is used to ‘screen out’ such compartments. The first screening step is usually based on qualitative arguments. For example, compartments that contain no safety-related equipment or electrical cables, and where fires cannot induce a plant transient (e.g., manual trip), are often qualitatively screened as insignificant risk contributors. A second stage of screening is typically conducted based on conservative quantification of the three-factor formula cited previously. Quantitative screening generally focuses on the potential severity of fire damage and the likelihood of core damage given fire damage (i.e., the second and third terms). Compartments will rarely screen on fire frequency alone because virtually all compartments have a non-trivial fire frequency (generally no less than $1x10^{-4}$ fires per reactor year, or $1x10^{-4}$/ry and often higher).

It is important to note that fire PRAs usually credit components, systems, and functions that are not credited in the post-fire safe-shutdown analysis[29]. The post-fire safe-shutdown analysis is, first and foremost, intended to ensure that one train of equipment necessary to achieve and maintain safe shutdown will remain free of fire damage. However, other plant systems not credited in the post-fire safe-shutdown analysis will likely survive any given fire event and, in reality, could be used as available to support the post-fire plant recovery efforts. This fact presents a sometimes difficult challenge to fire risk analysis. Fire is a very spatially-oriented phenomena. Even given a rather severe fire, fire-induced component and electrical cable failures will likely occur only in a specific and limited physical region of the plant. Hence, accurate information on component and cable locations is often critical to the fire damage analysis. The more accurate the available information is, the more accurate the risk estimates can be made.

Because the post-fire safe-shutdown analysis is, in essence, a success-path analysis, it credits a limited subset of the plant systems. The electrical cables and components required to support these credited systems are traced within the plant and their locations are generally well known, at the least to the level of their presence in, or absence from, each fire area. However, for systems not credited in the safe-shutdown analysis, the associated components and electrical cables may not be traced and their locations may not be known. To avoid undue optimism, the analyst must verify that a fire cannot cause damage to a system’s components and electrical cables before credit for the system’s function can be taken in the risk analysis. For those systems not credited in the safe-shutdown analysis, this can require tedious and time consuming efforts, in particular, to trace electrical cables through the plant. An approach that is often taken is to assume failure of a system unless the lack of a fire threat to the system’s components and electrical cables can be verified for a given fire scenario. If the failure assumption is found to be critical to the quantification, then additional verification and cable tracing efforts may be undertaken.

8.3 Circuit Analysis and the Risk Analysis Framework

It is now possible to express the issues of circuit analysis in the context of the computational framework described previously. The first term in the CDF equation, the fire frequency, has essentially no interaction with the circuit analysis issues. Similarly, the second term, the likelihood that the fire will lead to some level of physical damage, is also not directly relevant to the circuit analysis issues. Circuit analysis comes into play through the third term, the likelihood that the fire-induced equipment failures will lead to core damage. In this context, we are especially interested in the fire-induced failure of electrical cables.

A fire may cause failures in power, control/indication, and/or instrument cables associated with various plant systems and functions. The response of the impacted systems, the circuit or system fault mode, will depend on the mode of electrical cable failure observed. The process of examining the various electrical cable failure modes in order to identify the potential circuit or system fault modes is referred to here as the process of circuit analysis. More formally, this is referred to as the electrical cable failure modes and effects circuit analysis.

[29] Note that some methods used in the Individual Plant Examination External Events (IPEEE) studies credited only the Appendix R systems (NUREG/CR-1742). When rigorously applied, such approaches typically yield conservative estimates of fire risk.

Circuit analysis is complicated in part because electrical cables may experience one or more of several failure modes. Furthermore, the failure behavior may be dynamic, changing throughout the course of the fire event. Each unique combination of electrical cable failures can potentially induce a unique circuit fault mode. Circuit fault modes of potential interest include loss of function, loss of control, loss of indication, corrupted indications or signals, and spurious actuation. Since the electrical cable failure behavior may be dynamic, the circuit's faulting behavior may also be dynamic. To illustrate, consider that two of the possible cable failure modes of particular importance are hot shorts and shorts to ground. Conductor-to-conductor short circuit cable failure modes, including hot shorts, are likely to transition to shorts to ground given an enduring fire exposure. Therefore, in some cases it may be important to assess both the initial cable failure mode, the anticipated duration of a specific failure modes, and the impact of an ultimate short to ground. As the fire scenario develops, multiple cables may fail at discrete points in time, and multiple circuit faults may come into play. This introduces the further question of concurrent behavior involving multiple circuits; for example, how likely is it that two or more circuits might experience concurrent spurious actuations.

It is not possible to exhaustively explore all of the potential electrical cable failure modes in a fully dynamic context for any but the most simplistic of fire damage state scenarios. Hence, it is widely recognized that some optimization of the circuit analysis process is both necessary and desirable. The specific optimization framework being discussed here is fire-induced core damage risk. That is, the process of circuit analysis is optimized to focus attention on those electrical cables, cable failure modes, and circuit fault modes that may be risk significant.

Typically, a given circuit or system will have a limited set of specific fault modes that will be unique in the context of fire risk. Depending on the circuit, some fault modes may be benign while others might challenge the safe-shutdown process. For example, loss of function in a valve may have little risk impact if operation of the valve is not required to mitigate the accident scenario. However, spurious actuation of that same valve might challenge safe-shutdown by opening an undesired coolant flow diversion path, or by closing a desired coolant flow path.

Circuit faulting behavior influences the likelihood of successful shutdown in three primary ways:

- Circuit faulting can lead to the unavailability of one or more desired plant systems.
- Circuit faulting might cause the maloperation of one or more plant systems (e.g., a spurious actuation or change of operational state).
- Circuit faulting may compromise instrument and control signals that operators depend on in their response to the event (e.g., the loss of control and instrument signals, or transmission of corrupted signals).

Each of these circuit faulting effects can have unique implications for fire risk. The practical objective of PRA circuit analysis is to identify the risk-important circuits and circuit fault modes, and to then quantify the likelihood that such faults might be observed during a given fire. Insights gained to date related to this objective are discussed below.

8.4 A Mechanistic View of the Problem

A mechanistic view of the circuit analysis problem is being developed in support of broader fire PRA development activities (LaChance, et al., 2000). As an entry condition to the fire PRA circuit analysis task, it is assumed that fire modeling tools of some type (potentially including expert judgement) have been applied separately and have predicted the failure of one or more electrical cables. Under the mechanistic view of circuit analysis, the problem is first split into two major pieces; namely, the electrical cable failure mode analysis and the circuit fault mode analysis. The discussions provided in this chapter are organized based on this mechanistic view.

The cable failure mode analysis addresses the short circuiting behavior of the damaged electrical cables. That is, given electrical cable failure, an analysis is performed to determine the relative likelihood that a particular mode of cable failure will occur. The circuit fault mode analysis considers the potential responses of the circuit to various cable failure modes. For example, the circuit fault mode analysis determines whether or not spurious actuation is possible given failures involving a particular electrical cable, and if so, what combination(s) of conductor shorting behaviors could lead to a spurious actuation fault mode.

There is a degree of iteration between the cable failure mode and circuit fault mode analyses. The circuit fault mode analysis will likely identify a unique combination of conductors that, if they short together, would cause a spurious actuation. Furthermore, the circuit fault mode analysis might also find that if one particular conductor were to become involved in the short circuit (e.g., a grounded conductor), the spurious actuation would be self-mitigated. Based on these insights, the cable failure mode analysis would be asked to estimate the likelihood that a combination of conductors leading to spurious actuation, and not involving the grounded conductor, will short together given electrical cable failure.

In practice, the iterative nature of the problem is addressed by dividing the cable failure mode analysis into two further steps. The first step is to consider the electrical cable failure behavior independent of the circuit. That is, the electrical cable in and of itself will experience some combination of conductor short circuits or failure modes. Conductors may short to other conductors in the same cable, they may short to the conductors of another electrical cable, or they may short to an external ground. This behavior should, at least to some extent, be relatively independent of the nature of the circuit to which the cable is connected. However, cable failures must also be considered in the context of the circuit to which the cable is connected, and this is the second step in the cable failure mode analysis.

A circuit utilizes each conductor in a given cable in a particular way. In a control circuit, for example, some conductors are energized to supply control power to the circuit, some conductors are normally de-energized and carry control power to an actuating device when the circuit is exercised (e.g., a control action is taken), other conductors will typically carry control indication signals back to the control station, one or more conductors may be grounded, and finally, some conductors may not be used in the circuit at all (spare conductors). The circuit fault behavior (i.e., how the circuit responds to the cable failures) will typically depend on the types of short circuits (the failure modes) experienced by key conductors among those conductors servicing the circuit. For example, short circuits between the normally energized (or source) conductors, and those normally de-energized conductors that feed power to actuating devices (the potential spurious actuation target conductors) can lead to spurious actuation of the circuit (the so-called hot short induced spurious actuation).

In the consideration of circuit faulting behavior, the initial cable failure behavior is often of paramount importance. In particular, the relative likelihood of conductor-to-external ground versus conductor-to-conductor short circuits is critical. Shorts to ground will generally trip circuit protective features leading to a loss of either control or motive power (see Section 8.6 below). In contrast, conductor-to-conductor short circuits carry the potential to cause spurious actuation of circuits and components. Hence, if a short to ground is the first failure mode observed, other potential failure modes may be rendered essentially moot. That is, if circuit protection is tripped open by a short to ground, then it may not be possible for a subsequent hot short to energize or spuriously actuate that system. However, the importance of subsequent failures and failure mode transitions must be viewed in the context of the circuit under analysis. For example, multiple shorts to ground on an ungrounded DC circuit may have more significant risk implications than only the first such short to ground.

It should also be noted that the cable failure and circuit fault mode discussions which follow are based largely on information gathered during fire experiments involving the failure of electrical cables. Virtually all of the available data is based on small-to-medium scale tests. Small-scale tests in particular cannot fully simulate actual plant installation and fire exposure conditions. Medium scale tests come closer to an actual application, but still cannot, or do not, capture potentially important features and variations of actual plant installations, fire exposure conditions, and conditions during fire suppression. This is true even of the most recent NEI/EPRI electrical cable fire tests (EPRI TR-1003326), even though these tests represent one of the most relevant data sources currently available. Hence, the data and insights derived from such data must be viewed in the context of how those data were gathered.

The available data are both limited and uncertain. The direct extrapolation any given test result to a particular application may be inappropriate. This is especially true in the circuit analysis context given that the data available have illustrated, but not fully investigated, the importance of various factors to the cable failure and circuit response behavior. In the discussion which follows, the author has tried to stress the uncertainties associated with our current understanding of cable failure behavior while at the same time providing as many numerical probability insights as possible. Both the qualitative and quantitative insights described here must be considered preliminary.

8.5 Electrical Cable Failure Modes

In both the regulatory and risk contexts, the failure of an electrical cable implies that the cable is no longer free of fire damage; that is, it is no longer “capable of performing its intended function during and after the postulated fire, as needed” (GL 86-10). From an electrical perspective, the function of an electrical cable is to provide a medium for the transmission of electrical energy (power and/or signals) between two points in a common electrical circuit while simultaneously maintaining the electrical isolation of the transmission path from other elements of the same circuit and from other co-located circuits. Failure, therefore, implies loss of continuity in the energy transmission path or diversion of a sufficient fraction of the available electrical energy to an unintended circuit destination such that proper function of the circuit is no longer ensured.

As discussed previously in Chapter 3, electrical cables are manufactured in a wide range of configurations. The primary configuration features that define a given electrical cable are the size of the individual conductors (expressed using the AWG), the number of conductors, shielding and/or armoring features, and the insulation/jacket materials used in the construction.

There are four primary modes of cable failure of potential interest. These failure modes relate to the electrical behavior of the conductors associated with a given electrical cable, as follows:

- A ***conductor to external ground short circuit*** results in the diversion of electrical energy to ground.
- A ***conductor to conductor short circuit*** may result in the diversion of electrical energy from one conductor (the source conductor) to one or more unintended conductors [the target conductor(s)]. One special case of the conductor to conductor short circuit is the *hot short*, that is, the shorting of an energized conductor to a non-energized and non-grounded conductor.
- ***Conductor insulation resistance degradation*** may result in the partial diversion of the available electrical energy to an unintended conductor path.
- A ***loss-of-conductor continuity*** (or open circuit conductor failure) is a physical break in the conductor that will result in electrical energy being unable to reach the intended circuit destination.

Before proceeding, two points related to cable failure behavior should be observed. First, the likelihood estimates discussed here are all conditional values given that an electrical cable has been damaged. That is, the likelihood that a particular fire might cause electrical cable damage is not included, only the likelihood that certain failure modes might be observed given that one or more electrical cables have been damaged by a fire.

Second, the discussion focuses on the initial failure mode (that is, the first failure mode that might be observed given failure). As noted previously in Section 8.4, cable failure behavior may be dynamic, but the initial failure mode is of paramount importance. Some limited discussion of this dynamic behavior is provided, primarily in the context of the duration of hot shorts. Given a fire exposure of sufficient duration and intensity, the available experimental evidence indicates that all of the conductors in the damaged electrical cables will ultimately short to the grounded raceway. However, in the context of a real fire event, fires do not burn forever, and fires do not always create intensely damaging exposures. Hence, the shorting behavior of a given electrical cable could, for example, involve sustained hot shorts, shorts to ground, or hot shorts that later transition to shorts to ground.

8.5.1 Conductor-to-Conductor Short Circuits

Conductor-to-conductor short circuits are broadly categorized as either intra- or inter-cable. Intra-cable conductor-to-conductor shorting implies that the short circuit involves conductors within a single multi-conductor electrical cable. Inter-cable conductor-to-conductor shorting implies that the short circuit involves the conductors of two or more separate electrical cables (single and/or multi-conductor). Note that it is possible to have both intra- and inter-cable conductor-to-conductor short circuits active concurrently.

Conductor-to-conductor short circuit electrical cable failures have the potential to induce a range of circuit faulting behaviors. Such failures can lead to loss of circuit function, corrupted indications, loss of control, and spurious actuations. The actual circuit fault observed is entirely dependent on which conductors actually short together. However, the relative likelihood of conductor-to-conductor short circuits is of critical interest to the risk quantification.

In this context, we are primarily interested in initial cable failures that are manifested as a conductor-to-conductor short circuit that does not simultaneously involve a short to an external ground. As discussed below, one or more of the shorting conductors may be grounded, in which case, the conductor-to-conductor short circuit may have the same circuit fault effect as a conductor-to-external ground short. However, from a mechanistic view of cable failure, the first question to ask is the likelihood that the initial short circuit involves only conductors and not an external ground. One can then consider the nature of the conductors present and potential combinations of conductors, each of which may have unique circuit faulting effects.

There is currently little data available on cable failure modes and effects. A recent review sponsored by the RES identified a small number of experiments providing relevant data but also concluded that most electrical cable fire experiments provided little or no information on cable failure modes and effects (LaChance, et al., 2000). Hence, of particular note is a recently completed set of tests performed by NEI and EPRI with the participation of the NRC (NUREG/CR-6776 and EPRI TR-1003326). These tests provide the most relevant data on cable failure modes and effects currently available and will be discussed in some detail.

A total of 18 fire tests were conducted, each involving a cable tray and four to five monitored cable bundles. The tests explored a limited range of fire exposure conditions, cable types, and routing conditions. The data have provided many interesting insights into cable failure modes and effects behavior. However, the data are subject to substantial limitations, and caution must be exercised in extrapolating the results to any specific application.

First, the data were gathered in an atypical room. The test room was a steel plate box of limited dimension [3.04 m x 3.04 m x 2.43 m (10 ft x 10 ft x 8 ft)]. Given the steel room construction, heat losses from the walls and ceiling of the room were much greater than would be anticipated given a wall material such as concrete or gypsum wallboard. Hence, the relationship between the fire intensity and the room temperature was somewhat distorted in comparison to other room fire tests. In many of the tests, the room temperatures hovered very near the anticipated failure threshold temperatures for, in particular, the thermoset cables being tested. Hence, consistent with past experiments, the fire damage times were often prolonged (in some cases in excess of one hour). At higher exposure temperatures, the damage times would have certainly been shorter. It was also observed that some of the larger fires burned in an under-ventilated condition (as evidenced by an increase in room temperature when the size of the ventilation opening was increased during a given test). Hence, fires may not have reached the full burning intensity cited as the nominal fire intensity in the test reports.

Second, the circuit tests conducted by NEI used a surrogate MOV control circuit. The same circuit, with some variations, was used in all tests. The characteristics of this circuit may not be typical of other types of control circuits. Further, quantification of the circuit fault mode results is in part dependent on the circuit design, in particular, the number and placement of fuses, the number of energized conductors, the number of target conductors, and the presence of a ground conductor in the control cable. For another circuit with a different combination of conductors, the results could be quite different. For example, the presence of a grounded conductor in each multi-conductor electrical cable almost certainly contributed to a higher incidence of shorts to ground and a lower likelihood of spurious actuation.

Finally, the tests used primarily AC power sources. The NRC portions of the tests did involve some DC testing, but experimental problems caused much of the DC data to be compromised. The data did result in some conflicting information, hence, the applicability of AC circuit test results to DC circuits remains uncertain.

The results for the NEI MOV circuits were expressed primarily in the context of two circuit fault modes; namely, fuse blows (indicating an energized conductor shorting to ground or to a grounded conductor) versus spurious actuations. Overall, a substantial fraction of the cable failures resulted in a spurious actuation circuit fault mode.

The NRC sponsored portions of the tests focused on monitoring conductor shorting behavior through measurements of the conductor insulation resistance (IR) values during the fire tests. As the electrical cables are heated, the electrical insulation value of the insulation material is degraded. This degradation was monitored for both conductor-to-conductor and conductor-to-external ground. As a result, the actual shorting patterns between various conductors and between each conductor and ground could be determined. The initial cable failures were dominated by intra-cable conductor-to-conductor short circuits. The conditional probability of this mode of cable failure was estimated as 80-percent or higher based on these and other tests (conditional on electrical cable failure attributable to fire).

One possible explanation for the high likelihood of intra-cable conductor-to-conductor short circuits revolves around manufacturing practices associated with multi-conductor electrical cables. When multi-conductor electrical cables (with more than two conductors) are constructed, the individual conductors are first formed and insulated. The various insulated conductors are then brought together and the filler[30] and jacket materials are applied. In the jacketing process, the insulated conductors are generally twisted around each other to form a tight arrangement. If, for example, a length of a multi-conductor electrical cable is laid out along the floor, one typically observes a spiral pattern in the outer ring of conductors. This spiraling may leave a residual tension between the conductors. As the insulation materials are heated and lose their physical integrity (i.e., either melting or charring) this residual tension may draw the conductors together.

8.5.2 Combinatorial Models for Conductor-to-Conductor Shorting

Section 8.5.1 has discussed conductor-to-conductor short circuit failures in a very broad context that is essentially independent of the circuit to which the electrical cable is attached. There is, however, an interest in more specific modes of conductor-to-conductor shorting that would be relevant to a given circuit. Some analysts have proposed the application of combinatorial models to address this problem. To date, such models have not been assessed for validity, hence, their application to risk analysis remains unproven.

[30] Filler materials fill voids between the individual conductors within a multi-conductor electrical cable and may include materials such as paper, natural fibers, or polymeric (e.g., nylon) fibers.

The most obvious example where such a model might be applied is in estimating the likelihood of hot shorts leading to spurious actuation. To illustrate the combinatorial model approach, consider a circuit where there is one specific conductor (one target conductor) within a seven-conductor electrical cable that, if energized, would cause a spurious actuation. Further assume that there is one other conductor in the same electrical cable that can provide the energizing source for the hot short (act as the source conductor). The analyst concludes that intra-cable shorting is the mode of cable failure most likely to cause a spurious actuation. The spurious actuation analysis then needs to estimate the likelihood that a cable failure will create a hot short between the one source conductor and the one target conductor of interest. The analyst might then consider the total number of conductor pair shorting combinations available. For a seven-conductor electrical cable there are 21 such combinations possible. Only one of these pair combinations leads to spurious actuation. Hence, the analyst might conclude that the likelihood of the spurious actuation is 1 in 21. This is a very simplistic example intended only to illustrate the approach; however, it is not a recommended approach. Indeed, the available experimental evidence would indicate a much higher likelihood of spurious actuation for this configuration illustrating that this simplistic model fails to capture the important behaviors adequately.

Potential problems with such approaches have not yet been resolved. First, the shorting behavior of multi-conductor cables is complex and often involves more than two conductors in a shorting group. Second, the conductor shorting behavior is not totally random, but rather, tends to involve adjacent conductors within the electrical cable. Hence, the likelihood that any two conductors might short together is dependent in large part on their relative proximity to each other within the electrical cable. In most cases the analyst will not know the exact orientation of circuit functions and individual conductors in an electrical cable. The conductor-to-circuit wiring configuration may need to be treated as an aleatory uncertainty, and that uncertainty could be substantial. Third, many circuits will contain a “mitigating conductor” (e.g., a grounded conductor) that if involved in the shorting could mitigate a hot short (e.g., by tripping the circuit protection features). Again, the combinatorial models need to address this aspect as well.

Combinatorial models represent a potentially valuable approach that will likely see further development in the near future. For example, one participant in the recent EPRI expert panel proposed a more complex combinatorial model that incorporates an advanced view of cable failure behavior (see Appendix B of EPRI TR-1006961). The model appeared to work well in comparison to the experimental data available to the expert panel, but remains unproven in a more general context.

8.5.3 Conductor-to-External Ground Short Circuits

For all electrical cables, there is a potential that the insulated conductors will short to an external ground source. In particular, the raceways in which electrical cables are routed (trays and/or conduits) are generally metal (often galvanized steel and less commonly aluminum) and are typically grounded. Hence, most electrical cables have more or less ready access to an external ground plane once the cable insulation breaks down.

Note that a conductor-to-conductor short circuit that happens to involve a grounded conductor will have the same circuit faulting effect as a conductor-to-external ground short circuit. However, in the mechanistic view of cable failure modes and effects, the relative likelihood of a conductor-to-conductor short involving a grounded conductor is treated separately. The current discussion focuses on the role of the external ground sources in cable failure modes and effects behavior.

The conductor to external ground failure mode can introduce unique circuit consequences. For most AC circuits, shorts to ground will render a control or power circuit non-functional, but will also have a mitigating effect on, in particular, the possibility of spurious actuation circuit faults. Shorts to ground on an energized electrical cable of a grounded circuit will generally cause circuit protection devices to trip deactivating the impacted circuit. This could impact either the control or motive power of a circuit depending on which electrical cables are impacted (see Section 8.5). Also note that if a conductor-to-conductor short circuit does form, and if any one of the involved conductors shorts to an external ground (or is itself grounded), then all of the involved conductors will also short to ground. In a risk context, the primary interest is the conditional likelihood that a short to ground will be observed before a hot short that might lead to a spurious actuation failure. Note that ungrounded DC circuits are unique with regard to shorts to an external ground. A single short to ground on an ungrounded DC circuit has essentially no impact on circuit performance. However, multiple shorts to ground may adversely impact the circuit. In effect, for an ungrounded DC circuit, the external ground acts as an external conduit for the formation of conductor-to-conductor shorts.

For multi-conductor electrical cables, 20-percent or less of the observed cable failures are likely to involve an initial short to external ground. For single conductor electrical cables the likelihood of a short to external ground failure is estimated to be substantially higher (perhaps 50-percent or higher) but there is little experimental data available to support this contention.

Experiments show that given a sustained damaging fire, all of the conductors in the damaged electrical cables will ultimately short to ground. Hence, another potentially important consideration in the context of fire risk is the transition time associated with this behavior (e.g., transitions from conductor-to-conductor to conductor-to-external ground short circuits). This transition behavior is important because it may, for example, determine whether a valve might fully reposition, or for how long a PORV might remain open, or how long an operator might have to recover a spurious actuation before the control function is lost.

Experimental evidence indicates that, given a sustained damaging fire, initial cable failures will likely transition to shorts to external ground over a wide range of times. In the recent NEI tests (EPRI TR-100326), for example, some of the spurious actuation circuit faults were of momentary duration (e.g., less than one second) while others were maintained for in excess of 11 minutes. The average duration of a spurious actuation signal was 1-3 minutes depending on the cable type. It should also be noted that in the NEI tests, one of the conductors in the multi-conductor control cable was grounded, and short circuits to this grounded cable would mitigate the actuation signal.

Overall, the test data available do suggest that sustained conductor-to-conductor shorts are possible. It should also be noted that suppression of the fire could “lock in” conductor-to-conductor electrical cable failures such that the short to external ground transition might not be observed in all cases. Hence, it would not be appropriate to assume that shorts to an external ground would mitigate all potential spurious actuation failure within any given time period. Statistically this is certainly a non-trivial possibility that increases in likelihood the longer a fire lasts. However, it is far from certain that this transition will occur, especially given aggressive firefighting activities.

Overall, short to external ground cable failures are high likelihood events given fire-induced cable failures and should be considered in a risk-informed analysis. Recall also that conductor-to-conductor short circuits may have the exact same impact as a conductor to external ground short circuit if one (or more) of the involved conductors happens to be grounded.

8.5.4 Loss of Conductor Insulation Resistance (IR)

Polymeric insulation materials, thermoset and thermoplastic, dominate the current electrical cable applications in the U.S. nuclear power industry. When these materials are heated, they lose their electrical insulation value. Based on available equipment qualification test results (NUREG/CR-4537), the degradation in resistance is logarithmic with linear increases in temperature. An example of this behavior is illustrated in Figure 8-1 (reproduced from NUREG/CR-6681). This same mechanism can lead to a loss of insulation resistance failure mode when electrical cables are heated in a fire.

In general terms, this mode of failure is associated with a degradation of the electrical cable that is less severe than an actual short circuit condition. This mode would be active at temperatures below the melting point of a thermoplastic material, and below the nominal gross failure threshold of thermoset materials. For some circuits, a significant degradation in the insulation resistance between individual conductors or between conductors and ground could compromise the performance of the circuit.

This mode of failure is particularly relevant to instrumentation circuits. A typical instrumentation circuit operates at 4-20 mA. Given the nature of the instrument loop circuit, a breakdown in the instrument cable insulation could cause all or part of the intended current signal to be diverted, bypassing the instrument display device. This would bias, or corrupt, the instrumentation reading. Note that the direction of the bias will be predictable because while one can divert some of the intended signal, one cannot increase the current flow to the indication device. The direction of the bias will always be towards the low-current indication, although whether low current corresponds to high or low on the process variable scale must be determined for each specific case. For other types of circuits (i.e., those with more robust electrical energy), this mode of failure is unlikely to compromise circuit function. Rather, for higher-energy circuits, actual short-circuit conditions will be the failure modes of interest.

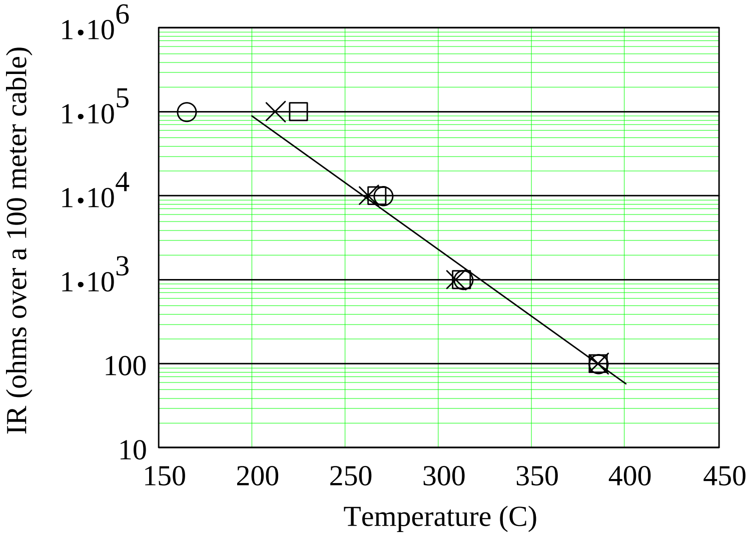


Figure 8.1 IR versus Temperature Behavior of a Typical Electrical Cable Insulation Material

This plot shows test data and a linear regression curve fit for a Brand Rex cross-linked polyethylene (XLPE) insulated 12 AWG 3-conductor electrical cable. The data are from Table 4 of NUREG/CR-5655, "Submergence and High-Temperature Steam Testing of Class 1E Electrical Cables" (NUREG/CR-5655). Similar plots can be generated for any given cable type, size and voltage rating given test data that reports IR as a function of temperature.

A recent test series examined this behavior for instrument circuits (NUREG/CR-6776). In general, a pronounced difference was noted between the behavior of thermoset and thermoplastic insulated instrument cables. Thermoplastic insulated electrical cables tended to fail abruptly and catastrophically with little or no indication of degraded signals prior to loss of signal. Thermoset insulated electrical cables illustrated a prolonged period of corrupted signal transmission before a complete loss of signal was observed. Hence, the use of thermoset insulated electrical cables appears to increase the potential that operators might be misled by a corrupted signal. An offsetting observation was that the thermoplastic insulated electrical cables failed far more quickly than did the thermoset insulated electrical cables. This is also consistent with the observation that thermoset insulated electrical cables are generally more resistant to fire-induced failure than are thermoplastic insulated electrical cables.

8.5.5 Loss of Conductor Continuity

As noted previously, a loss of conductor continuity implies that the physical and electrical integrity of the conductor itself is lost. That is, the conductor breaks. Note that this mode of failure may also be referred to as an open circuit cable failure, although this may lead to confusion with use of the term open circuit in the context of a mode of circuit faulting. An open circuit as a fault mode generally implies the opening of circuit protection devices (fuses or breakers). A loss-of-conductor continuity cable failure can have similar effects on a circuit, especially if the failure is associated with an energized power supply conductor.

Loss-of-continuity conductor failures have been observed both in actual fires and during tests. However, this mode of failure is considered highly unlikely to occur as the initial failure mode. Evidence taken from both experience and experiments indicates that fire-induced loss-of-conductor continuity failures may be observed under three circumstances as follows:

- During a prolonged fire exposure, the conductor material may melt causing a loss of conductor continuity. This is often a progressive behavior over an exposed length of electrical cable, rather than an abrupt or localized failure. In most cases, all of the electrical cable insulation materials would have long since burned away; hence, all of the conductors would have shorted to ground long before a loss-of-conductor continuity failure were observed.
- Loss-of-continuity may also be associated with other physical behaviors that could place an undue physical load on the electrical cables. This might include, for example, the collapse of cable supports or raceways, the impact of a hose stream on a badly damaged electrical cable, or physical stressors that may cause electrical cables to come loose from a terminal connection.
- High-energy electrical cables (i.e., those with a high voltage and/or current potential) may experience repeated, short duration, high-intensity arcing shorts (either phase-to-ground or phase-to-phase). These shorts are typically of such high energy that the conductor material is melted and/or vaporized at the location of the short causing the short to self-mitigate. Circuit protection devices (fuses and breakers) have a finite current/time response behavior, and conventional circuit protection devices are not designed to detect arcing faults (arcing fault circuit interrupters are available but are not widely used in the U.S. nuclear power industry). Hence, the circuit protective features may not be activated/tripped by these short duration arcing short circuits. If this behavior is repeated a sufficient number of times, the conductor continuity may eventually be lost.

The risk implications of a loss-of-continuity cable failure must be viewed in the context of the circuit under analysis. No concise risk analysis of this question has yet been conducted. Loss-of-conductor continuity failures are not expected to be risk-significant, in part because of their low likelihood of occurrence and in part because they are not expected to introduce unique risk scenarios or insights. The rationale for the second part of this conclusion depends on the type of circuit considered, as follows:

- **For control and instrument cables** the available power is not sufficient to induced high-energy arcing conditions. Hence, loss-of-conductor continuity failures will only be observed in long duration fires, and then only after all conductors have shorted to ground. This implies that other modes of cable failure (i.e., conductor-to-conductor and conductor-to-external ground short circuits) will determine the circuit faulting behavior.
- **For power cables** it is possible that a loss-of-conductor continuity might occur as a result of high-energy arcing. However, for power circuits, the loss-of-conductor continuity cable failure will mimic an open circuit fault associated with tripping of circuit protection features; namely, power will be unable to reach its intended destination. This same mode of circuit faulting is observed given a sustained short-to-external ground or phase-to-phase conductor shorting behaviors. Hence, in terms of the impact on the power electrical cables' own circuit, no unique fault modes are introduced. The only difference given a loss-of-conductor continuity failure is that the side of the broken conductor(s) leading back to the power supply source might remain energized; hence, these conductors might be available as a hot short source for other electrical cables. In the hot short analysis, the existence of an appropriate source is generally assumed unless the lack of such a source can be confirmed. Hence, again, the loss-of-conductor continuity failure should introduce no unique risk scenarios or insights.

8.5.6 Summary of Electrical Cable Failure Mode Insights

For multi-conductor electrical cables the dominant mode of cable failure anticipated is intra-cable conductor-to-conductor short circuits. Evidence in this area is strong and indicates that 80% or more of all fire-induced multi-conductor cable failures will initially involve intra-cable conductor-to-conductor short circuits. This appears to apply to both thermoset and thermoplastic insulated electrical cables. (Recall that not all intra-cable conductor-to-conductor shorts involve hot shorts leading to spurious actuation as discussed further below.)

The available data indicate that inter-cable conductor-to-conductor shorting is possible, but is less likely to occur than is intra-cable conductor-to-conductor shorting. The data also indicate that inter-cable shorting is more likely given thermoplastic insulated electrical cables than it is given thermoset insulated electrical cables. The available data on inter-cable shorting is not sufficient to provide firm estimates of conditional likelihoods. However, for thermoplastic insulated electrical cables, the likelihood of inter-cable conductor-to-conductor short circuits is probably 0.5 or less. For thermoset insulated electrical cables the likelihood of inter-cable shorting is probably 0.1 or less. For both electrical cable types the likelihood of inter-cable shorting may be much lower depending on the cable raceway configuration and fire exposure conditions.

For both electrical cable types, thermoplastic and thermoset, the likelihood of a hot short versus a short to ground will depend on a number of configuration factors that are currently not well characterized. While some of these factors may have little influence on the intra-cable shorting behavior, they likely have a stronger influence on the likelihood of inter-cable shorting. That is, for some configurations inter-cable shorts cannot be considered a rare event while for others, the likelihood may be very low. Factors that are believed to have a significant impact on the likelihood of inter-cable shorting include the following (NUREG/CR-6776):

- The nature of the fire exposure: Direct flame/plume exposures that heat the cables from below may be more prone to cause shorts to ground than would radiant heating that heats the cables from above.
- The loading of the raceway: A tray with many electrical cables would be more likely to experience inter-cable shorting than a sparsely loaded cable tray.
- Trays with maintained spacing of the electrical cables: For such configurations (generally used only for larger power cables), inter-cable shorting independent of the grounded raceway appears to be highly unlikely.
- The position of the critical electrical cables within the raceway: Electrical cables located at the bottom of a tray would be more likely to short to ground than electrical cables located on top of a cable load.
- Cable tray type: Cable tray type (e.g., ladder back versus solid bottom) impacts the cable support loading and may impact the failure behavior, but this parameter has not been investigated.
- Use of conduits: Electrical cables in conduits appear to have a higher likelihood of shorts to ground and a lower likelihood of hot-short induced spurious actuation in comparison to electrical cables in cable trays. This appears to apply to both intra- and inter-cable shorting behaviors.

It also appears that loss-of-conductor continuity failures are unlikely to occur as an initial failure mode. Such failures are likely to occur, but only after extended fire exposures or after repeated arcing faults for higher energy electrical cables. This failure mode is not expected to contribute significantly to fire risk.

Combinatorial models may be used in the future as a tool to estimate the likelihood of specific cable failure modes, and in particular the likelihood of hot shorts leading to spurious actuation. However, these models have not been fully developed and remain unproven.

8.6 Circuit Fault Modes

The risk implications of cable failure induced circuit faults will be discussed in the context of the three primary circuit types or functions; namely, power, indication/control, and instrumentation. For each circuit type, the cable failure modes and circuit fault modes of potential interest are somewhat unique. Fault modes of interest for each circuit type are as follows:

- Power circuit fault modes
  - a. Loss of primary or motive power to a system or component
  - b. Hot shorts leading to spurious actuation
  - c. Multiple high impedance faults

- Control and indication circuit fault modes
  - d. Loss of control function or power
  - e. Spurious actuation in control circuits
  - f. Loss of control indications
  - g. False control indications

- Instrumentation circuit fault modes
  - h. Loss of permissive signals
  - i. False permissive signals
  - j. Corrupted instrument gage readings

Each of these circuit types is discussed in detail in the subsections that follow.

8.6.1 Power Circuit Fault Modes

Loss of Primary Motive Power

For power circuits, many electrical cable failures will lead to a loss of primary motive power to plant devices[31]. A loss of primary motive power implies that the faulted system stops operating. Continuously operated devices such as pumps, fans, and motors will stop and/or will be unable to start. Intermittent operating devices such as MOVs would cease movement, if movement were in progress at the time of the cable failure, and would be unable to move through normal control functions (in some cases manual repositioning would still be possible, e.g., using a handwheel). Devices that require continuous power to maintain position, such as a solenoid operated valve, would cease to be operable and would stay in, or reposition to, their de-energized condition.

Loss of primary motive power could result from the following power cable failures:

- phase-to-ground short circuits involving an energized conductor
- phase-to-phase short circuits involving two or more energized conductors
- hot shorts to a power circuit of higher voltage potential

In each case, the cable failures would lead to opening of circuit protective features (e.g., breakers and/or fuses) — an open circuit fault mode for the power supply circuit.

Given the many ways that power cable failures might lead to an open circuit fault condition, the loss of motive power will be the predominant fault mode given the failure of power cables. It can nominally be assumed that 99-percent or more of the power cable failures would lead to this mode of circuit faulting.

Power Cable Hot Shorts Leading to Spurious Actuation

The likelihood of power cable failure induced spurious operations depends in large part on the nature of the power supply system. Single-phase AC power systems may be somewhat vulnerable to spurious actuation faults, whereas three-phase AC and ungrounded DC systems appear to have a far lower likelihood of spurious operation.

For the ungrounded DC and three-phase AC systems, multiple concurrent inter-cable hot shorts of the proper polarity are required to induce spurious actuation of plant components as a result of failures in power cables. However, the conditions leading to this fault mode are quite specific and are considered highly unlikely to occur. In general, a spurious actuation induced by power cable failures for these two types of systems requires either two or three (depending on whether the system is DC or three-phase AC) concurrent hot shorts of the proper polarity such that the attached device is appropriately powered.

[31] Motive power is distinguished from control power. Motive power is the source of energy that runs a primary electrical device such as a motor, while control power is a separate, although potentially dependent, light power circuit used to energize secondary control devices such as relays which in turn control the flow of motive power to the primary component.

For a single-phase AC system, the neutral power leg is typically tied to ground. Hence, a single hot short from the ‘hot’ leg of the AC system to a hot leg power lead for another device can cause spurious operation. Return power can be transmitted through the common ground, bypassing the neutral conductor (hence, a neutral-to-neutral short circuit may not be required). General practice for NPPs in the United States is to use separate electrical cables for each power supply circuit. Hence, spurious actuation would generally require an inter-cable hot short. Given that only one inter-cable conductor-to-conductor hot short is required, the likelihood is higher in comparison to the DC and three-phase AC cases. In all three cases, the voltage and current characteristics of the source conductors must be compatible with the target device. Application of an excessive voltage may damage the target device rather than cause it’s actuation. Similarly, application of a DC source to an AC device (or vise-versa) would likely damage rather than activate the target device. Finally, if the current available to the source conductors is not sufficient to power the target device, then an overcurrent condition will likely trip the source conductors’ protective circuit features mitigating the fault.

Nominally, the probability of such spurious actuation faults given the failure of power cables is judged to be low for all three cases, although no specific investigation of this potential has yet been undertaken. The conditions required depend on the nature of the power source involved:

- For three-phase AC power circuits (typical of large motors and MOVs), a spurious actuation would require three concurrent hot shorts, each provided by a source of compatible power (voltage and current). Shorts to an incompatible power source (wrong voltage or inadequate current) would likely either damage the target component or trip circuit protection on the source bus. All three source conductors must also be powered from the same electrical bus. Reversal of two phases of the source/target configuration could cause the target device to operate in reverse, and could well damage the target device. Spurious actuations for this configuration are considered highly unlikely and are estimated to have a 0.001 conditional likelihood or less. Note that if a ground conductor is routed with the energized conductors (e.g., a triplex cable with ground), the likelihood of a spurious actuation will be further reduced.
- For single-phase AC power circuits (typical of smaller motors and MOVs), the neutral is generally tied to ground so only one hot short from a power source of proper voltage and current would be required. Again, shorts to a source bus of improper voltage or inadequate current would likely either damage the target component or trip circuit protection for the source conductors. This is also considered an unlikely occurrence, but the conditional probability of occurrence given cable failure may be as high as 0.1 depending on the nature of the power cables and grounding provisions. For most cases the likelihood should be lower. For example, if an explicit ground conductor is routed with the high and low potential power cables (e.g., a two-conductor electrical cable with ground or three-conductor electrical cable), then the likelihood of a spurious actuation will be lower. Use of armored electrical cables could essentially eliminate this possibility because there is virtually no possibility of inter-cable shorts independent of the grounded armor. Routing of electrical cables in conduits would also reduce the likelihood even if the conduit contains more than one power cable such that inter-cable shorting remains a possibility.
- For an ungrounded DC power system, two concurrent hot shorts of the proper polarity are required to induce a spurious actuation. Alternatively, one of the two polarity hot shorts might be provided through the effects of multiple shorts to ground, however, one side of the power supply system must remain isolated from ground or circuit protection would be tripped.

If the DC voltage is not appropriate to the target device, the device would either fail to operate or might be damaged. Adequate current is also needed.

Overall, spurious actuations that are induced by failures in those electrical cables that provide motive power to a device are considered unlikely. The highest likelihood case is single-phase power systems, and while unlikely, this type of circuit fault might still have some non-trivial contribution to risk and should be considered. For the ungrounded DC and three-phase AC power systems, the occurrence of a power cable failure induced spurious actuation appears unlikely. Hence, consideration of such fault modes for other than high consequence applications (e.g., high-low pressure interfaces) does not appear to be warranted. The conditions required to cause such faults are simply too specific and too restrictive to be considered likely, and the potential for such faults will likely have little risk significance.

Multiple High-Impedance Faults

There is a potential that concurrent failures involving several power cables could introduce a unique failure mode for plant power distributions systems. In particular, if multiple power cables fed from a common bus experience low quality or high impedance shorts, each electrical cable could experience current leakage beyond that expected as a result of the normal operation of the powered component. Enough faults of this type could create a demand on a higher level circuit protection device that exceeds the protection level of the higher level bus, without exceeding the protection level of the individual circuits. The physics of such behaviors remain poorly understood, and cannot be dismissed out of hand. However, based on the knowledge we have regarding cable failure behavior, this mode of failure is considered to be unlikely in practice. Several factors work against such an occurrence.

One such factor is the precise quality of the faults required to create such a situation. The multiple high impedance fault scenario postulates that several electrical cables are leaking current at levels just below the trip point of the nearest up-stream circuit protection device. This would require a sustained fault with a rather precise resistance, and indeed a resistance that is relatively low.

However, the shorting behavior of energized electrical cables does not favor the formation of such shorts. Experiments do show that electrical cables will tend to degrade progressively over time (NUREG/CR-6776, NUREG/CR-5655, and NUREG/CR-5546). The data show that electrical cables energized to a non-trivial level (i.e., greater than approximately 50 V) display an abrupt shorting behavior beyond a certain level of degradation. It appears that once the degradation reaches the point where the insulation is providing about 1,000–10,000 ohms IR, there is an abrupt transition to a low-impedance or dead-short fault.

A second factor working against this scenario is timing. The multiple high impedance fault scenario requires that several faults be active concurrently. This is certainly possible, but experimental evidence suggests that even electrical cables located in a common tray will fail at discrete times rather than all at once. The issue of timing combined with the need for a sustained fault of a rather precise resistance value would appear to indicate that a multiple high-impedance fault, leading to the tripping of a higher level power distribution bus, while possible, is of low likelihood.

Finally, the risk implications of the multiple high impedance fault issue are mitigated to some extent given that operator response could potentially recover the undamaged circuits The scenario does not postulate that the higher level bus is damaged beyond recovery, simply that the circuit protection trips at a level higher in the distribution system than the level at which the actual cable failures occurred. Hence, isolating the damaged circuits would allow for re-setting of the tripped breaker/fuse and recovery of the higher level bus. The timing of such recovery actions, and the likelihood of success, would need to be considered in a risk assessment.

In the context of a fire PRA, the loss of a higher level bus, when treated, would typically be assumed to occur as a result of a random failure of the nearest circuit protection feature to trip on demand. In this scenario, a single electrical cable failure might fail to be isolated by the first upstream circuit protection feature, and would therefor cascade to the next level bus. The risk implications of the multiple high impedance issue could be estimated using a similar approach by increasing the random failure probability of the local circuit protection device to reflect the likelihood of the multiple high impedance fault scenario. The effect on the plant systems would be similar, although the multiple high impedance fault scenario would require that more failed circuits be isolated before the higher level bus can be recovered. Such an exercise has not yet been conducted.

8.6.2 Control and Indication Circuit Fault Modes

In U.S. NPPs, the control and indication functions tend to be combined in a common circuit for a given device. For example, the open/close/in-motion indicator lights for an MOV tend to be a part of the overall control circuit and the conductors associated with the indication functions are often routed in the same electrical cable as those associated with the control functions. Hence, circuit fault modes for both control and indication circuits are treated as a common subject.

Loss of Control Function or Power

One likely mode of circuit faulting for control and indication circuits is a loss of control function. For continuously operating systems, a loss of control function may leave the system components running. For some devices, such as solenoid operated valves, a loss of control power can lead to repositioning of the device to the fail-safe condition. For other devices, such as an MOV, the loss of control function would leave the device in its prior state and render the normal controls ineffective at changing that state. Loss of control function fault modes are of potential risk importance if the system or function lost must be manipulated to support hot shutdown. This would include both front line and support systems. Loss of control function failures impacting only cold shutdown functions are not likely to be risk significant provided that hot shutdown can be achieved. Loss of control function failures for containment isolation functions are also of low risk significance unless the ability to achieve hot shutdown is also compromised.

A loss of control function would typically be associated with failures in the control system electrical cables, and in particular, either a loss of control power or other short circuit conditions that will divert the control power in the event that a control operation is attempted. In most cases, a loss of control function will be associated with a loss of the control power source. If the conductors that supply control power to the control circuit short to ground (or across polarities for DC circuits), then circuit protection for the control power circuit would likely trip. In some cases, a control cable failure can leave a control circuit nominally intact. However, upon any attempt to manipulate the control circuit various faults can occur that would render the control system inoperable (e.g., see MOV circuit analysis examples in LaChance, et al., 2000).

Spurious Actuation in Control Circuits

The issue of spurious actuations (or spurious operations) has received much attention. Spurious actuation is one specific type of “maloperation” fault as identified in the NRC fire regulations. Spurious actuation involves activation of a functional mode of a system or component caused by fire-induced electrical cable failures. Based on current understanding of the circuit analysis issues, the most likely source of spurious actuations will be control circuit electrical cable failures. Because the shorting behavior of the electrical cable conductors is complex, the analysis of spurious actuations is also complex.

A spurious actuation is generally caused by hot shorts, but not all hot shorts will lead to a spurious actuation, so care must be taken in estimating the likelihood of a spurious actuation. The short circuit must involve the right set of conductors. For many circuits, a specific pair of conductors must be involved in a common short. For grounded circuits, the short must not involve an external ground or grounded conductor. For ungrounded DC circuits, a pair of correct-polarity hot shorts is required. The exact configuration of shorts that could cause spurious actuation is potentially unique for each circuit in the plant; however, in practice many circuits will share common configurations and common failure/fault modes. The number of unique configurations that might need to be considered has not been determined.

A detailed analysis of spurious actuation is a tedious undertaking for most circuits. For the purposes of regulatory compliance, simplified methods of analysis are often employed. One common approach is the “hot probe” analysis. Under this approach the analyst assumes that a source conductor of proper voltage and current will be available. Each conductor in a circuit is then systematically energized by this “hot probe” source conductor to determine if a spurious actuation is possible. For the purposes of risk assessment, the regulatory analysis results can be applied, but generally only with some considerable uncertainty in quantification of the results. A more rigorous quantification requires a more rigorous analysis.

Time may also be a factor for some cases. Time may be important from two primary perspectives. Specifically, time may be important from the perspective of when the spurious actuation occurs and how long it persists. For example, a spurious actuation may open an solenoid-operated valve (SOV), but if the actuation is mitigated within a short period of time, the fault may have minimal risk implications. Similarly, a hot short may initiate a spurious actuation of an MOV, and the duration of the hot short may determine whether the valve fully repositions or only partially repositions. For some systems, a hot short might start the system (e.g., a pump), but mitigation of the hot short might cause the system to stop.

The questions of timing are also important when the issue of multiple spurious actuations is considered. In some cases, spurious actuations may only be risk significant if they are postulated in combination with other spurious actuations (or potentially other specific system faults). Hence, the timing of onset and the duration of the faults will influence the likelihood that any two or more spurious actuations might be active simultaneously.

The only experimental study that has directly assessed electrical cable failures leading to spurious actuation are the recent joint NEI/NRC electrical cable failure modes and effects tests described previously. In particular, the NEI MOV circuit tests provided many insights into spurious actuations.

As previously noted, a number of spurious actuations were observed, and the likelihood of spurious actuation given electrical cable failure was found to depend on a number of factors. Overall, the likelihood of spurious actuation given cable failure cannot be considered small. For most configurations a screening value ranging from 0.1 to 1.0 would be appropriate. A recent EPRI expert panel estimated the spurious actuation likelihood for the "base case" configuration[32] of this circuit ranges from 0.1 to 0.5 due only to intra-cable hot shorts (Reference EPRI TR-1006961). Variations from the base case led to other likelihood estimates, including the following general effects:

- Armored electrical cables showed a somewhat lower likelihood of intra-cable hot shorting, presumably due to the prevalent ground plane represented by the grounded armor.
- Electrical cables in conduits appeared less susceptible to hot-short induced spurious actuations, again presumably due to the prevalent ground plane represented by the grounded conduit.
- The lack of a CPT in the circuit increased the likelihood of a hot-short induced spurious actuation (by a factor of approximately 2). Note that CPTs are common in MOV control circuits.
- Inter-cable conductor-to-conductor short circuits are substantially less likely than intra-cable conductor-to-conductor short circuits. One explanation for the lower likelihood of inter-cable shorting is that there is no inherent residual tension between the conductors of two separate electrical cables as there is between the conductors of a multi-conductor electrical cable (see previous description).
- As compared to thermoset insulated electrical cables, the thermoplastic insulated electrical cables showed a similar likelihood of intra-cable hot shorts leading to spurious actuation, but an increased likelihood of inter-cable hot shorts leading to spurious actuation.

Multiple Spurious Actuations

A particular aspect of the spurious actuation question is the likelihood that multiple spurious actuations might be observed during a given fire. The evidence both from testing an actual fire experience clearly indicates that multiple spurious actuations are possible. However, it is appropriate to consider multiple spurious actuations in a more structured context.

There are several potential aspects to the multiple spurious actuation question, each of which may have unique risk implications. One of the most critical questions relates to timing. Specific issues related to timing include the following:

- Simultaneous behaviors: Simultaneous implies that events occur at essentially the same moment in time. To date no specific applications where simultaneity has been a critical factor to risk have been identified. Based on our understanding of electrical cable failure behavior, the onset of multiple cable failures simultaneously is possible, but appears unlikely. The most likely case leading to simultaneous spurious actuation faults would be where multiple faults might be created by the failure of a single cable. If the multiple faults require the failure of multiple cables, simultaneity appears unlikely. Fire testing indicates that even within a given raceway cable failures tend to be somewhat distributed over some time period, usually

[32] The base case involved a thermo-set insulated electrical cable in a cable tray with a control power transformer (CPT) in the circuit to limit the available total circuit power.

measured in minutes. Several factors likely account for this observation. For example, the heating from a fire is generally nonuniform; variations in electrical cable size lead to variations in their thermal response; variations in cable placement within a raceway lead to variations in the heating rate. Overall, it would appear that simultaneous spurious actuation faults are not of substantial concern in the risk context unless they can be induced by the failure of a single electrical cable.

- Concurrent behaviors: Concurrent implies that multiple faults occur at discrete points in time, but that they endure for a sufficient period of time that they overlap. Note that in this context we are referring to circuit faults, not cable failure. Note in particular that a self-mitigating cable hot short (e.g., a hot short that subsequently shorts to ground) may not mitigate the fault condition. For example, a repositioned MOV may not return to its original position when the hot short self-mitigates. Rather, some active intervention by plant operators may be required to mitigate the fault.
- Sequential behaviors: Sequential faulting implies that one fault is mitigated before being followed by another fault at a later time. Clearly, sequential behaviors are possible if not likely. For example, it appears that the 1975 Browns Ferry fire involved primarily a sequential series of spurious actuations (see discussion below) that were either self-mitigated or mitigated through operator actions during the event. However, even with sequential faults, some risk important scenarios may arise.

The test data and experience clearly indicate that concurrent hot shorts are possible. Hence, concurrent spurious operations are also possible. During the NEI MOV circuit tests, for example, some tests experienced concurrent hot shorts on two separate control circuits given the exposure of just four control circuits to potential actuation. This would tend to indicate a high potential for concurrent hot shorts and spurious actuation faults. One factor in this behavior was likely the co-location of the cables in a common raceway. The failure behavior for electrical cables located in separate raceways has not been explored extensively, although some data is available. The intensity of the fire exposure will be the primary factor in determining the timing of electrical cable failures, especially when multiple raceways are exposed.

An example where concurrent spurious actuation faults would be important is a case with two normally-closed SOVs in series in a significant diversion path. For the diversion path to open both valves must open and be held open concurrently. Self-mitigation of either hot short (e.g., by a subsequent short to ground) would return that valve to the normally closed position closing the diversion path.

A similar situation involving two MOVs, rather than SOVs, presents some interesting insights. Even given sequential self-mitigating hot short cable failures, both valves may be left open concurrently. That is, once each MOV repositions, mitigation of the hot short may not return the valve to a closed position. Rather, it is likely that mitigation of the hot short will cause a loss of control power and a loss of the normal control function while leaving the valve in the open position. Similar behaviors could be observed in circuits with latching or locking relays where even a momentary hot short might lock in a spurious actuation circuit fault. Again, the existence of concurrent spurious actuation faults is distinct from the existence of concurrent hot short cable failures for certain cases.

The assumption of sequential faults is, in essence, the basis most commonly used for current fire safe-shutdown analyses, and is the so called "any and all, one at a time" approach (a detailed discussion of the application of this approach is provided in Appendix B of this document). Two additional considerations related to multiple spurious actuations are as follows:

- Multiple actuations of a single system: It appears likely that a system that experiences one spurious actuation signal will experience two or more such signals. This was observed in both the 1975 Browns Ferry fire and during the NEI MOV circuit tests. It is also nominally consistent with the NRC/RES insulation resistance measurements made during the NEI tests as well. In the NRC/RES measurements, groups of conductors were observed to form dynamic conductor shorting groups, a behavior that could lead to multiple actuations of a circuit as a result of the failure of a single control cable.
- Actuations involving multiple systems: Both experience and testing demonstrate the potential for the actuation of multiple systems. During the NEI MOV circuit tests, for example, as many as three of the four exposed circuits experienced spurious actuations during a given test.

Overall, one cannot dismiss the possibility of multiple spurious actuations, either concurrently or sequentially. Further, one cannot dismiss either multiple actuations of a single system, or the spurious actuation of multiple systems. The obvious question is how likely are such events and how many spurious actuations are reasonable to postulate? Given the NEI MOV circuit tests in particular, the likelihood of spurious actuation of a circuit (given damage to a susceptible control cable[33]) was relatively high. The likelihood was found to be dependent on a number of factors, and varied over a fairly wide range. Important factors explored in the tests were discussed previously.

Given the identification of several important factors, it is not possible to cite a single value that would be characteristic of a "typical" control circuit. In broad terms, the mean likelihood of actuation (given failure of a susceptible control cable as observed in the NEI MOV circuit tests) ranged from about 0.1 to about 0.6, depending on how the tests are parsed. For at least one configuration, the EPRI expert panel cited an upper bound estimate of the spurious actuation likelihood of 1.0. This range represents a significant variation even given that a limited set of potential factors of importance were varied, that only one basic control circuit configuration was tested, and that the factors varied were only explored over a limited range. Overall, there is still at least one order of magnitude uncertainty in the likelihood of spurious actuation for any given circuit (assuming some level of susceptibility).

Given spurious actuation likelihoods of this order, the possibility of multiple spurious actuations cannot be dismissed. Given the data, the number of spurious actuations may be limited only by the number of susceptible cables damaged by the fire. This still, however, leaves open the questions of likelihood (how likely is it that two or more actuations would be experienced) and timing (sequential versus concurrent faults). Neither question, unfortunately, has a clear cut answer. One can, for estimation purposes, assume nominal likelihoods based on the NEI tests for a given circuit. If the conditions of the associated electrical cables are well characterized, then the estimates can be refined. If one assumes circuits with the highest level of susceptibility (e.g., a mean value of 0.6 given cable damage), and assuming independence between failures, then as many as four spurious actuations would still have a likelihood of $(0.6)^4$, which equals 0.13.

[33] By susceptible control cable we mean a control cable configuration wherein intra-cable shorts do hold the potential to cause a spurious actuation.

It is likely that more risk consequence mitigation will be achieved by considering the likelihood of damage to multiple control cables than from consideration of the likelihood of spurious actuation given control cable failure. In particular, most electrical cables used by the U.S. nuclear industry are fairly robust and resistant to fire damage (thermoset insulated electrical cables in particular). Experience illustrates that most fires are small, causing damage to few, if any, exposed electrical cables. These observations substantially reduce the likelihood that fires leading to multiple spurious actuations will occur. Nonetheless, given a severe fire and damage to many electrical cables, it appears that one or more spurious actuations are likely.

Lost or Misleading Control Indications

As noted previously, the indication functions are generally carried by conductors that reside in the same electrical cable with the control functions for the same circuit. (Note that instrument signals are discussed in Section 8.6.3 below.) There are various circuit fault modes of potential interest to these indication functions. Fault modes of potential interest include the following:

- Hot shorts can illuminate indicators inconsistent with the actual system status (e.g., a valve open light might illuminate even though the valve is actually closed).
- A short to ground can fail an indication (e.g., an indication lamp may go out).
- Some indication faults may not be manifested until an attempt is made to operate circuit (e.g., given an attempt to operate a valve, both the open and closed indicator lights might be illuminated).

The importance of such faults to risk is primarily driven by the operator’s response. Operators take control actions based on the signals presented to them. False indications may lead to unsafe actions. The importance of such faults may be mitigated by redundancy in the signals available to operators. Further, inconsistency between corrupted and intact signals may lead operators to diagnose control circuit problems. For example, if an operator sees both open and closed indicators illuminated for a single valve, they may conclude a circuit fault has occurred and will not place much faith in that circuit. Indeed, experience includes cases where operators have diagnosed the existence of a fire based on faults in their control circuits.

The risk importance of indication circuit faults has not yet been assessed. No fire risk analysis to date has explicitly considered this issue.

8.6.3 Instrumentation Circuit Fault Modes

Instrument circuits present potentially unique circuit analysis concerns. Instrument circuits provide critical information regarding the status of the plant to operators. As opposed to status indicators (discussed previously in Section 8.6.2), instrument circuits provide a variable output reading that is proportional to some process variable (e.g., temperature, pressure, level, flow rate, current draw on an electrical circuit, etc.). Instruments are important to post fire safe-shutdown for several reasons:

- Instruments provide operators with needed information on the status of the plant. The degradation of instrument reading (e.g., transmission of a corrupted reading) might mislead operators into taking improper response. A complete loss of an instrument reading might be more obvious, but deprives the operator of potentially important information.

- Instruments are often associated with permissive interlocks. A loss of an instrument signal might cause a loss of the permissive signal. This could in turn cause the shutdown, or prevent the startup, of a desired system. (An example of this is cited below where the fire-induced failure of an oil pressure signal cable caused a false low oil pressure signal and prevented the operators from starting the associated pump.)
- Some instrument signals are tied to automatic control systems or functions. Degradation in these instrument readings could lead to the undesired actuation of automated control functions.

Note that to date no fire PRA has systematically evaluated the implications of fire-induced failures in instrument circuits. Hence, the available insights in this area are limited.

Instrument Loop Fire Damage Testing

During the joint NEI/NRC electrical cable fire tests described previously, several instrument cables were tested (NUREG/CR-6776). These tests utilized a simulated 4–20 A instrument loop, a common instrument circuit configuration. With respect to instrumentation cable failures, the following insights were observed:

- The instrument cables failed earlier in the test than did the co-located control cables. The instrument cables tested were all rather small, and this result generally reflects the thermal mass effect. That is, smaller cables heat more quickly, and hence fail more quickly, than do larger cables.
- Thermoplastic insulated instrument cables failed early in the fire tests, and the signal was lost quite abruptly. The instrument readings in such cases would abruptly change from normal to full loss of signal (off-scale low). Such behavior would likely be an obvious indicator to plant operators of a problem in the circuit.
- Thermoset insulated cables experienced degradation and failure later in the exposures, and over a more extended time period, typically of several minute duration. The initial degradation was manifested as an unsteady drop in the simulated process variable value. The degradation in some cases became progressively worse over a period of some minutes. Eventually, a sudden loss of signal was observed in each case. Such behavior may not be as obviously indicative of instrument circuit degradation.
- The behavior of an instrument circuit given cable degradation (e.g., the signal bias direction) can be predicted based on fairly simple circuit analysis.

Loss of Permissive Signal

The loss of a permissive instrument reading may induce a loss of function for the associated system. In some cases, multiple signal losses may be required to cause a loss of function (e.g., given a two out of three polling scheme). Loss of function faults might be recoverable, but only if operators can bypass the permissive signal and re-start the system. Such recovery actions are probably not covered by the operator’s procedures, and hence, may be unlikely. Success would require ‘on-the-fly’ circuit diagnosis and modification. Such operations would not typically be credited in a fire PRA.

It appears that few fire PRAs have explicitly considered the implications of loss of permissive signals. The extent to which such failures are captured would depend on the approach taken. If the regulatory compliance safe-shutdown equipment list included those electrical cables that carry the permissive signal for safe-shutdown systems, then loss of those electrical cables was likely assumed to cause loss of the system. However, particularly for systems not credited in the safe shutdown analysis but credited in the fire PRA, permissive signals may or may not have been identified as a part of the plant shutdown model, and as a part of the electrical cable tracing efforts.

False Permissive Signal

There is a potential that certain types of corrupted or lost signals could cause a spurious actuation signal to be generated through automatic control systems. This potential would depend on the control logic. For example, multiple sensor line polling might make such spurious control signals unlikely. Some advanced circuits may also be designed to detect and reject corrupted signals. Again, the potential risk significance of such faults has not been addressed in any PRA known to the authors of this chapter.

Corrupted Instrument Gage Readings

As noted previously, the instrument signals are of critical importance to operators and are used to guide the operator actions or operator manual actions. A complete loss of several control signals may mean that operators would not know the actual reactor status. This, of course, depends on number of independent or redundant sensors available. It is also important to note that an instrument reading that is completely lost is likely to be readily apparent to operators as a damaged circuit. A more difficult question arises if one postulates that corrupted signals are transmitted to operators.

If corrupted signals are transmitted to operators, they may be misled as to reactor status and may take improper response. For example, a false low water level signal could lead operators to activate additional water sources leading to overcooling of the reactor vessel. A false high level reading could lead operators to shut down or throttle coolant injection systems potentially leading to voiding of the core. To date, no fire PRA known to the authors has systematically addressed such issues.

As noted previously, a pronounced difference between thermoplastic and thermoset insulated cables has been observed which is directly relevant to the potential for transmission of corrupted signals. Thermoplastic insulated cables experienced a sudden failure with no appreciable pre-failure degradation of the transmitted signal. In contrast, thermoset insulated cables degraded over a period of minutes before ultimate loss of signal. Hence, it would appear that the potential for corrupted signals is primarily a factor for plants that utilize thermoset insulated instrument wires. While thermoset insulated cables are known to be predominant in control and power cable applications in the United States, the proportion of plants using thermoplastic versus thermoset insulated instrument cables is not known.

8.6.4 Summary of Circuit Fault Insights

Circuit faults have been discussed in the context of three primary circuit functions; namely, power, control/indication, and instrument circuits. Insights have been derived from both testing, and as discussed in Section 8.7 below, experience.

For power circuits, it is anticipated that most electrical cable failures will lead to a loss of motive power to the related components. Such losses will generally not be recoverable without some repair to replace or bypass the damaged electrical cables. Spurious actuations attributable to hot shorts in power cables are considered unlikely, but the actual likelihood depends on the nature of the power supply system.

The highest likelihood case involves single-phase AC power systems where only a single hot short is needed to cause a spurious operation. In general, an inter-cable hot short is required because of the common practice of utilizing separate electrical cables for each power circuit. A nominal upper bound conditional probability for these cases is estimated at 0.1, although a number of factors could reduce this probability substantially. For these systems some consideration of the risk implications of power cable failure induced spurious actuations would appear appropriate.

The likelihood of spurious actuation for ungrounded DC and three-phase AC power systems is far lower because multiple concurrent correct-polarity, correct voltage inter-cable hot shorts are required. Given the configuration of most power cables, and the apparently low likelihood of inter-cable hot shorts, such concurrent faults appear of low likelihood. Furthermore inter-cable hot shorts in power cables are unlikely to be sustained for any substantial period of time; hence, they are not likely to be risk significant.

One unique aspect of power cables discussed is the issue of multiple high-impedance faults. These scenarios postulate the concurrent existence of several electrical cable short circuits. Furthermore, the short circuit fault paths must each be of a very specific quality (i.e., fault resistance) in order for the postulated scenario to come about. For a number of reasons discussed previously, this would appear to be an unlikely scenario. In a risk context, loss of a higher-level bus attributable to failures in lower-level supply cables can be addressed based on random failure of the first line of circuit protection. In order to further assess the potential risk significance of such scenarios, these random failure probabilities could be adjusted to account for multiple high impedance fault scenarios, but no analysis of this type has yet been undertaken.

For control/indication circuits, many potential failure modes involving both the control and indication functions were discussed. The indication function circuit faults are primarily of interest to risk analysis in relation to their potential impact on operator actions or operator manual actions. No fire PRA to date has considered these issues; hence, their importance to risk is not known. The control functions, on the other hand, have broad-ranging implications. The one control circuit fault mode given the most attention has been spurious actuations. Both experience and experiments indicate that spurious operations are of relatively high likelihood given the failure of electrical cables that are susceptible to inducing such faults. Although a number of factors have been identified that substantially impact this behavior. Spurious actuation probabilities conditional on cable damage vary by at least one order of magnitude given variations in the identified factors.

A particular aspect of the spurious actuation fault mode discussed at some length was the question of multiple spurious actuations. Based on the existing evidence, multiple spurious actuations are both possible and potentially likely given the failure of multiple control cables susceptible to inducing such faults. Using the current estimates of the conditional probability of spurious actuation (given electrical cable failure), it is difficult to justify the screening of any given number of spurious actuation faults based on low likelihood and on a generic basis. For some special cases, such screening might be justified (e.g., cases involving armored electrical cables, cases involving electrical cables in conduits, and cases that require inter-cable hot shorts rather than intra-cable hot shorts). However, no firm basis for such screening has yet been established.

In the case of instrument circuits, the importance of circuit faults was discussed in the context of permissive signals and their impact on operator actions or operator manual actions. Again, no fire PRA to date has included a rigorous treatment of instrument circuit failure; hence, risk insights in this area are lacking.

8.7 Experience-Based Spurious Actuation Insights

As a closing discussion, this section provides a brief summary of insights related to spurious actuation circuit faults that derive from actual fire experience. In the experience base there are several fire incidents, both in the US and abroad, that illustrate spurious actuations. Chapter 3 of this report has already discussed the occurrence of multiple spurious actuations during the 1975 Browns Ferry electrical cable fire. The following additional spurious actuation examples are cited in NUREG/CR-6738:

- During a 1982 fire at the Armenian NPP, three reported spurious actuations and other control and indication problems are reported, all apparently caused by fire-induced electrical cable failures.
- The main generator breakers were closed inadvertently as a result of fire damage to the associated control cables. This led to the non-operating generators being connected to the grid and in turn caused secondary fires in one of the turbine-generators and in the startup transformer.
- One of the diesel generators spuriously disconnected from its emergency loads apparently as a result of control cable damage. Attempts to correct the failure during the fire were not successful.
- One feedwater pump spuriously started following damage to an electrical cable, apparently, in the control circuits. In this last case, the fault that actuated the pump by-passed the normal start logic allowing the pump to start without first starting the lube-oil pumps. Hence, the pump ran for some period without proper lubrication. The fault also by-passed or defeated the normal control room start/stop functions and operator attempts to shut down the pump from the main control room failed. The pump was ultimately secured by electrical technicians who isolated the pump from the power bus manually.
- Neutron flux and other reactor related instrumentation indicated conditions that may not have been the actual conditions of the reactor. This was likely because many of the instrument

cables were degraded and/or failed by the fire. These indications led to the actuation of various emergency signals. This incident is one of the few incidents where there is specific information indicating that multiple spurious actuations actually occurred during a fire.

- During a 1988 fire at the Ignalinan NPP, there were a number of cases where equipment was lost as a result of spurious trip signals caused by the failure of instrument and control cables. These included the following events:
- The control room received oil level alarms for one of the main coolant pumps and the pump tripped automatically. Failures in the oil level indicator and alarm circuit electrical cables are suspected to be the cause of the trip (rather than an actual drop in oil inventory).
- Instrumentation and control cable failures led to the opening of supply breakers for two normal 6 kV buses and two essential (nonsafety) buses.
- Control cable damage tripped Transformer 5 and prevented it from taking up the loads for these buses.
- A 1991 fire at Chernobyl Unit 2 was attributed to cable damage that resulted from poor cable pulling practices during plant construction. In this instance, a conductor-to-conductor short in a multi-conductor electrical cable led to spurious closure of a generator breaker, grid back-feed into the generator, generator rotor failure, turbine oil and generator hydrogen release and a large fire. In this case, an electrical cable failure caused spurious component actuations that in turn caused the fire.
- During a 1995 fire at Waterford, the event sequence log and the control room operator observations indicate erratic behavior in the position indication of a breaker or a pump. There is no verification in the incident report regarding the behavior of these items in the field. Hence, it is not clear if these are spurious indications only or are, in fact, spurious actuations.

Based on this experience, it is reasonable to conclude that given fire-induced electrical cable failures, spurious actuations are possible, if not likely. Event reports are not sufficiently detailed, however, to allow for a reliable statistical estimate of the likelihood of a spurious actuation given a fire and/or given fire damage. Fire event descriptions do not, in general, provide a sufficient level of detail regarding component/electrical cable damage and systems performance during a fire to support such an analysis with confidence.

The data also show that multiple spurious actuations involving either a single system (i.e., a system that actuates repeatedly during an event) or multiple systems are also possible. Again, data limitations prevent us from providing reliable estimates of the likelihood that any given number of actuations might occur in a fire. The cases noted previously show spurious actuations impacting up to three independent systems during a single fire event.

CHAPTER 9. REFERENCES

U.S. Nuclear Regulatory Commission Documents

Regulations

10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities.”

10 CFR 50.48, “Fire Protection.”

10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”
GDC 3, “Fire Protection.”
GDC 5, “Sharing of Structures, Systems, and Components.”
GDC 19, “Control Room.”
GDC 23, “Protection System Failure Modes.”

10 CFR Part 50, Appendix R,“Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979.”

Final Policy Statement, “Use of Probabilistic Risk Assessment Methods in Nuclear Activities,” U.S. Nuclear Regulatory Commission, *Federal Register*, V60, p. 42622, August 16, 1995.

Regulatory Guides

RG 1.6, “Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems,” March 1971.

RG 1.32, “Criteria for Safety-Related Electric Power Systems for Nuclear Power Plants,” Revision 2, February 1977.

RG 1.75, “Physical Independence of Electrical Systems,” Revision 2, September 1978.

RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis,” July 1998.

RG 1.189, “Fire Protection for Operating Nuclear Power Plants,” April 2001.

Branch Technical Positions

BTP APCSB 9.5-1, “Guidelines for Fire Protection for Nuclear Power Plants,” May 1, 1976.

BTP APCSB 9.5-1, Appendix A, “Guidelines for Fire Protection for Nuclear Power Plants Docketed Prior to July 1, 1976,” February 24, 1977.

BTP ASB 9.5-l, “Guidelines for Fire Protection for Nuclear Power Plants,” Revision 1, March 1979.

BTP CMEB 9.5-1 (Formerly BTP ASB 9.5-1), “Guidelines for Fire Protection for Nuclear Power Plants,” Revision 2, July 1981.

Generic Letters

GL 77-02, “Nuclear Plant Fire Protection Functional Responsibilities, Administrative Controls, and Quality Assurance,” August 29, 1977.

GL 80-100, “Resolution of Fire Protection Open Items,” November 24, 1980.

GL 81-12, “Fire Protection Rule (45 FR 76602, November 19, 1980),” February 20, 1981, and Clarification Letter, March 1982.

GL 83-33, “NRC Positions on Certain Requirements of Appendix R to 10 CFR Part 50,” October 19, 1983.

GL 85-01, “Fire Protection Policy Steering Committee Report,” January 9, 1985.

GL 86-10, “Implementation of Fire Protection Requirements,” April 24, 1986.

GL 86-10, Supplement 1, “Fire Endurance Test Acceptance Criteria for Fire Barrier Systems Used to Separate Redundant Safe Shutdown Trains Within the Same Fire Area to Implementation of Fire Protection Requirements,” March 25, 1994.

GL 88-12, “Removal of Fire Protection Requirements from Technical Specifications,” August 2,1988.

GL 91-18,”Information to Licensees Regarding Two NRC Inspection Manual Sections on Resolution of Degraded and Nonconforming Conditions and on Operability,” Revision 1, October 8, 1997.

Bulletins

BL 75-04, “Cable Fire at Browns Ferry Nuclear Power Station,” March 24, 1975.

BL 75-04A, “Cable Fire at Browns Ferry Nuclear Plant,” April 3, 1975.

BL 75-04B, “Cable Fire at Browns Ferry Nuclear Power Station,” November 3, 1975.

Information Notices

IN 84-09, “Lessons Learned From NRC Inspections of Fire Protection Safe-Shutdown Systems (10 CFR Part 50, Appendix R),” February 13, 1984.

IN 85-09, “Isolation Transfer Switches and Post-Fire Shutdown Capability,”January 31, 1985.

IN 87-50, “Potential LOCA at High- and Low-Pressure Interfaces from Fire Damage,” October 9, 1987.

IN 88-45, “Problems in Protective Relay and Circuit Breaker Coordination,” July 7, 1988.

IN 90-69, “Adequacy of Emergency and Essential Lighting,” October 31, 1990.

IN 91-17, “Fire Safety of Temporary Installations,” March 11, 1991.

IN 91-77, “Shift Staffing at Nuclear Power Plants,” November 26, 1991.

IN 92-18, “Loss of Remote Shutdown Capability During a Fire,” February 28, 1992.

IN 93-71, “Fire at Chernobyl Unit 2,” September 13, 1993.

IN 95-33, “Switchgear Fire and Partial Loss of Offsite Power at Waterford Unit 3,” August 23, 1995

IN 95-36, “Potential Problems with Post-Fire Emergency Lighting,” August 29, 1995.

IN 95-48, “Results of Shift Staffing Study,” October 10, 1995.

IN 97-37, “Main Transformer Fault With Ensuing Oil Spill Into Turbine Building,” June 20, 1997.

IN 98-31, “Fire Protection System Design Deficiencies and Common-Mode Flooding of Emergency Core Cooling System Rooms at Washington Nuclear Project Unit 2,” August 18, 1998.

IN 99-17, “Problems Associated With Post-Fire Safe-Shutdown Circuit Analyses,” June 3, 1999.

NUREG-Series Reports

Bennett, P.R., A.M. Kolaczkowski, and G.T., Medford, "Summary Report: Electrical Equipment Performance Under Severe Accident Conditions (BWR/Mark I Plant Analysis), NUREG/CR-4537, U.S. Nuclear Regulatory Commission, Washington, DC, September 1986.

Jacobus, M. J., and G.F. Fuehrer, "Submergence and High Temperature Steam Testing of Class 1E Electrical Cables,” NUREG/CR-5655, U.S. Nuclear Regulatory Commission, Washington, DC, May 1991.

Kazarians, M., and G. Apostolakis, "Fire Risk Analysis for Nuclear Power Plants,” NUREG/CR-2258, U.S. Nuclear Regulatory Commission, Washington, DC, September 1981.

Nowlen, S.P., M. Kazarians, and F. J. Wyant, "Risk Methods Insights Gained from Fire Incidents,” NUREG/CR-6738, U.S. Nuclear Regulatory Commission, Washington, DC, September 2001.

Nowlen, S.P., "Ampacity Derating and Cable Functionality for Raceway Fire Barriers,” NUREG/CR-6681, U.S. Nuclear Regulatory Commission, Washington, DC, August, 2000.

Nowlen, S. P., "An Investigation of the Effects of Thermal Aging on the Fire Damageability of Electric Cables,” NUREG/CR-5546, U.S. Nuclear Regulatory Commission, Washington, DC, May 1991.

NUREG-0050, "Recommendations Related to Browns Ferry Fire,” Report by Special Review Group, U.S. Nuclear Regulatory Commission, Washington, DC, February 1976.

NUREG/CR-1742, "Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program,” U.S. Nuclear Regulatory Commission, Washington, DC, April 2002.

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Section 19.0, Use of Probabilistic Risk Assessment in Plant-Specific Risk-Informed Decision Making: General Guidance,” U.S. Nuclear Regulatory Commission, Washington, DC, November 2002.

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition,” Section 9.5.1, "Fire Protection System,” U.S. Nuclear Regulatory Commission, Washington, DC, July 1996.

Subudhi, M., "Literature Review of Environmental Qualification of Safety Related Electric Cables,” NUREG/CR-6384, Volume 1, U.S. Nuclear Regulatory Commission, Washington, DC, April 1996.

Wheelis, W. T., "Users Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base,” NUREG/CR-4586, U.S. Nuclear Regulatory Commission, Washington, DC, August 1986.

Wyant, F. J., and S. P. Nowlen, "Cable Insulation Resistance Measurements Made During Cable Fire Tests, NUREG/CR-6776, U.S. Nuclear Regulatory Commission, Washington, DC, June 2002.

Commission Papers

SECY 80-438A, “Rule on the Fire Protection Program for Nuclear Power Plants Operating Prior to January 1, 1979,” September 30, 1980.

SECY 83-269, “Fire Protection Rule for Future Plants,” July 5, 1983.

SECY 93-143, “NRC Staff Actions to Address the Recommendations in the Report on the Assessment of the NRC Fire Protection Program,” May 21, 1993.

SECY 95-034, “Status of Recommendations Resulting from the Reassessment of the NRC Fire Protection Program,” February 13, 1995.

SECY 96-267, “Fire Protection Functional Inspection Program,” December 24, 1996.

SECY 99-040, “Second Interim Status Report–Fire Protection Functional inspection Program,” February 5, 1999.

SECY 99-140, “Recommendations for Reactor Fire Protection Inspections,” May 20, 1999.

SECY 99-182, “Assessment of the Impact of Appendix R Fire Protection Exemptions on Fire Risk,” July 9, 1999.

Inspection Program Documents

IMC 0609 Appendix F, “Fire Protection Significance Determination Process,” 2000.

IP-64100, NRC Inspection Manual, IM-64100, “Post-Fire Safe-Shutdown, Emergency Lighting and Oil Collection Capability at Operating and Near-term Operating Reactor Facilities.”

IP-64704, “Fire Protection Program,” June 24, 1998.

IP-71111.05, “Triennial Fire Protection Inspection Procedure,” March 2003.

NRC Inspection Reports

IR 50-254/98-011 and 50-265/98-011, “Fire Protection Inspection Quad Cities Nuclear Generating Station Units 1 and 2.”

IR 50-259/00-08, 50-260/00-08, and 50-296/00-08, “Fire Protection Baseline Inspection Browns Ferry Units 1, 2, and 3.”

IR 50-282/98-016 and 50-306/98-016, “Inspection of Prairie Island Nuclear Generating Station Fire Protection Functional Inspection Self Assessment.”

IR 50-313/01-06 and 50-368/01-06, “Triennial Fire Protection Baseline Inspection of Arkansas Nuclear One.”

IR 50-335/98-201 and 50-389/98-201, “Fire Protection Functional Inspection of St. Lucie Plant.”

IR 50-387/97-201 and 50-388/97-201, “Fire Protection Functional Inspection of Susquehanna Steam Electric Station.”

IR 50-458/97-201, “Fire Protection Functional Inspection River Bend Station Unit 1.”

Letters and Memoranda

BWROG Letter 1999 (BWROG-99-079), W.G. Warren to J. Hannon, “BWR Owners Group Appendix R Fire Protection Committee Generic Guidance for BWR Post-Fire Safe-Shutdown Analysis,” November 15, 1999.

Collins Letter 1997, S.J. Collins to R.E. Beedle (NEI), “Assessment of NEI Concerns Regarding NRC Information Notice 92-18, Potential for Loss of Remote Shutdown Capability During a Control Room Fire,” March 11, 1997.

Dembek Memo 1999, S. Dembek to S.A. Richards, “Summary of Meeting with Boiling-Water Reactor Owners Group (BWROG) Appendix R Committee on Post-Fire Safe-Shutdown Circuit Analysis Issues (Fire-Induced Circuit Failures).”

Denton Letter, Harold R. Denton, NRC, Letter to S.A. Bernsen, Bechtel Power Corporation (No subject), April 30, 1982.

Hannon Letter 2001, J. Hannon to D. Modeen (NEI), “Nuclear Energy Institute/Electric Power Research Institute Fire Testing: Comprehensiveness With Respect to Outstanding Circuit Analysis Issues (TAC No. MA4745),” February 1, 2001.

Holahan Memo, Gary M. Holahan, Memo to Dennis Crutchfield, Subject: “Request for Assistance: Determine Whether Two Hot Shorts in a Multiconductor Cable Associated with a Non-High/Low-Pressure Interface Should Be Analyzed for Fire-Induced Spurious Actuation (GL 86-10, Section 5.3.1, Non-High/Low-Pressure Interfaces in Ungrounded AC and DC Circuits) (AITS 205-89),” December 4, 1990.

Mattson Memo 1982, Roger J. Mattson, Memo to Richard H. Vollmer. Subject: “Position Statement on Allowable Repairs for Alternative Shutdown and on the Appendix R Requirement for Time Required To Achieve Cold Shutdown,” July 2, 1982.

Mattson Memo 1983, Roger J. Mattson, Memo to D. Eisenhut, Subject: “Task Interface Agreement #8 3-53, ‘Physical Independence of Electrical Systems,’ TAC No. 51567,” July 22, 1983.

Richards Letter 2000, S.A. Richards, Letter to J.M. Kenny, BWR Owners Group, “BWROG Appendix R Fire Protection Committee Position on SRVs and Low-Pressure Systems Used as Redundant Shutdown Systems Under Appendix R,” December 12, 2000.

Rubenstein Memo 1982, L.S. Rubenstein, Memo to Roger J. Mattson, Subject: “Use of the Automatic Depressurization System (ADS) and Low-Pressure Coolant Injection (LPCI) To Meet Appendix R, Alternate Shutdown Goals,” December 3, 1982.

Rubenstein Memo 1983, L.S. Rubenstein, Memo to Roger J. Mattson, Subject: “Statement of Staff Position Regarding Source Range Flux, Reactor Coolant Temperature, and Steam Generator Pressure Indication to Meet Appendix R, Alternate Shutdown Capability,” January 7, 1983.

Stello Letter, Victor Stello, Jr., Letter to David Bixel, Consumers Power Company, Subject: “Manpower Requirements for Operating Reactors,” Docket No. 50-255,” June 8, 1978.

Thadani Memo 1993, A.C. Thadani to T.E. Murley, Subject: “Report on the Reassessment of the NRC Fire Protection Program,” February 27, 1993.

Vollmer Memo 1983, R.H. Vollmer, Memo to Darrel G. Eisenhut, Subject: “Emergency Lighting Requirements,” (TIA 83-87; TAC 52308),” December 21, 1983.

Licensee Event Reports

LER 219/92-011, “Design Deficiency Causes Noncompliance with Appendix R Criteria,” Oyster Creek, September 15, 1992.

LER 247/96-007-00, “Potential Challenge of High/Low Pressure Interface,” Indian Point Unit 2, April 29, 1996.

LER 247/96-014-00, “Loss of Process Monitoring Function During Postulated Fires (Appendix R),” Indian Point Unit 2, August 26, 1996.

LER 266/97-020-01, “Conditions Outside Appendix R Safe-Shutdown Analysis,” Point Beach Nuclear Plant Unit 1, October 14, 1997.

LER 266/97-032-00, “Inadequately Rated Electrical Buses Could Disable Switchgear and Cause Secondary Fires That Prevent Shutdown Per Appendix R,” Point Beach Nuclear Plant Unit 1, July 30, 1997.

LER 266/99-008-00, “Postulated Fire Could Lead to Loss of Redundant Trains of Charging Capacity,” Point Beach Nuclear Plant Unit 1, November 3, 1999.

LER 266/00-008-00, “Inadequate Procedural Guidance for Spurious Opening of RHR to Containment Sump Valves SI-851A/B During Appendix R Alternate Shutdown,” Point Beach Nuclear Power Plant Unit 1, October 19, 2000.

LER 266/01-006-00, “Appendix R Requirements Not Satisfied for Unanalyzed Fire-Induced Damage to the Auxiliary Feedwater System,” Point Beach Nuclear Plant Units 1 and 2, February 4, 2002.

LER 272/99-011-00, “125 VDC Control Power Circuits for 4 kV Breakers Do Not Meet Requirements of 10 CFR Part 50 Appendix R,” Salem Generating Station Unit 1, November 12, 1999.

LER 280/99-003-00, “Potential Loss of Charging Pumps Due to Main Control Room Fire,” Surry Power Station Unit 1, April 28, 1999.

LER 298/96-009-00, “Appendix R Safe-Shutdown Analysis Vulnerabilities,” Cooper Nuclear Station, June 1, 1998.

LER 298/00-002-00, “Appendix R Safe Shutdown Analysis Vulnerability Due to Potential Conductor-to-Conductor Hot Shorts,” Cooper Nuclear Station, February 10, 2000.

Other Documents

ANSI/IEEE C.2, “National Electrical Safety Code.”

“Design Basis Document for Appendix R, Susquehanna Steam Electric Station Units 1 and 2,” DBD076, Pennsylvania Power and Light LLC, July 12, 2001.

Engineering Calculation EC-013-0843, “SSES 10 CFR Part 50 Appendix R Compliance Manual,” Susquehanna Steam Electric Station Units 1 and 2,” Pennsylvania Power and Light LLC, April 22, 2002.

Engineering Calculation G13.18.3.6*07, “Safe Shutdown Common Enclosure Associated Circuit Analysis, Gulf States Utilities,” September 27, 1994.

EPRI TR-1000894, “Fire Events Database for U.S. Nuclear Power Plants: Update Through 1999,” Electric Power Research Institute, Palo Alto, California 2000.

EPRI TR-1003326, “Characterization of Fire-Induced Circuit Faults: Results of Cable Fire Testing,” Electric Power Research Institute, Palo Alto, California 2002.

EPRI TR-1006961, “Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of an Expert Elicitation,” Electric Power Research Institute, Palo Alto, California 2002.

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

“Good Design Prevents High-Impedance Fault,” *Actual Specifying Engineer*, Volume 17, No. 4, Medalist Publications, Inc., Chicago, IL, 1967.

IEEE Std. 100-1998, “IEEE Standard Dictionary of Electrical and Electronics Terms,” 4th Edition, Institute of Electrical and Electronics Engineers.

IEEE Std. 242-1986, “IEEE Recommended Practices for Protection and Coordination of Industrial and Commercial Power Systems (Buff Book),” Institute of Electrical and Electronics Engineers.

IEEE Std. 141-1986, “IEEE Recommended Practices for Electric Power Distribution for Industrial Plants (Red Book),” Institute of Electrical and Electronics Engineers.

IEEE Std. 383, “IEEE Standard for Type Test of Class IE Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers.

IEEE Std. 690-1984, “IEEE Standard for the Design and Installation of Cable Systems for Class 1E Circuits in Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers.

IEEE Std. 835, “Standard Power Cable Ampacity Tables,” Institute of Electrical and Electronics Engineers.

LaChance, J., et al., “Circuit Analysis — Failure Mode and Likelihood Analysis: A Letter Report to the USNRC,” Sandia National Laboratories, Albuquerque, New Mexico, May 8, 2000.

NEI-00-01, Draft Revision C, “Guidance for Post-Fire Safe-Shutdown Analysis,” Nuclear Energy Institute, October 2001.

NEI-00-01, Draft Revision D, “Guidance for Post-Fire Safe-Shutdown Analysis,” Nuclear Energy Institute, October 2002.

NFPA Fire Protection Handbook, Section 6, 18th Edition, National Fire Protection Association, Quincy, Massachusetts.

NFPA 805, “Performance-Based Standard for Fire Protection for Light-Water Reactor Electric Generating Plants,” 2001 Edition, National Fire Protection Association.

Ramsey, C., et al., “United States Department of Energy Reactor Core Protection Evaluation Methodology for Fires at RBMK and VVER Nuclear Power Plants, DOE/NE-0113 Revision 1, U.S. Department of Energy (DOE), June 1997.

Sullivan, K., et al., “A Historical Fire Protection Licensing Document Describing Requirements for Commercial Nuclear Power Plants Operating in the United States,” USNRC Technical Report R7017/U7010, Brookhaven National Laboratory (BNL), Upton, New York, March 1995.

Sullivan, K., “Electrical Post-Fire Safe Shutdown Assistance for FPFI Procedure,” Technical Letter Report to NRC Office of Nuclear Reactor Regulation, Brookhaven National Laboratory (BNL), Upton, New York, September 23, 1996.

Sullivan, K., and R.E. Deem, “Baseline Tri-Annual Fire Protection Inspection — Braidwood Nuclear Power Station,” Technical Letter Report Input to NRC Region III, Brookhaven National Laboratory (BNL), Upton, New York, April 9, 2003.

Sullivan, K., “U.S. Commercial Nuclear Reactor Plant Post-Fire Safe-Shutdown Circuit Analysis History and Safety Significance/Discussion of Potential Severity of Fire-induced Reactor Plant Transients,” Technical Letter Report to the USNRC Office of Nuclear Reactor Regulation (JCN J-2427), Brookhaven National Laboratory (BNL), Upton, New York, July 20, 1998.

This page intentionally left blank.

APPENDIX A.
SUCCESSFUL IMPLEMENTATION OF APPENDIX R CIRCUIT ANALYSIS

APPENDIX A.
SUCCESSFUL IMPLEMENTATION OF APPENDIX R CIRCUIT ANALYSIS

A.1 Circuits of Concern to Post-Fire Safe-Shutdown

As described in Chapter 6, circuits of concern to post-fire safe-shutdown, fall into one of two broad categories:

(1) Circuits/cables of equipment needed to ensure the proper operation of the *systems* credited in the SSA for performing essential shutdown functions ("required" or "safety" circuits)

(2) Circuits/cables of equipment that, if damaged by fire, could impact the shutdown capability ("associated, "nonessential" or "nonsafety" circuits of concern)

Required Circuits

Because a cable or circuit is related to the operation of a required shutdown component does not necessarily mean it is of concern to post-fire safe-shutdown. As discussed below in Section A.2 below, the determination of whether or not a specific cable is required for safe-shutdown may depend on such factors as the specific function of the cable, the position/status (open, closed, running, stopped, etc.) of the component at the onset of fire, and the desired position/status of the component for shutdown. In general, a circuit/cable is considered to be required for safe-shutdown if it has the following characteristics:

(1) It is related to the operation of a required shutdown component

(2) Fire-induced faults in the circuit/cable can prevent the operation or cause a maloperation of the shutdown system in which the component is located

Power and control cables of Pump P-1 in Figure A-1 and control cables of valve V6 are typical examples of "required cables." In contrast,"associated nonsafety cables" are not directly related with the operation of any of the credited shutdown systems. Cable/circuits related to the operation of Valves V-9 and V-10 in Figure A-1 are examples. Although not needed to ensure operation of the credited shutdown systems, fire damage to circuits such as these could significantly impact the shutdown capability.

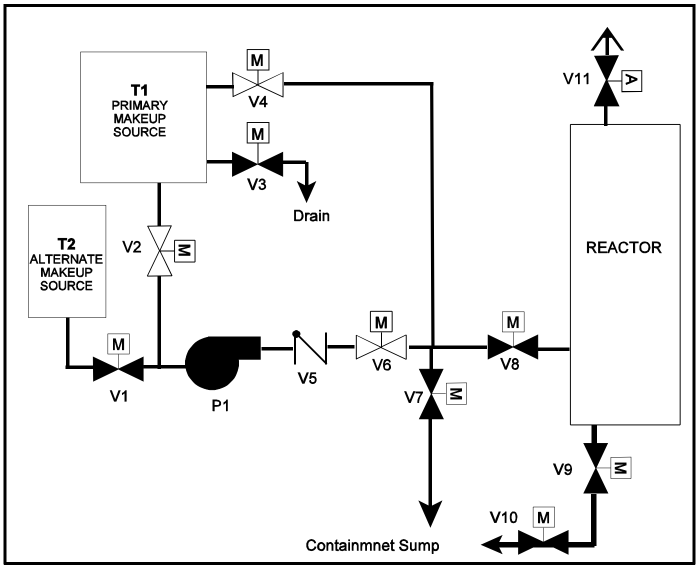


Figure A-1 Simplified Shutdown System Flowpath

Associated Circuits of Concern

The achievement of safe-shutdown is dependent on ensuring the active control of some components and preventing the maloperation of other components. A post-fire safe-shutdown analysis should be a bounding analysis that identifies the range of possible fire impacts within each fire area (vulnerabilities) and ensures that appropriate measures are in place to prevent this damage from affecting the ability to safely shutdown the plant. Therefore, it is not sufficient to only consider the effects of fire damage to cables of equipment needed to ensure operation of credited shutdown *systems* (required circuits). The scope of a successful shutdown strategy will consider the effects of fire damage to nonessential equipment and systems of which inadvertent or spurious actuation could impact the shutdown capability (associated nonsafety circuits).

The principal staff guidance related to the potential impact of fire-induced circuit failures in “nonessential” or “associated” circuits is contained in GL 81-12, dated February 20, 1981, and its subsequent clarification, dated March 22, 1982. As described in these documents, there are three specific configurations of associated circuits of concern to post-fire safe-shutdown:

- Nonessential circuits that share a **common power supply** (e.g., SWGR, MCC, Fuse Panel) with circuits of equipment required to achieve and maintain safe-shutdown; or,
- Nonessential circuits that share a **common enclosure**, (e.g., raceway, conduit, junction box, etc.) with cables of equipment required to achieve and maintain safe-shutdown
- Circuits and cables that have a connection to equipment of which **spurious operation** would adversely affect the shutdown capability.

With few exceptions, most licensees successfully resolve common power supply and common enclosure associated circuit concerns on a plant-wide basis through the performance of generic evaluations of electrical protective devices (e.g., fuse/breaker coordination studies). When resolved in this manner, the types of circuits/cables of concern to post-fire safe-shutdown are then reduced to two specific classifications:

(1) *Required Cables*: Circuits/cables of equipment needed to ensure the proper operation or functioning of shutdown systems defined/designated in the SSA.

(2) *Spurious Nonsafety Cables*: Circuits/cables of systems and equipment that are not needed to ensure the operation of shutdown systems credited in the SSA, but of which inadvertent (spurious) actuation or maloperation could impact the shutdown capability.

In its clarification of GL 81-12, the staff defined the scope of the spurious operation associated circuit concern as those circuits/cables that could impact the safe-shutdown capability if they are damaged by fire*.* As shown in Figure A-2 (Reference GL 81-12 Clarification, Enclosure 2), a fundamental presumption of the GL is that circuits/cables of equipment that could prevent operation or cause the maloperation of redundant shutdown systems (i.e., required circuits) are provided with fire protection features sufficient to meet Section III.G.2 of Appendix R, and therefore, would remain *free of fire damage*. As shown in Figure A-2, however, even when redundant trains of "required" cables meet III.G.2 criteria, fire damage to circuits/cables of "nonessential" systems and equipment (i.e., not needed to ensure operation of the defined/credited shutdown systems) may significantly impact the shutdown capability.

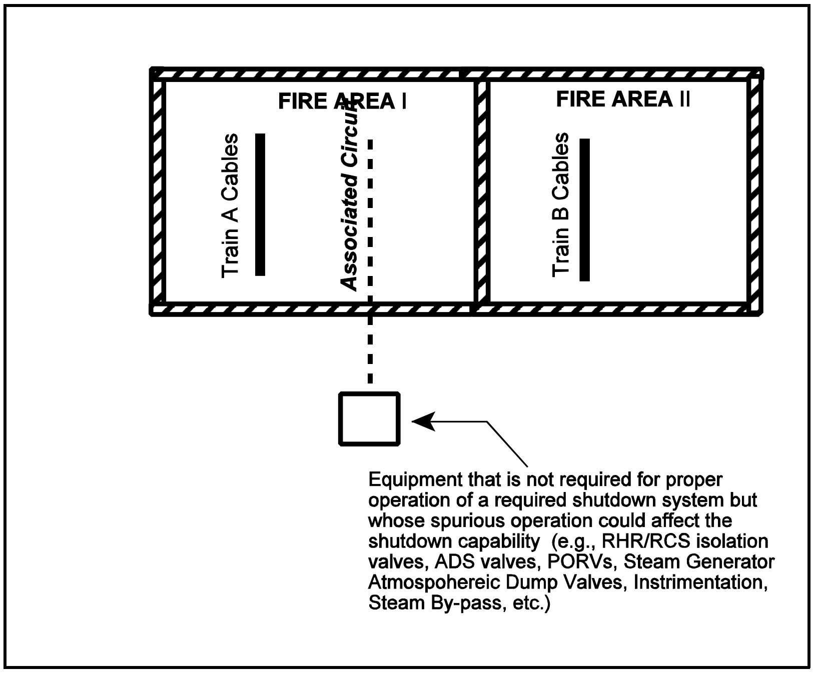

FIRE AREA I
FIRE AREA II
Train A Cables
Associated Circuit
Train B Cables
Equipment that is not required for proper operation of a required shutdown system but whose spurious operation could affect the shutdown capability (e.g., RHR/RCS isolation valves, ADS valves, PORVs, Steam Generator Atmospohereic Dump Valves, Instrimentation, Steam By-pass, etc.)

Figure A-2 Spurious Operation Associated Circuits of Concern

As described in this document, a common approach for ensuring that the SSA sufficiently bounds the range of circuit failures of concern to post-fire safe-shutdown starts by defining *shutdown success paths* (redundant and alternative), where each path is comprised of a set of systems (i.e., credited shutdown systems) capable of accomplishing each of the required shutdown functions (e.g., reactivity control, DHR). With the shutdown paths and systems defined, equipment needed to ensure the proper operation of the credited shutdown systems (required components) *and* nonessential/nonsafety equipment or systems of which spurious actuation could impact the shutdown capability are then identified and documented on a SSEL. As a result of this process, the SSEL will include all components (essential and nonessential) that could impact the shutdown capability if they are damaged by fire, and will not be limited to only those components needed to ensure the operation of the defined shutdown systems. From this comprehensive listing of equipment, the SSEL can then serve as a starting point for identifying circuits and cables of concern to post-fire safe-shutdown in each fire area.

A.2 Resolving Identified Vulnerabilities

When circuits/cables of concern to post-fire safe-shutdown are found to be located in a specific fire area under evaluation, the analyst has several options for ensuring that an appropriate level of fire safety is achieved, as illustrated by the following examples:

(1) Assuming that fire damage to affected circuits/cables will cause connected equipment to fail in an undesired manner and providing fire protection features sufficient to satisfy Section III.G.2 of Appendix R (while this approach requires no additional analysis it may not be cost-effective),

(2) Revising the shutdown strategy developed for the specific fire area under evaluation (e.g., use of other equipment)

(3) Demonstrating, through the performance of a detailed circuit failure mode and effects analysis (circuit analysis), that the credible range of circuit faults (as described in Chapter 6) to all exposed circuits/cables of concern will not impact the shutdown capability

(4) Requesting an exemption or deviation from specific technical requirements of regulatory requirements (see Section 4.5)

The challenge to the fire safety analyst and plant operating organization is to determine the best solution possible based on its ability to provide cost-effective protection against the threat of fire in a manner that is consistent with regulatory criteria and the plant’s fire protection licensing basis.

During the initial stages of a fire area assessment, it is not uncommon to identify a large number of cable/circuit “interactions” or “cable hits.” Since each “interaction” or “hit” represents a potential noncompliance with established separation/protection requirements, all interactions must be resolved. This may be accomplished by either the installation of additional fire protection features (e.g., meet Section III.G.2 of Appendix R), or through a rigorous analysis of the effect of fire damage to each circuit/cable involved in the identified interactions (circuit analysis).

Since it is typically not desirable to perform unnecessary plant modifications, most plants elect to perform a comprehensive analysis of each interaction. Since such an analysis can also be a time-consuming, resource-intensive process (particularly if excessive engineering effort is expended in the evaluation of circuits/cables that would not impact safe-shutdown if they are damaged by fire), it is desirable to limit its scope to only those circuits/cables that could actually impact the shutdown capability if they are damaged by fire. In cases where the SSEL is sufficiently comprehensive to bound the range of circuit failures of concern to post-fire safe-shutdown, licensee's have shown that the number of circuits/cables requiring a detailed review can be significantly reduced by considering the function, normal operating mode/status, and desired operating mode/status of components related to the identified cable/circuit interactions. The application and benefits of this screening technique are illustrated in the following example.

As discussed in Chapter 6, not all cable/circuit failures identified as "potential interactions" will impact the ability of connected equipment to function as needed for post-fire safe-shutdown. For example, since MOVs fail to the "as-is" position upon a loss of motive power, a loss of power to "normally closed" MOVs V-3, V-7, V-9 and V-10 (shown in Figure A-1), will not impact the shutdown capability. A loss of motive power to these valves will only cause them to remain "closed" which is their desired position for post-fire safe-shutdown. Additionally, if spurious actuation (opening) would not result in a LOCA, (i.e., the valves do not comprise a high/low pressure interface boundary) the power cables may be screened from further consideration for spurious actuation concerns. For the example shown, this would include power cables for valves V-3 and V-7. Since valves V-9 and V-10 comprise a high/low pressure interface, their power cables can not be screened at this point in the evaluation.

A.2.1 Use of Operator Manual Actions

Section III.G.2 of Appendix R requires that circuits that could prevent the operation or cause maloperation of redundant trains of safe-shutdown equipment have one of the specified fire protection features. Operator manual actions to respond to maloperations are not listed as an acceptable method for satisfying this requirement. However, the NRC has previously accepted plant-specific operator manual actions in formal exemption/deviation requests and in SERs. Rulemaking is currently in progress to codify the use of acceptable manual operator actions as discussed below.

Based on inspection results and industry comments the NRC determined that licensees have, without request for exemption/deviation from the code, implemented operator manual actions where the specified requirements of Section III.G.2 cannot be met. The staff concluded that rulemaking would be required to allow licensees committed to Appendix R to substitute operator manual actions in lieu of Section III.G2 compliance. For an interim period, while rulemaking is in progress, the staff determined that acceptance criteria can be developed which would facilitate evaluations of certain operator manual actions. Authority to approve a licensee methodology that does not meet NRC regulations is not delegated to the inspectors. However, inspectors will ensure that plant-specific operator manual actions meet the following guidelines:[34]

[34] NRC Inspection Procedure 71111.05, March 6, 2003.

- **Diagnostic Instrumentation**
  Adequate diagnostic instrumentation, unaffected by the postulated fire, is provided for the operator to detect the specific spurious operation or maloperation that occurred. Additional instrumentation beyond that identified in IN 84-09 may be needed to properly assess a spurious operation. Annunciators, indicating lights, pressure gages, and flow indicators are typical examples. Sufficient instrumentation should also be available to verify that the operator manual action accomplished the intended objective.

- **Environmental Considerations**
  The environmental conditions the operator may encounter while accessing and performing the operator manual action have been fully considered. Radiation levels should not exceed normal 10 CFR Part 20 limits. Emergency lighting should be provided as required in Appendix R, Section III.J or by the licensee's approved FPP. Temperature and humidity conditions should be reviewed to ensure that temperature and humidity do not affect the capability to perform the operator manual action. Fire effects should be reviewed to ensure that smoke and toxic gases from the fire do not affect the capability to perform the operator manual action.

- **Staffing**
  Adequate qualified personnel are on shift and available perform the required operator manual actions and to safely operate the reactor.

- **Communications**
  If operator manual action coordination with other plant operations is required, then communications capability must be protected from effects of a postulated fire.

- **Special Tools**

  If special tools are required they are dedicated for use and readily available from an accessible nearby location.

- **Training**
  Operators are trained on the operator manual actions and the procedure is adequate and current.

- **Accessability**
  Operator is capable of reaching the required location without personal hazard. If a ladder or other special access equipment is needed, it should be readily available.

- **Procedures**
  Procedural guidance has been developed to implement the operator manual actions. Operators should not rely on having time to study normal plant procedures to find a method of operating plant equipment that is seldom used.

- **Verification and Validation**
  All operator manual actions have been verified and validated (V&V) by plant walkdowns using the current procedure. The licensee has adequately evaluated the capability to perform the operator manual action in the time available before the plant will be placed in an unrecoverable condition.

A.3 Plant-Specific Examples of Successful Implementation

The following six examples show how cable/circuit vulnerabilities have been successfully identified and resolved by licensees. The examples are based on actual problems that were identified by licensees during recent re-evaluations for Appendix R compliance. In addition to illustrating the potential impact that fire-induced circuit failures may have on the ability to achieve and maintain safe-shutdown conditions, the examples also illustrate the extent and depth of the analysis.

Case 1 Potential for Secondary Fire Initiation

Problem During a reevaluation of its Appendix R program in 1997, a licensee of a PWR discovered that fault currents generated as a result of fire damage to power cables could be larger than the interrupting capability of the connected SWGR. If the associated SWGR is located in a different fire area, then this overcurrent condition could lead to another, secondary fire. This condition is unacceptable because the SSA assumes the occurrence of a single fire. The capability of the plant to achieve and maintain safe-shutdown for fires in multiple fire areas had not been demonstrated.

Resolution In order for the failure scenario described above to occur two conditions must exist: (1) the fault current must exceed the interrupting capability (rating) of the SWGR and (2) the fire must occur in a fire zone other than where the SWGR is located. Since cable impedance (which is generally proportional to cable length) will reduce the magnitude of fault current, the licensee performed an evaluation to determine the minimum distance away from the SWGR that a fault must occur for the cable's impedance to reduce the magnitude of fault current to a value within the rating of the SWGR. In addition, the routing of each cable was reviewed to determine whether the cable's route took it through different fire areas than that in which the SWGR was located. As a result of this review, the licensee identified six fire zones where the initiating fire had a potential to cause a secondary fire at the associated SWGR. As an immediate corrective action the licensee implemented compensatory measures to establish a roving fire watch in each of the six identified fire zones. As a permanent corrective action, the licensee implemented design changes to ensure that the subject SWGRs are capable of interrupting fault currents that may be generated during a fire.

Case 2 Inadequate Coordination Could Disable Essential Instrumentation

Problem In 1997, during a review of electrical cable routing, a PWR licensee discovered that a 125 VDC power cable was exposed to the effects of fire damage. Fire-induced faults (short to ground) in this cable, coupled with a lack of circuit breaker coordination on the 125 VDC system, could result in a loss of power to instrumentation that is essential for achieving and maintaining post-fire safe-shutdown. The licensee determined that this condition was caused by an inadequate review of a plant modification for Appendix R concerns. (See Chapter 7.) The modification routed a new "associated circuit" cable without verifying the adequacy of circuit breaker coordination.

Resolution Compliance with Section III.G.2 of Appendix R was achieved by implementing a plant modification to enclose the power cable in a 1-hour rated fire wrap.

Case 3 “Hot Short” Could Result in a Loss of the Service Water System

Problem In year 2000 the licensee of a BWR discovered that a fire-induced circuit fault resulting from fire in the CSR could lead to a loss of all service water cooling to essential shutdown systems. Although three sources of water to the service water pump seals are normally available, all three sources could be lost as a result of fire damage in the cable spreading room. The specific vulnerability involved a multi-conductor cable that carries 24 VDC start control circuits for the pump that is credited in the licensee’s analysis for providing cooling water to the gland seals of the service water pumps. A conductor-to-conductor short, either between individual conductors of the multi-conductor cable, or between conductors of the multi-conductor cable and conductors of two other cables located inside the same conduit, could cause the 24 VDC start control circuits to be energized by 120 VAC power. This condition could disable the automatic starting and running of the pump relied on to provide cooling water to the service water pump gland seals. The service water pumps are required to operate during and after a fire to supply cooling water to essential shutdown equipment. The loss of the service water system would prevent the plant from achieving and maintaining safe-shutdown conditions.

Resolution The licensee has developed modifications to eliminate this vulnerability. In the interim, the licensee posted a continuous fire watch in the cable spreading room.

Case 4 Multiple Circuit Faults Could Cause a Loss of all Makeup/Charging Capability

Problem During a re-evaluation of its Appendix R analysis a licensee of a PWR discovered that a fire could result in damage to any of the operating charging pumps. The charging system provides makeup water to the RCS, reprocesses water letdown from the RCS, and provides seal water injection to the reactor coolant pump seals. During normal plant operations two pumps are running and the third pump is secured in standby. At least one pump must be available to support safe-shutdown. A temporary loss of charging is acceptable as long as one pump can be restored within 30 minutes with full pump capacity. However, if the running pump(s) is the only credited pump available (i.e., other pumps are unavailable because of fire-induced failures), its failure/loss as a result of fire would lead to a total loss of all charging capability.

The normal suction supply to the operating charging pumps is from the volume control tank (VCT). During its re-evaluation the licensee discovered that multiple circuit faults could cause a loss of all charging capability. Specifically, a hot short on the control cable of an MOVs located in the VCT supply line could cause the valve to shut. Although an alternative source of water is available from the refueling water storage tank (RWST), the same fire could also damage cables for the charging water supply valve and prevent that valve from opening. The spurious actuation (close) of the VCT isolation valve and a failure of the RWST valve to open would result in a loss of suction and subsequent pump damage.

Resolution The licensee identified the specific fire zones where this scenario may occur and installed modifications to correct cable routing and separation deficiencies.

Case 5 Potential Loss of All Vital Buses As a Result of Multiple Faults In Ungrounded DC Control Circuits

Problem The alternative shutdown strategy developed by a licensee of a PWR relied on operator manual actions to isolate 125 VDC control power to breakers of 4 kV SWGR. This was accomplished by opening the feed breaker to the bus. With the control power isolated, the licensee had assumed that the 4kV breakers could then be manually operated as needed. During a recent, 1999 reassessment of its safe-shutdown analysis, however, the licensee discovered that in the event of fire in certain alternative shutdown areas, cables associated with the 125 VDC control circuits could experience fire damage resulting in an external hot short on the positive side of the open/close coils. If this fault were to occur in combination with multiple grounds on the negative legs of the 125 VDC circuit, the closing or trip coils would become energized. Fire-induced shorting/grounding of 4 kV circuit breaker 125 VDC control circuits could result in inadvertent opening or closing of these breakers, or inability to locally position these breakers manually. This scenario could lead to a loss of all three vital buses.

Since the 125 VDC system was ungrounded, the licensee had assumed that a review of these circuits for spurious actuation was not required. At the time of its original analysis, operator manual actions to remove 125 VDC control power from the breakers was considered adequate to isolate the 4 kV breakers from the alternative shutdown areas and allow manual manipulation of the breakers. During its re-evaluation, however, the licensee recognized that this assumption was not consistent with staff guidance described in Question 5.3.1 of GL 86-10, which requires an analysis of sufficient depth to determine the adverse impacts of hot shorts, shorts to ground, or open circuits on safe shutdown related control circuits and their associated logic.

Resolution The licensee intends to implement corrective actions necessary to resolve compliance with Appendix R as part of its corrective action program.

Case 6 Spurious Opening of Multiple Safety Relief Valves

Problem During a reevaluation for compliance with Appendix R to 10 CFR Part 50 the licensee of a BWR determined that a control room or relay room fire could cause multiple SRVs to spuriously open resulting in rapid depressurization and inventory loss. The cables associated with the SRVs share a common cable tray, and single hot short will result in the spurious opening of each SRV. Given the potential for fire-induced failures high-volume makeup systems capable of mitigating this event [CR, RHR, low-pressure coolant injection (LPCI) and HPCI] may not be immediately available. The consequence of multiple SRV failures without the availability of a high-volume injection system could lead to core uncovery.

There are 11 DC-operated SRV, of which seven in the ADS are automatically controlled by relay logic circuits. The remaining four SRVs are manually controlled. For each valve, one of the two solenoids is operable from the control room. The other solenoid is operated from the local SRV control panel located in the reactor building. The solenoids are powered from redundant DC power sources. In the event of fire requiring control room evacuation, all eleven SRVs can be operated manually at the Local SRV control panel. However, since there was no provision for isolating the SRV solenoids from the control room, a control room or reactor building fire could induce a hot short and spuriously open these valves irrespective of the position of control switches located in the control room.

Resolution To ensure SRV operation in the event of a control room fire the licensee implemented plant modification to install a dedicated isolation switch for each of the eleven SRVs in a new auxiliary shutdown panel located outside the control room. In addition, the licensee modified the circuitry of the seven ADS valves and the four manual SRVs to provide additional isolation capability in the event of a reactor building or control room fire.

APPENDIX B.
SPECIFIC CIRCUIT ANALYSIS ISSUES

APPENDIX B.
SPECIFIC CIRCUIT ANALYSIS ISSUES

This appendix discussed certain circuit analysis issues that specific have been the subject of much confusion and debate and include: multiple spurious actuations, fire damage to nonessential systems, and multiple circuit faults. The discussion is provided in terms of "real world"examples of technical issues that were identified during the review of safe-shutdown analyses developed by various licensees.

B.1 Multiple Spurious Actuations

In Question 5.3.10 of GL 86-10, the staff provides a response to a question posed by industry regarding the type of plant transients that should be considered in the *design of the alternative or dedicated shutdown systems*. In its response the staff states, in part: *"the safe shutdown capability should not be adversely affected by any one spurious actuation or signal resulting from a fire in any plant area."*

The intent of the guidance contained in the staff's response is to ensure that the *design* of the alternative or dedicated shutdown capability is sufficiently robust to be capable of mitigating the occurrence of one worst-case spurious actuation prior to isolation of potentially affected circuits from the fire-affected area. In certain instances, however, the staff's response has been mis-interpreted to mean that only a single spurious actuation need be considered for any fire area, without any further consideration of the number, type, function, or specific location of potentially affected circuits and cables. This misunderstanding appears to have been further complicated by the fact that this approach (i.e., assumption of a single spurious actuation per fire event) has been accepted in several NRC safety evaluations of plant-specific post-fire safe-shutdown methodologies. While the fire protection licensing basis for these facilities would only require consideration of a single spurious actuation, it should be noted that certain licensees recognize that the application of this assumption could result in a shutdown strategy that is inconsistent with the fundamental objective of ensuring that one train of systems needed to achieve and maintain hot-shutdown conditions remains free of fire damage. For example, although the "single spurious actuation per fire event" assumption was accepted by the staff in a safety evaluation of a BWR, an NRC inspection of this facility did not identify any cases where the potential for fire to cause multiple spurious actuations had not been sufficiently evaluated. Specific cases of how this "single spurious actuation per fire event" assumption can impact the shutdown capability are illustrated by the following examples:

- At one PWR cooling water flow to the EDG may be provided by one of two parallel flowpaths. Since a "normally open" MOV is located in each flowpath, at least one of these valves must remain open to ensure an adequate supply of cooling water is supplied to the EDG. Based on its interpretation of Question 5.3.10 of GL 86-10, however, the licensee had not considered the potential for both valves to spuriously change position as a result of fire damage. In lieu of identifying the routing of cabling associated with both valves by fire area and evaluating for the potential effects of fire damage to these circuits/cables within each fire area, the licensee had dispositioned this potential vulnerability on the assumption (per its interpretation of GL 86-10 Question 5.3.10) that only one spurious actuation would occur per fire event. As a result of its interpretation, the potential for fire to cause both valves to inadvertently change position as a result of fire damage was not considered in the analysis.

- As described in Chapter 6, the SSEL identifies equipment that is needed to ensure the successful accomplishment of essential shutdown functions. Based on its assumption that only one spurious actuation would occur per fire event, the shutdown methodology developed by a licensee of a 4-loop Westinghouse PWR relied on operator intervention to mitigate this "one" actuation should it occur. Since no action is taken before fire damage occurs, the successful implementation of this approach is largely predicated on the operators' ability to detect the spurious actuation and perform manual actions in a timely manner to defeat its effect on safe-shutdown capability. Based on this approach, the SSEL did not include any automatically actuated flow-path valves MOVs or air-operated valves (AOVs)] that were in their desired position for post-fire safe-shutdown during normal plant operations (e.g., a normally open MOV in the flowpath of a required shutdown system). Since the SSEL serves as a starting point for identifying circuits and cables that could impact the shutdown capability if they are damaged by fire, the routing of cables associated with these components was not considered. As a result, the potential for fire to cause more than one automatically actuated valve to spuriously change position in an undesired manner for post-fire safe-shutdown had not been evaluated for each fire area.

- A review of the SSA submitted by the licensee of a BWR identified examples where redundant components may be subject to spurious actuations (i.e., undesirable change of position or operating state) as a result of a single hot short on each of their respective control circuits. Although the control circuits of the redundant MOVs were subject to damage by a single fire, in its evaluation of this issue, the licensee stated: "*For both valves to open simultaneously, a hot short on each valve is required. NRC GL 86-10 does not require the assumption of multiple hot shorts for non-high/low-pressure interfaces. Therefore, one of these two valves is assumed to remain closed."* In subsequent meetings and correspondence, the staff informed the licensee of its concern that the application of this assumption may result in an inability to adequately demonstrate compliance with Sections III.G.2 and III.L of Appendix R to 10 CFR Part 50. In a subsequent response, the licensee submitted revised criteria it had developed and employed for the analysis of potential spurious operations. Under its revised methodology, all circuits which could cause undesirable spurious operations were identified and evaluated for potential fire damage. With the exception of components which comprise a high/low pressure interface boundary the licensee's evaluation considered any and all spurious operations that may occur as a result of a single fire, on a one-at-a-time basis (i.e., sequential, nonconcurrent). That is, for each fire area all potential spurious operations that may occur as a result of a postulated fire were identified, and corrective actions were implemented as needed on a one-at-a-time basis. Fire-initiated faults were assumed to exist until action was taken to negate their effects. The fire was not postulated to eventually clear the faults. For redundant components which form a high/low pressure interface boundary, the evaluation considered the potential for concurrent, simultaneous, spurious operations. When cables or equipment of which spurious operation could affect safe-shutdown were identified, they were included as required cables in the licensee's Appendix R separation analysis.

- The licensee of a BWR used the single spurious actuation per fire event assumption as a basis for not providing fire protection features for redundant trains of shutdown equipment. In this case, although redundant suction valves of the RCIC system were identified as being required to achieve and maintain hot shutdown conditions and their cables were located in close proximity [<4.56 m (<15 ft)], the licensee did not consider the separation requirements of Section III.G.2 to be applicable on the basis that both valves must fail (spuriously actuate to the closed position) in order to cause a total loss of makeup capability.

Section III.G of Appendix R to 10 CFR Part 50 requires, in part, that circuits and cables that could prevent operation or cause maloperation of SSCs important to safe-shutdown be provided with a level of fire protection necessary to ensure that such circuits will remain free of fire damage. Consistent with the deterministic approach described in Chapter 6, circuits and cables which lack a suitable level of fire protection (as delineated in Section III.G.2 of Appendix R) must be assumed damaged by their exposure to fire and this damage should be expected to cause one or a combination of circuit faults to occur between conductors of each cable or circuit that may be affected by the fire. Accordingly, if, because of a lack of fire protection features, there is a potential for multiple cables or circuits to be faulted, it follows that faults between the conductors of the affected cables or circuits may lead to the occurrence of one or more (i.e., multiple) spurious actuations. In a letter to the NEI dated March 11, 1997, the staff reiterated the deterministic approach where the number of spurious signals or changes in operational configuration that may be expected to occur as a result of fire damage to unprotected cables or circuits cannot be predicted.

As described in Chapter 6 and Appendix A to this document, licensees have historically identified equipment (safety-related and nonsafety-related) of which spurious operation could impact the safe shutdown capability described in the plant-specific SSA. If it can be demonstrated that the occurrence of all credible circuit failure modes (hot shorts, open circuits and shorts to ground), will not cause the connected equipment to spuriously actuate or malfunction in a manner that would adversely impact the post-fire safe-shutdown capability, no further analysis is necessary and the component may be screened from further evaluation. For example, a review of plant P&IDs may indicate that the spurious actuation (opening) of two, series connected, MOVs has the potential to impact the shutdown capability by creating an undesired diversion (i.e., loss) of process coolant flow. If it can be shown that this failure mode (both valves open) would not impact the shutdown capability (e.g., if the amount of flow lost was small compared to the makeup capability of the system) the components (MOVs) can be screened from further consideration. However, if this initial evaluation determines that spurious actuation of the components (opening of both MOVs) could impact the shutdown capability (flow loss in excess of makeup capability), a detailed circuit analysis that considers the impact fire damage to connected circuits and cables is necessary.

As discussed in Chapter 6, with the exception of components that comprise a high/low pressure interface boundary, the evaluation should consider any and all spurious operations that may occur as a result of a single fire, on a one-at-a-time basis. That is, for each fire area, all potential spurious operations that may impact the shutdown capability should be identified. While it is not assumed that all such spurious actuations will occur instantaneously at the onset of fire, the analyst must consider the possibility for each spurious actuation to occur in a sequential manner, as the fire progresses, on a one-at-a-time basis. Since it is not assumed that the fire will clear the fault(s) that caused the undesired actuation (Reference GL 86-10, response to Question 5.3.2), the potential for sequentially occurring failures to result in the concurrent failure of two or more components (such as the MOVs described above) must be considered. Accordingly, if control cables of two components (e.g., normally-closed MOVs) are subject to damage, the potential for both valves to spuriously actuate (open) as a result of fire damage cannot be ignored. Since the control cable of neither valve is ensured to remain free of fire damage, it is considered credible that both valves could spuriously open sequentially during a fire event. It is expected that such conditions would be identified where they may exist and appropriate preventive or mitigating actions implemented.

Although they do not satisfy the certain technical requirements of Appendix R, the use of operator manual actions to mitigate this event may provide an acceptable resolution (see Appendix A). For example, the licensee's evaluation of a control room fire at one BWR found circuits of three valves to be susceptible to fire damage. Since the spurious opening of all three valves would result in a drain down of the suppression pool, the potential for all three valves to spuriously actuate could not be ignored. To mitigate this event, the licensee implemented procedural changes which require one of the valves to be ensured closed by operator manual actions.

B.2 Fire Damage to Nonessential Systems

Fire damage to systems that are not needed to perform essential shutdown functions (i.e., nonessential or nonsafety systems) can have a significant impact on shutdown capability, as illustrated by the following examples:

- Inadvertent initiation of the HPCI system: The analysis performed by one BWR revealed that inadvertent initiation of the HPCI system and concurrent loss of the 137.16-cm (54-in.) high-water trip for HPCI as a result of a control room fire could, in a short time period (approximately 3 minutes), cause a vessel overfill condition to the point where HPCI would be disabled and the main steam lines would be filled with high pressure water.
- Inadvertent feedwater initiation: Certain BWRs employ steam-driven feedwater pumps in their design. Since these pumps are not electrically powered they will continue to provide flow during feedwater system coast down as long as sufficient steam is available. The concern with this configuration is that a fire-induced spurious signal on the feedwater pump control circuit (typically located in the control room) could cause a false demand for the steam-driven pumps to inject coolant at maximum capacity. If this were to occur, operators would have a very short time frame to implement mitigating actions, such as closing the MSIVs, closing of the feedwater discharge valves, and tripping the feedwater turbine from outside the MCR.
- The normal charging line to the RCS was not credited for post-fire safe-shutdown by the licensee of a PWR. This flowpath, which branches off the credited RCP seal injection flowpath, includes four normally open valves before entering the regenerative heat exchanger. The pressurizer auxiliary spray valve (PASV), which is located downstream of the regenerative heat exchanger, is a normally closed MOV. Since the normal charging flowpath was not credited for safe-shutdown, none of the valves in its flowpath were included in the SSEL. As a result, none of the cables associated with these valves were fully evaluated for the effects of fire damage. While not needed to perform an essential shutdown function, the spurious opening of PASV as a result of fire-induced faults in its control circuitry could have a significant impact on the shutdown capability by causing a collapse of the steam bubble in the pressurizer and rapid depressurization of the RCS.
- The shutdown strategies developed by most PWRs do not credit the use of pressurizer heaters. While not needed for safe-shutdown, fire damage that causes the heaters to inadvertently actuate (load) at a time when power is being supplied from the onsite source of electrical power (e.g., EDG) could significantly impact safe-shutdown capability if the EDG was not capable of supplying this additional load (EDG overload).

As discussed in Chapter 6 and Appendix A, the achievement of safe-shutdown is dependent on ensuring the active control of some components and preventing the maloperation of other components. A post-fire safe-shutdown analysis should be a bounding analysis that identifies the range of possible fire impacts within each fire area (vulnerabilities) and ensures that appropriate measures are in place to prevent this damage from affecting the ability to safely shutdown the plant. Therefore, it is not sufficient to only consider the effects of fire damage to cables of equipment needed to ensure operation of credited shutdown systems. The scope of successful shutdown strategies also includes consideration of the effects of fire damage to nonessential equipment and systems of which inadvertent or spurious actuation could impact the shutdown capability.

B.3 Multiple Circuit Faults

In GL 81-12 and GL-86-10, the NRC established that either physical protection from fire (per Section III.G.2 of Appendix R), or detailed electrical circuit analyses may be used to demonstrate that fire will not cause equipment to mal-operate in a manner that could adversely affect the post-fire safe-shutdown capability of the plant. While either approach is acceptable, the use of analytical techniques places greater importance on the assumptions, criteria, and review methodology which form the basis of the analysis. Also in GL 86-10, the NRC staff defined the circuit failures to be considered. Specifically, in Question 5.3.1 the staff provided the following guidance:

> *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 (emphasis added). Therefore, valves could fail open or closed; pumps could fail running or not running; electrical distribution breakers could fail open or closed…*

In accordance with this guidance, when performing a circuit failure analysis, one or more circuit failure modes (e.g., multiple hot shorts, a hot short combined with a ground or open circuit etc.) must be considered. When considering the effects of fire damage to a multi-conductor cable, the potential for fire to cause multiple hot shorts between individual conductors must be considered. The failure to fully evaluate the potential for fire to cause more than a single fault in each circuit/cable under consideration may have potentially significant consequences on the plant's shutdown capability.

For example, the circuit analysis performed by a licensee of a BWR was found to arbitrarily limit the number of failure modes to one hot short, or one short to ground, or one open circuit on an individual device or component basis. As a result of this approach, the potential for fire to cause electrical contact between individual conductors of two twisted-pairs of conductors located within a single multiconductor cable was not considered credible by the licensee. In this case, an instrument cable contained two pairs of twisted conductors. If fire were to cause the individual conductors of the twisted pairs to short together (i.e., a short between conductors of twisted pair No. 1 and a short between conductors of twisted pair No. 2) two false high RCS pressure signals would be generated. The two high pressure signals would cause all 16 SRVs to fully open to rapidly de-pressurize the reactor. In addition, the fault current associated with these two circuit failures would not be large enough to open the protective fuse. Fire test data provided by the cable vendor showed that the wires could short in about 3 minutes when exposed to a test fire.

This page intentionally left blank.

NRC FORM **335**
(2-89)
NRCM 1102,
3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-1778

2. TITLE AND SUBTITLE

Knowledge Base for Post-Fire Safe-Shutdown Analysis

Draft Report for Comment

3. DATE REPORT PUBLISHED

MONTH	YEAR
January	2004

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

M.H. Salley

6. TYPE OF REPORT

Technical

7. PERIOD COVERED *(Inclusive Dates)*

8. PERFORMING ORGANIZATION - NAME AND ADDRESS *(If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)*

Division of Systems Safety and Analysis
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS *(If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)*

Same as above

10. SUPPLEMENTARY NOTES
S.D. Weerakkody, NRC Project Manager

11. ABSTRACT *(200 words or less)*

Every operating nuclear power plant is required to have a program that demonstrates the capability to safely shut down and maintain the reactor in the event of a fire. The U.S. Nuclear Regulatory Commission (NRC) initially issued its requirements in the Fire Protection Rule set forth in Title 10, Section 50.48, of the Code of Federal Regulations (10 CFR 50.48) and Appendix R to 10 CFR Part 50. The NRC has since issued numerous related generic communications over the past 20 years. The purpose of this document is to facilitate understanding of this technically challenging process and the regulatory framework upon which it is based by compiling all essential information in a single source. This document also lays the groundwork for future risk-informed activities in the post-fire safe-shutdown area.

12. KEY WORDS/DESCRIPTORS *(List words or phrases that will assist researchers in locating the report.)*

Circuit analysis
Post-fire safe-shutdown
Appendix R
Risk-informed approach

13. AVAILABILITY STATEMENT
unlimited

14. SECURITY CLASSIFICATION
(This Page)
unclassified
(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE