Guidance for Post-fire Safe Shutdown Analysis

Kenneth Sullivan, Steven P. Nowlen*

Department of Energy Sciences and Technology
Brookhaven National Laboratory
Upton, New York 11973-5000

* Sandia National Laboratories
Albuquerque New Mexico 87185-0747

Prepared for
U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Washington, DC 20555

PRELIMINARY DRAFT

December 2002

USNRC JCN J2844

This "Preliminary Draft" document is incomplete. In addition, the document has not been subjected to the standard BNL technical or editorial review processes. The document is being made available at the request of the NRC Technical Monitor to provide an opportunity for public comment prior to a public meeting currently scheduled to take place in February 2003.

PRELIMINARY DRAFT

Table of Contents

Guidance for Post-fire Safe Shutdown Analysis

December 2002

2. POST-FIRE SAFE SHUTDOWN TERMINOLOGY

The following definitions were developed as an aid in assuring consistent interpretations of common terms used in post-fire safe shutdown analyses. To the extent practical, definitions were derived from established fire protection guidance documents promulgated by the NRC (Regulatory Guides, Generic Letters and Information Notices) and industry recognized standards including IEEE Std 100*, "IEEE Standard Dictionary of Electrical and Electronics Terms,"* and IEEE Std. 242, *"IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems."* In an effort to further minimize ambiguity, certain terms are supplemented with additional discussion, notes, graphic illustrations and/or examples.

Actuated Equipment
The assembly of prime movers and driven equipment used to accomplish a protective action (IEEE Std 100-1988)

Actuation Device
A component or assembly of components that directly controls the motive power (electricity, compressed air, etc.) for actuated equipment. Examples of actuation devices are: a circuit breaker, a relay and a pilot valve used to control compressed air to the operator of a containment isolation valve (IEEE Std 100-1988).

Actuation
A change in position or operating state of a component. *See:* Spurious Actuation/Operation

Adverse Affect
An undesired change in the operation or functional integrity of structures, systems or components (SSC). Adverse affects may occur as a result of exposure to the effects of fire (heat or smoke) and/or fire suppression activities.

Affected Systems and Components
Structures, systems, and components (SSC) that may be adversely affected as a result of fire (including an exposure fire)or subsequent fire suppression activities in a single fire area.

Alternative Shutdown
The capability to safely shut down the reactor in the event of a fire using existing systems that have been rerouted, relocated, or modified (Regulatory Guide 1.189).

Alternative Shutdown Capability
A defined and documented process (equipment, personnel and procedures) for accomplishing safe shutdown conditions in the event of fire in areas where one train of the redundant systems (see note below) needed to achieve and maintain hot shutdown conditions has not been assured to remain free of fire damage (i.e., not provided with fire protection features sufficient to satisfy applicable requirements (Section III.G.2 of Appendix R or Position C.5.b of SRP 9.5.1).
Note: If the system is being used to provide its design function, it generally is considered redundant. If the system is being used in lieu of the preferred system because the redundant components of the preferred system do not meet the separation criteria of Section III.G.2, the system is considered an alternative shutdown capability. (GL 86-10, Q 5.8.3)

Ampacity
Current carrying capacity, expressed in amperes, of a wire or cable under stated thermal conditions (IEEE Std 100-1988)
Clarification: When current flows in a conductor, heat is produced. This happens because every conductor offers some resistance to current flowing. The National Electrical Code (NEC) defines ampacity as: *The current in amperes a conductor can carry continuously under the conditions of use without exceeding its temperature rating*. The current carrying capacity of a particular wire is dictated by its *"ampacity"* - how many amps it can handle. Ampacity is a function of the cross sectional area or diameter of the wire and its material type. Larger diameter wires have larger cross section areas and can safely carry more electrical current without overheating. The *ampacity rating* of a specific conductor may be obtained from tables in the National Electrical Code (NEC). These tables are based on the size of the wire and the particular insulation type for the particular wire. include a safety margin that is sufficient for most installations. However, there are instances where the application of the NEC ampacity tables are insufficient. For example, although the addition of fire barrier wrap around cable trays and conduits will effect the ampacity of a conductor, the NEC tables do not address this problem. Several inches of fire barrier material can have a significant effect on the ampacity rating specified in the NEC tables. Since there are no derating tables in the NEC for this kind of situation, calculations must be performed to determine the current carrying capacity of the enclosed cables.

American Wire Gauge (AWG)
A standardized system used to designate the size or “gauge” of wire. As the diameter of wire gets smaller, the “AWG” number of the wire gets larger. The smallest AWG size is 40 and looks like a metal thread. “Four ought” (0000) is the largest AWG wire size designation. Wires larger than this size are designated by the Thousand Circular Mill system or "KCMIL" sizes (known until recently as MCM).

Ampere
A standard unit of electric current flow (equal to a flow of one coulomb per second).

Any-and-All / One-at-a-Time
All potential spurious actuations that may occur as a result of fire in a single fire area must be addressed and either prevented or the effects of each actuation appropriately mitigated on a one-at-time basis. That is, in the evaluation of non-high/low pressure interface components, the analyst must assume that "any and all" spurious actuations that could occur, will occur, on a sequential, one-at-a-time, basis. Therefore, for each fire area, all potential spurious operations that may occur as a result of a postulated fire should be identified. While it is not assumed that all potential spurious actuations will occur instantaneously at the onset of fire, the analyst must consider the possibility for each spurious actuation to occur sequentially, as the fire progresses, on a one-at-a-time basis.

Appendix R Cables
The set of cables that must remain free of fire damage to ensure safe shutdown conditions can be achieved within established criteria. *Synonym:* required cables.

Arcing Fault
See: High-impedance fault.

Associated Circuits
Circuits that do not meet the separation requirements for safe shutdown systems and components but are associated with safe shutdown systems and components by common power supply, common enclosure, or the potential to cause spurious operations that could prevent or adversely affect the capability to safely shut down the reactor as a result of fire-induced failures (hot shorts, open circuits, and shorts to ground).(Regulatory Guide 1.189). 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 9.5-1. It is explicitly required in Appendix R. (SECY-80-438A, 9/30/80, Re: Commission Approval of the Final Rule on Fire Protection Program).
Clarification: An *associated circuit of concern to post-fire safe shutdown* may include any circuit or cable that is not needed to support the proper operation of required shutdown equipment (i.e., a non-essential circuit) but whose damage due to fire could adversely affect the plant's ability to achieve and maintain safe shutdown conditions. For example, while operation of the PORV in a PWR may not be needed to ensure the operation of a defined shutdown system, its maloperation due to fire damage to connected cabling could have a significant impact on the plant's overall safe shutdown capability.

Associated Circuit Analysis
A documented, systematic, evaluation of associated circuits of concern to post-fire safe shutdown.

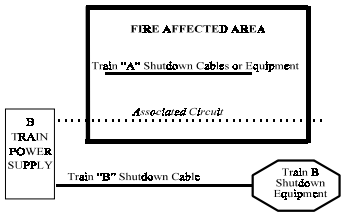
Associated Circuits of Concern

Any (associated) non-safety or safety circuits in a fire area that could adversely affect the identified shutdown equipment by feeding back potentially disabling conditions (e.g., hot shorts or shorts to ground) to power supplies or control circuits of that equipment should be evaluated. Such disabling conditions should be prevented to provide assurance that the identified safe shutdown equipment will function as designed (Regulatory Guide 1.189)

Note: Concern with associated circuits is not limited to only those circuits whose damage due to fire could adversely affect *equipment* on a required shutdown path. Rather, the concern includes all circuits within a fire area whose damage due to fire may adversely affect the post-fire safe shutdown *capability*.

Associated circuits of concern are defined as those cables (safety-related, non-safety-related Class 1E and non-Class 1E) that have a physical separation less than that specified in a through c of Regulatory Position 5.5 and have one of the following:

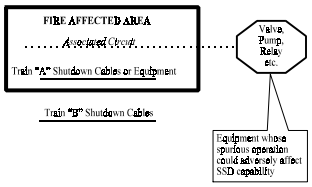
a. A *common power source* with the shutdown equipment (redundant or alternative) and the power



Associated Circuit Concern - Common Power Source

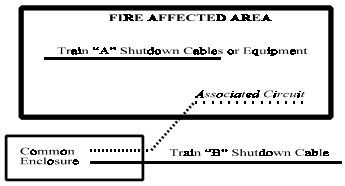
source is not electrically protected from the circuit of concern by coordinated breakers, fuses, or similar devices.

b. A connection to circuits of equipment whose *spurious operation* would adversely affect the shutdown capability (e.g., RHR/RCS isolation valves, ADS valves, PORVs, steam generator atmospheric dump valves, instrumentation, steam bypass).



Associated Circuit of Concern - Spurious Operation

c. A *common enclosure* (e.g., raceway, panel, junction box) with the shutdown cables (redundant or alternative) (1) that is not electrically protected by circuit breakers, fuses, or similar devices



Associated Circuits of Concern - Common Enclosure

or (2) will allow propagation of the fire into the common enclosure.

Automatic
Self-acting, operating by its own mechanism when actuated by some monitored parameter such as a change in current, pressure, temperature, or mechanical configuration. (Regulatory Guide 1.189)

Automatic Actuation Signal
A signal that is initiated in response to a previously defined variable or set of variables that will cause equipment to change position or operating mode. Example: the undervoltage signal that causes an emergency power source (e.g., Emergency Diesel Generator) to automatically start and load in response to a low voltage condition on safety related switchgear.

Bolted Fault
(1) A short circuit or electrical contact between two conductors at different potentials, in which the impedance or resistance between the conductors is essentially zero (IEEE Std 100-1988)
(2)A simplifying assumption used when calculating the value of short-circuit fault current to ensure that the short-circuit ratings of the equipment are adequate to handle the currents available at their locations. This assumption simplifies calculation, since the resulting calculated values are a maximum and equipment selected on this basis will always have an adequate rating. (ANSI/IEEE Std 242-1986).

Cable
A conductor with insulation or a stranded conductor with or without insulation and other coverings (single conductor cable) or a combination of conductors insulated from one another (multiple-conductor cable). (IEEE Standard 100-1988).

Cable Failure
A breakdown in the physical and/or chemical properties (e.g., electrical continuity, insulation integrity) of cable conductor(s) such that the functional integrity of the electrical circuit can not be assured (e.g., interrupted or degraded).

Cable-Fire Break
Material, devices, or an assembly of parts, installed in a cable system, other than at a cable penetration of a fire-resistive barrier, to prevent the spread of fire along the cable system. (IEEE Std. 100-1988)

Cable Jacket
A protective covering over the insulation, core, or sheath of a cable (IEEE Std.100-1988).

Cable and Raceway Database
A database unique to the plant that delineates the routing and location of cables and their associated raceways (cable trays, conduits, pull-boxes etc.).

Cable Penetration
An assembly or group of assemblies for electrical conductors to enter and continue through a fire-rated structural wall, floor, or floor-ceiling assembly. (IEEE Std. 100-1988)

Cable Routing
The pathway electrical wiring takes through the plant from power source or control point to component location.

Cable Size
See American Wire Gauge (AWG)

Cable-to-cable Fault
A fault condition of relatively low impedance between conductors of one cable and conductors of a different cable.

Circuit
(1) A conductor or system of conductors through which electrical current flows (IEEE Std100-1988).
(2) Interconnection of components to provide an electrical path between two or more components.

Circuit Analysis
A detailed, logical and systematic evaluation performed to evaluate the effects of fire-induced cable/circuit failure modes (e.g., hot shorts, open circuits, insulation degradation and shorts to ground) on the performance of plant systems and equipment and determine the impact of any ensuing mal-operations of equipment on the plant's post-fire safe shutdown capability.
Note: Performance of detailed circuit analyses is not a requirement. Section III.G of Appendix R and Regulatory Position C.5.b of SRP 9.5.1 establish fire protection design features necessary to ensure that structures, systems and components important to safe shutdown will remain free of fire damage. Where these fire protection features are provided, analysis is not necessary. When relied on in lieu of providing these features, circuit analyses must demonstrate an equivalent level of safety to that which would be achieved through compliance with applicable regulatory requirements.

Circuit Breaker
(1) A device designed to open and close a circuit by nonautomatic means, and to open the circuit automatically on a predetermined overload of current without injury to itself when properly applied within its rating. (IEEE Std 100-1988)
(2) A mechanical switching device capable of making, carrying and breaking currents under normal circuit conditions and also, making, carrying for a specified period of time, and breaking currents under specified abnormal circuit conditions such as those of short circuit.(IEEE Std 100-1988)

Circuit / Cable Fault
See: Fault, Fire-induced fault

Cold Shutdown Repair
Activities performed on equipment needed to bring the plant to cold shutdown conditions.
Note: Systems and equipment needed to achieve and maintain hot shutdown conditions must remain free of fire damage, repairs are not permitted.

Common Enclosure
An enclosure (e.g., cable tray, conduit, junction box) that contains circuits required for the operation of safe shutdown components and circuits for non-safe shutdown components (Regulatory Guide 1.189) *See:* Associated Circuits of Concern

Common-Mode Failure
Multiple failures that are attributable to a common cause. (IEEE Std. 100-1988)
Example: Circuit faults resulting from the exposure of cables to the direct effects of fire (heat, smoke) and subsequent fire suppression activities in a single fire area.

Common Power Supply/Source
A power supply that feeds safe shutdown circuits and non-safe shutdown circuits (Regulatory Guide 1.189) *See: Associated Circuits of Concern*

Conductor
(1) A substance or body that allows a current of electricity to pass continuously along it. (IEEE Std 100-1988)
(2) A wire or combination of wires, not insulated from one another, suitable for carrying an electric current (IEEE Std. 100-1988)
Clarification: For cables, the term conductor commonly refers to a single insulated wire located within a cable; For circuits, the term conductor may refer to a single wire, contact, wire termination, or other conductive pathway such as those used on printed circuit boards.

Conductor-to-Conductor Fault
(1) A circuit fault condition of relatively low impedance between two or more conductors of the same or different circuit.
(2) A cable failure mode of relatively low impedance between two or more conductors of the same multi-conductor cable (Intra-cable fault) or between two or more separate cables (Inter-cable fault).

Contact
A conducting part that co-acts with another conducting part to make or break a circuit. (IEEE Std 100-1988)

Control Cable
Cable applied at relatively low current levels or used for intermittent operation to change the operating status of a utilization device of the plant auxiliary system. (IEEE Std 100-1988)

Control Circuit
The circuit that carries the electrical signals directing the performance of the controller but does not carry the main power circuit (IEEE Std 100-1988).
Clarification: A control circuit is a low-voltage (typically 120VAC or 125VDC) circuit, consisting of switches, relays and indicating devices, which direct the operation of remotely located plant equipment that is powered from a completely separate power supply.

Control Panel
An assembly of man/machine interface devices (IEEE Std 100-1988)

Control Power/Voltage
The voltage applied to the operating mechanism of a device to actuate it. (IEEE Std 100-1988)
Clarification: Electrical power/voltage (typically 120VAC or 125VDC) used to power control circuit devices (e.g. relays, indicating lights).

Control-Power Transformer
A transformer which supplies power to motors, relays, and other devices used for control purposes (IEEE Std 100-1988).

Coordination (of Electrical Protection Devices)
Coordination is the selection and/or setting of protective devices so as to sequentially isolate only that portion of the system where the abnormality occurs. To achieve this isolation, it is necessary to set protective devices so that only the device nearest the fault opens and isolates the faulted circuit from the system. It is obvious that such selectivity becomes more important with devices that are closer to the power source, as a greater portion of the system can be affected. Backup protective devices are set to operate at some predetermined time interval after the primary device fails to operate. A backup device is able to withstand the fault conditions for a longer period than the primary device. If a primary device fails to clear a fault and the backup device must clear it, then the design of the protective system becomes suspect. To optimize the coordination of protective devices, good engineering practice requires that consideration be given to the following: (1) available maximum short circuit currents; (2) time interval between the coordination curves; and (3) load current. (IN 88-45)
Clarification: It must be ensured that electrical fault currents generated as a result of fire damage will not cause an interruption in the power being supplied to required shutdown equipment. To insure this "continuity of service" cables and equipment fed from electrical power sources required for post-fire safe shutdown must either be provided with suitable fire protection features (e.g. meet III.G.2 of Appendix R) or the fault-protection devices (relays, fuses and/or circuit breakers) of the required power sources must be selectively coordinated. *See also:* High Impedance Fault

Coordination Study
The process of evaluating the performance of electrical distribution system protection devices (breakers, fuses, relays) to ensure fault conditions caused by fire will be isolated and power outages to unaffected equipment will be minimized. A coordination study is based on a comparison of the time it takes individual overcurrent protection devices (circuit breakers, fuses, relays) to operate (trip) under abnormal (faulted) conditions. For post-fire safe shutdown, this study must ensure that electrical power to shutdown equipment will not be interrupted as a result of fire-induced faults in non-essential loads (equipment or cables) of a required power supply (Switchgear, Load Center, MCC, fuse panel, etc.).

ANSI/IEEE Standard 242-1986, "IEEE Recommended Practices for Protection and Coordination of Industrial and Commercial Power Systems" provides detailed guidance on achieving proper co-ordination. (Regulatory Guide 1.189, IN 88-45)

Credited Shutdown Equipment
The set of equipment that is relied on (credited in the SSA) for achieving post-fire safe shutdown conditions in the event of fire in a specific fire area.

Current Carrying Capacity
See *ampacity*

Current Licensing Basis (CLB)
The set of NRC requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect. The CLB includes the NRC regulations contained in 10 CFR Parts 2, 19, 20, 21, 26, 30, 40, 50, 51, 54, 55, 70, 72, 73, 100 and appendices thereto; orders; license conditions; exemptions; and technical specifications. It also includes the plant-specific design-basis information defined in 10 CFR 50.2 as documented in the most recent final safety analysis report (FSAR) as required by 10 CFR 50.71 and the licensee's commitments remaining in effect that were made in docketed licensing correspondence such as licensee responses to NRC bulletins, generic letters, and enforcement actions, as well as licensee commitments documented in NRC safety evaluations or licensee event reports. (10 CFR 54.3) *See also:* Regulatory Guide 1.189

Current Transformer
A device used to transform high currents used by a large equipment and switchgear to lower levels that can safely be measured by standard metering equipment. The current reduction ratio of a CT is given on their nameplate. A CT with a current reduction ratio of 400:5 would reduce the current by a ratio of 400 divided by 5 or 80 times.
Note: The hazard of electric shock, burn, or explosion exists on an open-circuited CT. Death, severe personal injury, or equipment damage can result if the leads are touched when the CT is open-circuited. As much as 4000V on the secondary has been measured on large core CTs with an open-circuited secondary. CTs must *always* be shorted *or* connected to a burden such as a meter or relay. Open-circuiting may also damage the CT insulation. Once a CT has been open-circuited, it must be demagnetized or accuracy may be reduced. (Square D Application Bulletin No. 4200PD9203R8/95, April 1996)

Dedicated Shutdown
The ability to shut down the reactor and maintain shutdown conditions using structures, systems, or components dedicated to the purpose of accomplishing post-fire safe shutdown functions (Regulatory Guide 1.189).

Diagnostic Instrumentation
Instrumentation beyond that previously identified in Attachment 1 to I&E Information Notice 84-09, needed to assure proper actuation and functioning of safe shutdown equipment and support equipment (e.g., flow rate, pump discharge pressure). The diagnostic instrumentation needed depends on the design of the alternative shutdown capability. (GL 86-10, Q. 5.3.9).
Clarification: Section IX of IN 84-09 establishes the minium set of instrumentation deemed acceptable to the NRC staff for meeting the *Alternative Shutdown* process monitoring function. Although diagnostic instrumentation is included in this list, it is not specifically defined. Alternative Shutdown strategies that rely on operator intervention (manual operator recovery actions) to mitigate equipment mal-operations and/or failures that may occur as a result of fire, must be supported by sufficient monitoring capability (diagnostic instrumentation) to assure prompt detection of those failure(s) that may occur and confirm proper system response.

Emergency Control Station
The control stations located outside the main control room where actions are taken by operations personnel to manipulate plant systems and their controls to achieve safe shutdown of the reactor.

Enclosure
An identifiable housing such as a cubicle, compartment, terminal box, panel or raceway used for electrical equipment or cables (IEEE Std 100-1988)

Exposed (Cables/Circuits/Equipment/Structures)
(1) Structures, systems and components (SSC), that are subject to the effects of fire and/or fire suppression activities.
(2) SSC not provided with fire protection features sufficient to satisfy Section III.G.2 of Appendix R or Position C.5.b of SRP 9.5.1.

Exposure Fire
A fire in a given area that involves either in situ or transient combustibles and is external to any structures, systems, and components located in or adjacent to that same area. The effects of such fire (e.g., smoke, heat, or ignition) can adversely affect those structures, systems, and components important to safety. Thus, a fire involving one success path of safe shutdown equipment may constitute an exposure fire for the redundant success path located in the same area, and a fire involving combustibles other than either redundant success path may constitute an exposure fire to both redundant trains located in the same area. (Regulatory Guide 1.189)

Failsafe Circuits
Circuits designed in such a way that fire-induced faults will result in logic actuation(s) to a desired, safe, mode which can not be overridden by any subsequent circuit failures.

Fire Area
The portion of a building or plant that is separated from other areas by rated fire barriers adequate for the fire hazard (Regulatory Guide 1.189).

Fire Area Boundaries
The term "fire area" as used in Appendix R means an area sufficiently bounded to withstand the hazards associated with the area and, as necessary, to protect important equipment within the area from a fire outside the area. In order to meet the regulation, fire area boundaries need not be completely sealed floor-to-ceiling, wall-to-wall boundaries. However, all unsealed openings should be identified and considered the evaluating the effectiveness of the overall barrier. Where fire area boundaries are not wall-to-wall, floor-to-ceiling boundaries with all penetrations sealed to the fire rating required of the boundaries, licensees must perform an evaluation to assess the adequacy of fire boundaries in their plants to determine if the boundaries will withstand the hazards associated with the area. This analysis must be performed by at least a fire protection engineer and, if required, a systems engineer. (GL 86-10)

Fault
(1) Any undesired state of a component or system. A fault does not necessarily require failure (for example, a pump may not start when required because its feeder breaker was inadvertently left open (IEEE Std 100-1988)
(2) A partial or total local failure in the insulation or continuity of a conductor (IEEE Std 100-1988)
(3) A physical condition that causes a device, a component or an element to fail to perform in a required manner, for example a short-circuit, a broken wire, an intermittent connection (IEEE Std.100-1988)

Fault Current
(1) A current that flows from one conductor to ground or another conductor owing to an abnormal connection (including an arc) between the two. (IEEE Std 100-1988)
(2) A current that results from the loss of insulation between conductors or between a conductor and ground (NEMA Std. ICS-1, 1988)
Clarification: Fault current is an abnormal level of current that is induced in an electrical circuit. Fault currents may be initiated by various mechanisms including insulation degradation, arcing or physical contact between two conductors. Fault currents include short circuit current (bolted fault), high-impedance (arcing) fault currents, and overload currents.

Feeder Breaker / Fuse
A general term used to describe a circuit breaker or fuse located upstream of an electrical load. Depending on usage, it may refer to a circuit breaker provided for a specific component (load breaker) or it may refer to a breaker located upstream of a switchgear, load center or distribution panel. Opening a feeder breaker will cause a loss of power to all downstream loads.

Fire-induced Fault
An electrical failure mode (e.g., hot short, open circuit, or short to ground) that may result from circuit/cable exposure to the effects of fire (e.g., heat and smoke) and/or subsequent fire suppression activities (e.g., water spray, hose streams).

Fire Suppression
Control and extinguishing of fires (firefighting). Manual fire suppression employs the use of hoses, portable extinguishers, or manually actuated fixed systems by plant personnel. Automatic fire suppression is the use of automatically actuated fixed systems such as water, Halon, or carbon dioxide systems. (Regulatory Guide 1.189)

Fire Suppression Impacts
The susceptibility of structures, systems and components and operations response to suppressant damage (due to discharge or rupture) (NFPA 805)

Fire Zones
Subdivisions of fire areas (Regulatory Guide 1.189)
Note: Compliance with Section III.G.2 cannot be based on rooms or zones. (GL 86-10, Q 3.1.5)

Free of Fire Damage
In promulgating Appendix R, the Commission has provided methods acceptable for assuring that necessary structures, systems and components are free of fire damage (see Section III.G.2a, b and c), that is, the structure, system or component under consideration is capable of performing its intended function during and after the postulated fire, as needed. Licensees seeking exemptions from Section III.G.2 must show that the alternative proposed provides reasonable assurance that this criterion is met. The term "damage by fire" also includes damage to equipment from the normal or inadvertent operation of fire suppression systems. (Generic Letter 86-10)
Note: Section III.G.2 of Appendix R and Position C.5.b of SRP 9.5.1 establish fire protection features necessary to ensure that systems needed to achieve and maintain hot shutdown conditions remain free of fire damage.

Fuse
(1) A device that protects a circuit by fusing open its current responsive element when an overcurrent or short-circuit current passes through it. (IEEE Std. 100-1988)
(2) A protective device that opens by the melting of a current-sensitive element during specified overcurrent conditions (NEMA Std. FU-1 1986)

Fuse Current Rating
The ac or dc ampere rating which the fuse is capable of carrying continuously under specified conditions. (NEMA Std. FU-1 1986)

Fuse Voltage Rating
The maximum rms ac voltage or the maximum dc voltage at which the fuse is designed to operate.. (NEMA Std. FU-1 1986)

Ground
A conducting connection, whether intentional or accidental, by which an electric circuit or equipment is connected to the earth, or to some conducting body of relatively large extent that serves in place of the earth (IEEE Std. 100-1988).

Grounded Circuit
A circuit in which one conductor or point (usually the neutral conductor or neutral point of transformer or generator windings) is intentionally grounded, either solidly or through a non-interrupting current limiting grounding device (IEEE Std.100-1988).

High / Low Pressure Interface
Reactor coolant boundary valves whose spurious operation due to fire could: (a) potentially rupture downstream piping on an interfacing system, or (b) result in a loss of reactor coolant inventory in excess of the available makeup capability.

High-impedance Fault
(1) An electrical fault of a value that is below the trip point of the breaker on each individual circuit (GL 86-10, Q5.3.8).
(2) A circuit fault condition resulting in a short to ground, or conductor to conductor hot short, where residual resistance in the faulted connection maintains the fault current level below the component's circuit breaker long-term setpoint. (Regulatory Guide 1.189)
Clarification: High-impedance faults (HIF) are typically initiated by damaged or degraded insulation and are characterized by low and erratic current flow. Unlike a short circuit (bolted fault), a high-impedance fault has an element of resistance between the affected power conductor and its return path (typically ground). This resistance serves to limit the value of fault current. Due to these characteristics, HIFs may continue undetected by conventional circuit protective devices. Should a sufficient number of these faults occur, the summation of fault currents may be sufficient to cause a trip of the upstream feeder breaker, resulting a loss of power to required shutdown loads connected to the affected power source. With regard to the analysis of their potential impact on post-fire safe shutdown capability, high-impedance faults should be postulated to occur simultaneously on all exposed cables located in the fire area and should be assumed to be of a magnitude that is just below the long-term trip point setting of the individual load breaker.

Hot Short
Individual conductors of the same or different cables come in contact with each other and may result in an impressed voltage or current on the circuit being analyzed. (Regulatory Guide 1.189)
Clarification: The term "hot short" is used to describe a specific type of short circuit fault condition between energized and de-energized conductors. Should a de-energized conductor come in electrical contact with an energized conductor (or other external source), the voltage, current or signal being carried by the energized conductor(or source) would be impressed onto one or more of the de-energized conductors.

Important to Safety
Nuclear power plant structures, systems, and components "important to safety" are those required to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public. (Regulatory Guide 1.189)

Instrument Sensing Line
Small diameter tubing (usually stainless steel but may be copper) used to interconnect plant process instrumentation.

Inter-cable fault
A fault between conductors of two or more separate cables.

Intra-cable fault
A fault between two or more conductors within a single multi-conductor cable.

Interlock
A device actuated by the operation of some other device with which it is directly associated to govern succeeding operations of the same or allied devices.
Note: Interlocks may be either electrical or mechanical (IEEE Std.100-1988).

Interrupting Device
A breaker, fuse, or similar device installed in an electrical circuit to isolate the circuit (or a portion of the circuit) from the remainder of the system in the event of an overcurrent or fault downstream of the interrupting device. (Regulatory Guide 1.189)

Isolating Device /Isolation Device
A device in a circuit which prevents malfunctions in one section of the circuit from causing unacceptable influences in other sections of the circuit or other circuits (IEEE Std. 100-1988; Regulatory Guide 1.189).

Isolation Transfer Switch
A device used to provide electrical isolation from the fire affected area and transfer control of equipment from the main control room to the local control station (alternate shutdown panel).

Insulated Conductor
A conductor covered with a dielectric(other than air) having a rated insulating strength equal to or greater than the voltage of the circuit in which it is used. (IEEE Std. 100-1988).

Insulation (Cable, Conductor)
That which is relied on to insulate the conductor or other conductors or conducting parts from ground. (IEEE Std. 100-1988)

Leakage Current (Insulation)
The current that flows through or across the surface of insulation and defines the insulation resistance at the specified direct current potential (IEEE Std. 100-1988).

Local Control
Operation of shutdown equipment using remote controls (e.g., control switches) specifically designed for this purpose from a location other than the main control room. Example: Operating the Emergency Diesel Generator from controls provided at the remote/alternate shutdown panel.

Local Control Station
A control panel located in the plant which allows operation and monitoring of plant equipment from outside of the main control room. For post-fire safe shutdown control functions and monitoring variables on these panels must be independent (physically and electrically)from those in the main control room.

Local Operation
Manipulation of plant equipment from a location outside of the main control room. For example, manual operation of the circuit breakers or turning the handwheel on the valve to change its position.

Load Breaker

A circuit breaker that is located on the load side of a power source. Synonym: branch breaker.

Mal-operation
The inability of a component to operate as desired or expected.

Manual Action
Physical manipulation (operation) of equipment when local or remote controls are no longer available of a plant component such as a valve, switch or circuit breaker.

Manual Valve
A valve that does not have the capability of being manipulated remotely.

Manually Operated Valve
Term used to denote a valve credited in the SSA or shutdown procedures for being manually manipulated.
Note: A manually operated valve may be a manual valve or a remotely operated valve (e.g., MOV) that has its power and control capability disabled or removed.

Molded-Case Circuit Breaker
A circuit breaker that is assembled as an integral unit in a supporting and enclosing housing of molded insulating material. (IEEE Std. 100-1988)

Multi-conductor Cable (Multiple Conductor Cable)
A combination of two or more conductors cabled together and insulated from one another and from sheath or armor where used.
Note: Specific cables are referred to as 3-conductor cable, 7-conductor cable, 50-conductor cable, etc. (IEEE Std 100-1988).

Non-essential (Conductor, Cable, Component or System)
Structures, systems, and components (Class 1E, Non-Class 1E, safety related or non-safety related) whose operation is not required to support the performance of systems credited in the SSA for accomplishing post-fire safe shutdown functions.

Normally Closed or Normally Open
The component status during normal operating modes of the plant. This terminology is usually applied to valve, circuit breaker, and relay operating positions.

Open Circuit:
A failure condition that results when a circuit (either a cable or individual conductor within a cable) loses electrical continuity. (Regulatory Guide 1.189)
Clarification: A circuit fault condition where the electrical path has been interrupted or "opened" at some point so that current will not flow. Open circuits may be caused by a loss of conductor integrity due to heat or physical damage (break).

Overcurrent
Any current in excess of the rated current of equipment or the rated ampacity of a conductor. It may result from overload, short-circuit, or ground-fault. A current in excess of rating may be accommodated certain equipment and conductors for a given set of conditions. Hence, the rules for overcurrent protection are specific for particular situations (IEEE Std. 100-1988).

Overcurrent Protection
A form of protection that operates when current exceeds a predetermined value. (IEEE Std. 100-1988)

Overcurrent Relay
A relay that operates when its input current exceeds a predetermined value. (IEEE Std. 100-1988)

Overload:
(1) Loading in excess of normal rating of equipment (IEEE Std 100-1988).
(2) Generally used in reference to an overcurrent that is not of sufficient magnitude to be termed a short circuit. (IEEE Std. 100-1988).
Clarification: An overload is a circuit fault condition that occurs when the amount of current flowing through the circuit (cable, wire) exceeds the rating of the protective devices (fuse, circuit breaker etc.). Without proper overload protection wires can get hot, or even melt the insulation and start a fire. Overloads are most often between one and six times the normal current level. Usually, they are caused by harmless temporary surge currents that occur when motors are started-up or transformers are energized. Such overload currents, or transients, are normal occurrences. Since they are of brief duration, any temperature rise is trivial and has no harmful effect on the circuit components. (It is important that protective devices do not react to them.) A sustained overload current results in over-heating of conductors and other components and will cause deterioration of insulation, which may eventually result in severe damage and short-circuits if not interrupted.

Paired Cable
A cable in which all the conductors are arranged in the form of twisted pairs (IEEE Std. 100-1988).

Potential Transformer
A special class of transformer used to step down high distribution system level voltages (typically 480V and above) to a level that can be safely measured by standard metering equipment. PT's have a voltage reduction ratio given on their nameplate. A PT with a voltage reduction ratio of 200: 5 would reduce the voltage by a ratio of 200 divided by 5 or 40 times.

Power Cable/Circuit
A circuit used to carry electricity that operates a load.

Pre-fire Position/Operating Mode
Terminology used to indicate equipment status prior to a fire.

Protective Relay
A device whose function is to detect defective lines or apparatus or other power system conditions of an abnormal or dangerous nature and to initiate appropriate control action. A protective relay may be classified according to its input quantities, operating principal, or performance characteristics. (IPEEE Std. 100-1988)
Clarification: Protective relays are small, fast acting, automatic switches designed to protect an electrical system from faults and overloads. A single 4160V switchgear have many relays, each with a specific purpose. Protective relays are classified by the variable they monitor or the function they perform. When a relay senses a problem (e.g., short circuit) it quickly sends a signal to one or many circuit breakers to open, or trip, thus protecting the remainder of distribution system.

Raceway
An enclosed channel of metal or nonmetallic materials designed expressly for holding wires, cables, or busbars, with additional functions as permitted by code. Raceways include, but are not limited to, rigid metal conduit, rigid nonmetallic conduit, intermediate metal conduit, liquid-tight flexible conduit, flexible metallic tubing, flexible metal conduit, electrical nonmetallic tubing, electrical metallic tubing, underfloor raceways, cellular concrete floor raceways, cellular metal floor raceways, surface raceways, wireways, and busways.(Regulatory Guide 1.189; IEEE Std 100-1988)

Rated Voltage
(1) The voltage at which operating and performance characteristics of apparatus and equipment are referred. (IEEE Std. 100-1988)
(2) For cables, either single-conductor or multiple conductor, the rated voltage is expressed in terms of phase-to-phase voltage of a three phase system. For single phase systems, a rated voltage of / 3 * the voltage to ground should be assumed. (IEEE Std. 100-1988)

Redundant Shutdown
(1) If the system is being used to provide its design function, it generally is considered redundant. If the system is being used in lieu of the preferred system because the redundant components of the preferred system do not meet the separation criteria of Section III.G.2, the system is considered an alternative shutdown capability. (GL 86-10, Q 5.8.3)
(2) For the purpose of analysis to Section III.G.2 criteria, the safe shutdown capability is defined as one of the two normal safe shutdown trains. If the criteria of Section III.G.2 are not met, an alternative shutdown capability is required. (GL 86-10, Q 5.1.2)
Note: For BWRs, the use of safety relief valves and low pressure injection systems has been found to meet the requirements of a redundant means of post-fire safe shutdown under Section III.G.2 of 10 CFR 50, Appendix R (Letter from: S. Richards, NRC, To: J. Kenny, BWR Owners Group, 12/12/2000).

Relay
An electrically controlled, usually two-state, device that opens and closes electrical contacts to effect the operation of other devices in the same or another electric circuit (IEEE Std. 100-1988).

Remote Control
(1) Control of an operation from a distance: this involves a link, usually electrical, between the control device and the apparatus to be operated (IEEE Std. 100-1988).
Note: Remote control may be accomplished from the control room or local control stations.

Remote Shutdown Location
A plant location external to the main control room that is used to manipulate or monitor plant equipment during the safe shutdown process. Examples include the remote shutdown panel or valves requiring manual operation.

Remote Shutdown Panel
Depending on usage the term *Remote Shutdown Panel* (RSP) may refer to control and monitoring stations (panels) having significantly different design capabilities. For example, RSP may refer to:
(1) The control panel included in the plant design for the purpose of satisfying GDC 19 (shutdown due to loss of control room habitability).
Note: The controls and instruments on this panel are not necessarily isolated from the effects of fire. For GDC 19, damage to the control room is not considered.
(2)The control panel included in the plant design for the purpose of controlling and monitoring alternative shutdown functions from outside the main control room.
Note: Alternate shutdown systems need not be redundant but must be both physically and electrically independent of the control room. (GL 86-10 Q 5.3.11)

Repair
To restore by replacing a part or putting together what is broken. (Webster's Ninth New Collegiate Dictionary)
Clarification: In general, any manual action involving: (a) the use of a tool (screwdriver, pliers, wrench, etc.), (b) the installation of components (e.g., fuse, electrical/pneumatic jumpers), or a modification of plant SSC is considered a repair. Such repairs are only permitted on equipment needed to achieve and maintain cold shutdown conditions. *Notes:* (1) appropriately controlled equipment provided to facilitate the implementation of procedurally directed operator actions such as ladders, flashlights, fuse pullers, extension bars/handles are not considered tools. (2) the removal of fuses (fuse pulling) is generally not considered a repair. However, this determination must be made on a case-by-case basis that considers such factors as feasibility, time, adequacy of emergency lighting, potential for human error and personnel safety hazards.

Required Circuits and Cables
Cables and circuits needed to support operation or prevent the mal-operation of components identified on the safe shutdown equipment list for a particular fire area. In general, a circuit (cable) is considered to be *required* for safe shutdown if it is needed to assure the operation of required equipment and fire-induced faults in the circuit (cable) can cause the required component(s) to fail and/or mal-operate in an undesired condition for safe shutdown. In the absence of a specific exemption/deviation, required cables and circuits must be provided with fire safety features specified in applicable requirements (Section III.G.2 of Appendix R or Position C.5.b of SRP 9.5.1) or circuit analysis must demonstrate an equivalent level of safety to that which would be achieved through compliance with these requirements (i.e., no credible combination of circuit faults resulting from fire and/or fire suppression activities will cause equipment to operate in an undesired manner).
See Section 6
Note: Required equipment designations may be found to vary between fire areas (e.g. a cable may be required for shutdown in the event of fire in one area but not required in another).

Required Equipment List
See *Safe Shutdown Equipment List*

Required Shutdown Equipment/Components
Equipment needed to ensure the capability to achieve and maintain post-fire safe shutdown conditions may be accomplished within established criteria.

Required Shutdown System
The systems credited in the SSA for performing each nuclear safety function.

Resistance
Opposition of the flow of electricity through a material.
Clarification: A number of factors determine the resistance to current flow such as wire diameter, wire length and any impurities in the wire's makeup. In general, smaller wires have more resistance than larger diameter wires and longer wires have more resistance than shorter wires. When electricity flows through any resistance, energy is dissipated in the form of heat.

Safe Shutdown Analysis (Post-fire Safe Shutdown Analysis)
A documented evaluation of the potential effects of a postulated fire (including an exposure fire) and fire suppression activities in any single area of the plant (fire area), on the ability to achieve and maintain safe shutdown conditions in a manner that is consistent with established performance goals and safety objectives. (i.e., Sections III.G and III.L of Appendix R or Position C.5.b of SRP 9.5.1).

Safe Shutdown Equipment List
A documented list of equipment and components that must operate or be prevented from mal-operating to ensure the capability to achieve and maintain post-fire safe shutdown conditions may be accomplished within established criteria. *Synonym:* Required Equipment List

Safe Shutdown System
All structures, equipment (components, cables, raceways cable enclosures etc.), and supporting systems (HVAC, electrical distribution, station and instrument air, cooling water, etc.) needed to perform a shutdown function.

Selectivity
A general term describing the interrelated performance of relays and breakers, and other protective devices; complete selectivity being obtained when a minimum amount of equipment is removed from service for isolation of a fault or other abnormality (IEEE Std 100-1988) See also: *Coordination*.

Short Circuit:
An abnormal connection (including an arc) of relatively low impedance, whether made accidentally or intentionally, between two points of different potential. (IEEE Std 100-1988).

Short Circuit Current (I_{sc})
Current that flows outside the normal conducting paths (e.g., conductor to ground).
Note: Unlike *high-impedance faults*, this fault current is generally very large since only the combined impedance of the object responsible for the short, the wire, and the transformer limit its magnitude. Short-circuit current is often two orders of magnitude greater than normal operating current. The symbol I_{sc} is frequently used to represent the value/magnitude of current flowing during a short circuit fault condition.

Short to Ground
A short circuit between conductor(s) and a grounded reference point (e.g., grounded conductor, conduit, raceway, metal enclosure, shield wrap or drain wire within a cable).

Solid Conductor
A conductor consisting of a single wire. (IPEEE Std.100-1988)

Spurious Actuation/Operation
A change (full or partial) in the operating mode or position of equipment. These operations include but are not limited to: (a) opening or closing normally closed or open valves, (b) starting or stopping of pumps or motors, (c) actuation of logic circuits, (d) inaccurate instrument reading.

Spurious Indications
False indications (process monitoring, control, annunciator, alarm, etc.) that may occur as a result of fire and fire suppression activities.

Spurious Signals
False control or instrument signals that may be initiated as a result of fire and fire suppression activities.

Stranded Conductor
A conductor made from number of smaller wire strands wrapped around each other.

Sub-component
Components that are required to ensure the proper control and/or operation of main flowpath components (e.g., pumps, flowpath valves) and components such as flow switches, temperature switches, relays, transmitters, signal conditioners which provide isolation or actuation signals to main components.

Tenability
The effects of smoke and heat on personnel actions. (NFPA 805)

Thermal/Hydraulic Timeline
A documented evaluation of the response of important reactor plant parameters to a postulated transient (thermal/hydraulic analysis) with respect to the time available to accomplish required shutdown functions. For example, the time available to establish Auxiliary Feedwater (AFW) following a reactor scram in a PWR would be determined by a thermal/hydraulic analysis. The objective of the thermal/hydraulic timeline is to compare this time to the time needed for operators to perform all system and equipment alignments necessary to establish a secure source of AFW..
Note: All operator actions delineated in alternative shutdown procedures must be supported by a thermal/hydraulic timeline. In this manner, the time available for operator actions may be verified for consistency with the plant-specific design.

Thermoplastic
A cable material which will soften, flow, or distort appreciably when subjected to sufficient heat and pressure. Examples are polyvinyl chloride and polyethylene.

Note: Cables using thermoplastic insulation are not usually qualified to IEEE Std. 383 and have a failure temperature of 425° F.

Thermoset
A cable material which will not soften, flow, or distort appreciably when subjected to heat and pressure. Examples are rubber and neoprene.

Note: Cables that meet IEEE Std.383 typically have *thermoset* insulation. Thermoset cables have a failure temperature of 700° F

Time/Current Characteristic Curve (Trip Curves)
A graphic illustration of the operating characteristics of electrical protection devices (fuse, circuit breaker, or relay). The tripping characteristics of protective devices is represented by a characteristic tripping curve that plots tripping time versus current level. The curve shows the amount of time required for the protective device to trip at a given overcurrent level. The larger the overload or fault current, the faster the breaker/fuse will operate to clear the circuit (referred to as inverse time characteristics). A comparison of characteristic trip curves is necessary to determine if proper coordination exists between devices.

Triplex Cable
A cable composed of three insulated single conductor cables twisted together. (IEEE Std 100-1988)
Note: AC power cables are commonly of triplex design.

Unprotected Cable/Circuit
A cable/circuit which is not provided with fire protection features sufficient to satisfy applicable requirements (Section III.G.2 of Appendix R or Position C.5.b of SRP 9.5.1).

Voltage
(1) The effective root-mean-square (rms) potential between any two conductors or between a conductor and ground. Voltages are expressed in nominal values unless otherwise indicated. (IEEE Std 100-1988)
Clarification: The electrical force that causes free electrons to move from one atom to another. Similar to pressure in a water pipe.

3. FIRE-INDUCED CIRCUIT FAILURES

3.1 Background

As with any large industrial complex, a nuclear power plant (NPP) contains an extensive array of systems and components; and nearly all of this equipment is directly or indirectly dependent on the continuous operation of one or more electrical cables and circuits. A typical boiling water reactor (BWR) requires approximately 60 miles of power cable, 50 miles of control cable and 250 miles of instrument cable. Almost 1000 miles of cable went into the containment building of Waterford III, a pressurized water reactor (PWR).[1] Because of their large quantity and the fact that much of the cable material is combustible (e.g., polymer insulation and outer jacket), cables are frequently a significant fraction of the total combustible FIRE loading in many areas of a plant.

As evidenced by the fire at Browns Ferry in 1975, electrical circuit failures resulting from fire damaged cables can have a major impact on SAFE plant operations. Although the fire was contained to a relatively small interior area of the plant, temperatures as high as 1500°F caused damage to more than 1600 cables routed in 117 conduits and 26 cable trays. As described below, fire-induced circuit failures resulting from damage to these cables caused equipment to operate in unexpected ways and significantly impeded the operator's ability to monitor and control reactor safety functions.

3.2 Circuit and Cable Primer

An electrical *circuit* is analogous to a circular path that electrons flow through. In the circuit illustrated in Figure 3.1, the flow path is from the negative terminal of the battery through the load

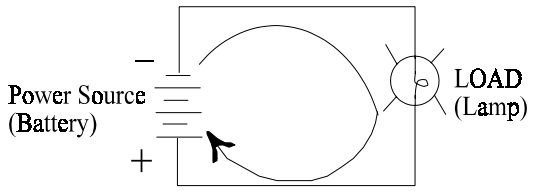


Figure 3.1 - Circuit Illustration

[1] NUREG/CR-6384, BNL-NUREG-52480, "Literature Review of Environmental Qualification of Safety Related Electric Cables," Vol.1, April 1996

(lamp) and back to the positive terminal of the battery. In more complex circuits many paths may split off to various components but they always form a line from one side (polarity) of the power source and return to the opposite side (polarity) of the power source.

For small, simple, circuits such as the one illustrated in Figure 3.1, the electrical path between components could be established by short lengths of individual wire *conductors*. In a large installation such as a nuclear power plant, however, the circuit components may be located great distances from each other. For example, the power source in the above illustration may be a fuse panel that is located in the service water intake structure while the load is a pump status indicator lamp located in the control room. For applications such as this, long lengths of *cable* containing one or more insulated wires or *conductors* are needed to establish the path for current to flow (i.e., complete the circuit). In a complex facility such as a power plant, many cables of various types, construction and size are needed to distribute electric power, control signals, and process system information. As depicted in Figure 3.2 below, these cables are are generally classified by the function they perform:

- *Power Cables :* distribute electric power from power supplies (switchgear, MCCs, panel boards) to utilization equipment. Within the plant, power cables are classified by the level of voltage they carry. Medium voltage power cables (4.16 kV, 6.9 kV) distribute power to auxiliary transformers, electrical switchgear, and large motors. Low voltage power cables (<1000 Volts) supply power to Motor Control Centers, motor-operated valves, pumps, and motors.
- *Control Power Cables:* Provide electrical power (typically 125V dc or 120V ac) to control circuits and components such as switches and relays.
- *Control Cables:* Provide remote control capability of a component or a permissive/interlock signal.
- *Instrument Cables:* Transmit low-level signals from the instrument sensor to an indicator, controller, or recorder.

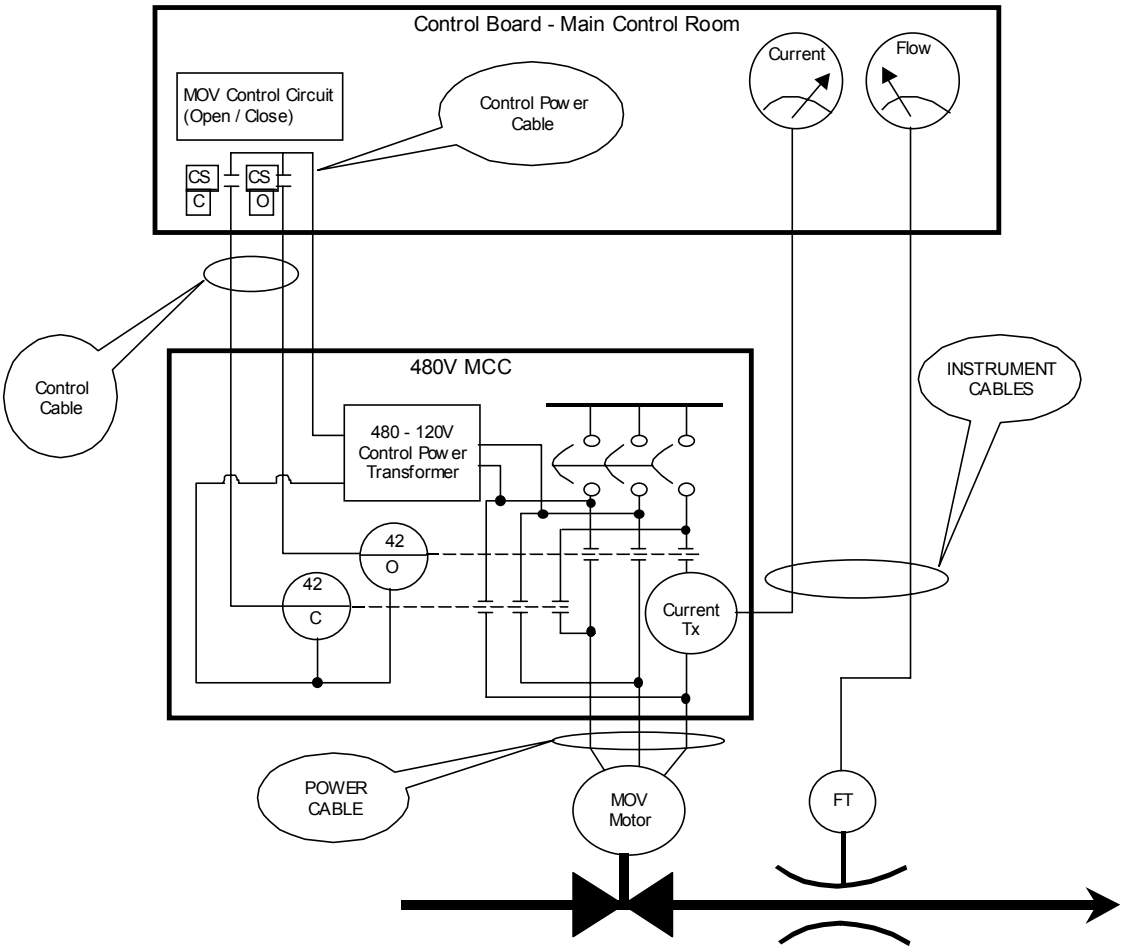


Figure 3.2 - General Cable Classifications

3.2.1 Cable Construction and Materials

As illustrated in Figure 3.3 below, most cables used in a nuclear power plant are comprised of three parts: a metallic conductor, insulation and a protective polymer jacket.

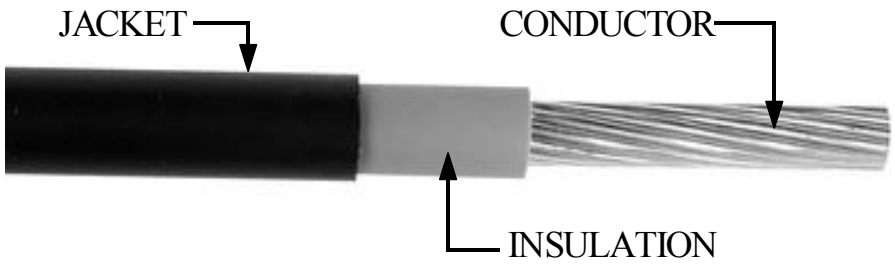


Figure 3.3 - Cable Components

The *conductor* provides a low resistance path for electrical voltage or signals. Copper and aluminum are popular conductor materials and may be either solid or stranded. As its name implies, a solid conductor is a single length of wire, whereas a stranded conductor is made by twisting individual strands of wire around each other until the desired conductor diameter or "gauge" is achieved. The conductor shown above in Figure 3.3 is a stranded conductor. While there is little difference in their electrical capabilities, stranded conductors are far more flexible than solid conductors of the same gauge, making them easier to install. The majority of cables found in plants contain stranded copper conductors. A cable may contain a single conductor (Fig. 3.3), or a large number of conductors. A cable containing more than one conductor is called a *"multi-conductor cable*" A cross sectional view of a 7-conductor cable is illustrated below in Figure 3.4.

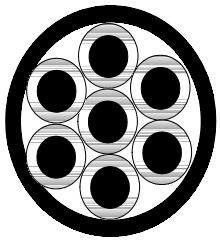


Figure 3.4 Multi-conductor Cable

Insulation isolates the conductor from unwanted paths of current flow (e.g., grounded conduit or cable tray, other conductors, and personnel). Many different types of insulation material are available to accommodate the specific application, environment and service conditions of the cable. In most nuclear power applications cables are insulated with either *thermoset* or *thermoplastic* materials. *Thermoplastic* materials are made from compounds that will re-soften and distort from their formed shapes by heating above a critical temperature peculiar to the material. Polyvinyl Chloride (PVC) is a thermoplastic compound. *Thermoset* insulation and jacket compounds will not re-soften or distort from their formed shapes by heating until a destructive temperature is reached. Insulation and cable outer jackets made from cross-linked polyethylene (XLPE), chlorosulfonated polyethylene (CSPE - commonly called Hypalon), and Neoprene are examples of thermoset materials. IPEEE 383 qualified cables have thermoset insulation and havea failure temperature of 700°F. Non-IPEEE-383 qualified cables are typically thermoplastic and have a a failure temperature of 425°F.
The *voltage rating* of a cable is the highest voltage that may be continuously applied and is generally a function of the type and amount (thickness) of insulation used. Cables used in low voltage applications (#600V) are generally rated at 600 Volts regardless of their actual application voltage. Cables in this range include instrument circuits (50 volts or less), control and control power circuits (120-250 volt range) and certain power circuit applications (120, 480 and 600 volts). Single conductor and multi-conductor cables used in medium voltage applications (e.g., 4160V) are available with nominal voltage ratings of 5, 8, 15, 25 and and 35 kV.

Cable jacket, and armor. The *jacket* is usually a plastic cover provided to protect the cable from mechanical damage and chemical attack during installation and over its service life. Some of the more common jacket materials are polyvinyl chloride (PVC), Neoprene and Hypalon. The jacket does not perform any electrical function. Where a high degree of physical protection is desired, cables may be furnished with a metallic outer sheath made from interlocked aluminum or steel. Cables of this type are called *armored cables*. An example of an armored power cable is shown in

Figure 3.5 below. Armoring protects the cable from penetration by sharp objects, crushing forces, and damage from gnawing animals or boring insects.

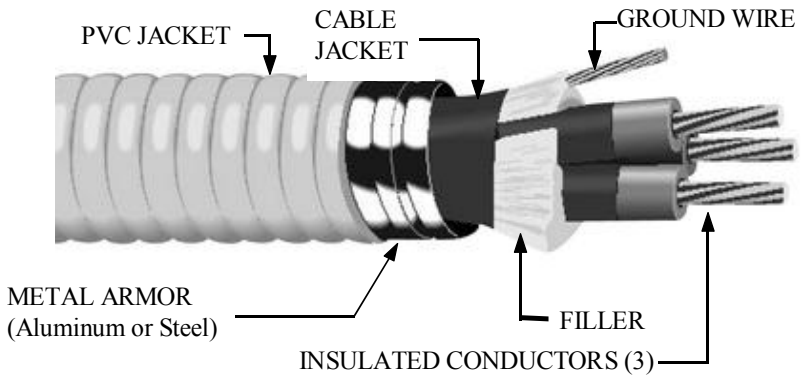


Figure 3.5 - Armored Cable

Power cables may be of single or multi-conductor design. Single conductor cables are typically found inside electrical enclosures and cabinets such as switchgear and motor control centers. A special type of multi-conductor cable called "Triplex cable,"is commonly used in three-phase power applications such as supplying power to a motor-operated valve from a motor control center. A triplex cable contains three individually insulated conductors that are twisted around each other and contained within an outer jacket (see Figure 3.5).

Control and instrument cables are nearly always multi-conductor design. Although the number of conductors that may be contained in a multi-conductor cable is theoretically unlimited, practical considerations such as as the difficulty of installing long runs of very large diameter cable tend to limit their size. Common control circuits employ multi-conductor cables having 3, 7, and 11 conductor configurations. Because of the need to block external sources of electrical "noise" generated by other plant equipment, *instrument cables* frequently use a number of *"twisted/shielded pairs*" of conductors contained within a protective outer jacket. The twisting of conductors serves

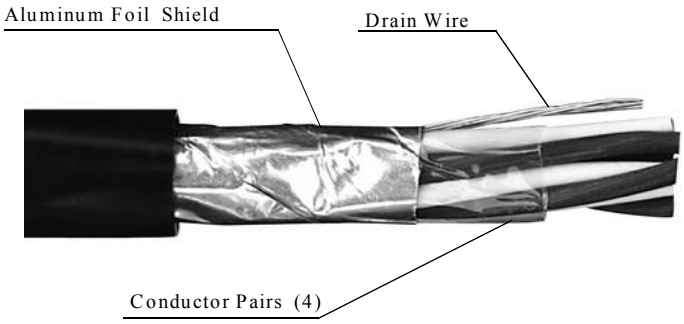


Figure 3.6 Illustration of Instrument Cable

to reduce magnetic noise while the shield and drain wire reduce electrostatic and radio-frequency interference. As shown in Figure 3.6, the *shield* consists of a conductive material (typically aluminum foil) that is wrapped around the twisted pairs of conductors. The uninsulated *drain wire* which is in physical and electrical contact with the shield, provides for easier termination of the foil shield to a common ground point (typically the metal chassis).

3.2.2 Functional Considerations of Conductors and Cables

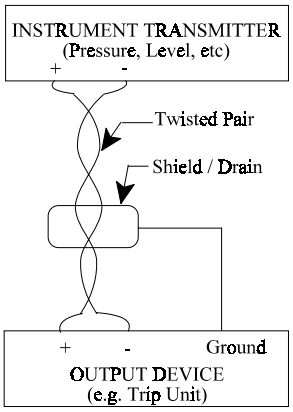


Figure 3.7 - Twisted / Shielded Pair

The fundamental purpose of a cable conductor is to provide a path for electrons to move from one location to another. The *force or pressure* that causes the electrons to move through the conductor is called *voltage*, measured in "volts". The quantity or *flow rate* of electrons moving through the conductor is called *current*. Current is measured in units called amps or amperes where one amp is equal to a flow of one coulomb per second through a wire (a coulomb is 6.28×10^{23} electrons). Simply stated, *voltage causes current.* Given a voltage and a complete path for the electrons (i.e., a complete circuit), current will flow. Given the path, but no voltage, or voltage without a path (e.g., an open circuit), there will be no current.

Resistance is a force that opposes the flow of electrons. Every material, including the most effective conductors (e.g., silver and gold) offers some resistance to current low. Principal factors affecting the amount of resistance presented by a conductor include:

1. Length. The longer the conductor, the higher the resistance.
2. Diameter (Gauge). The smaller the conductor, the higher the resistance.
3. Temperature. The resistance will increase as temperature increases.
4. Material. Some materials are better conductors than others. Gold and silver are excellent conductors but are also very expensive. Since copper is a very good conductor and is not cost prohibitive, it is widely used.

Many people tend to think of conductor size only in terms of its current carrying capability (ampacity). For example, one general "rule of thumb" is that a cable containing No. 12 AWG copper conductors is sufficient to power loads supplied from a circuit breaker that has a 20 ampere trip point. While this "rule of thumb" may be sufficient for most home wiring applications, in large facilities such as nuclear power plants other factors such as cable length and ambient temperature may also have a significant impact on cable selection.. As indicated above, the resistance of a conductor will increase as its length increases, its diameter decreases or the temperature of its surrounding environment (ambient temperature) increases. Whenever a current flows through a conductor heat is generated. As the cable length increases its resistance also increases. This resistance creates a voltage loss or "drop" in the cable. For example, if a cable is supplying power to a motor that is located some distance from its power source (e.g., MCC) and the gauge (diameter) of the cable conductors is not properly sized (increased) to accommodate for the additional resistance presented by the length of cable, the voltage measured at the motor will be less than that measured at the MCC, and in certain cases may be insufficient for proper motor operation. Depending on the specific application, *voltage drop* and *ambient temperature* may be important considerations in the selection of cables.

The *temperature rating* of a cable / conductor is the maximum temperature at which its insulating material may be used in continuous operation without loss of its basic properties The most common ratings are 60°, 75° and 90° centigrade (140°, 167°, and 194° F). *Ampacity* is the amount of current a cable / conductor can carry continuously under conditions of use without exceeding its temperature

rating. This definition of *ampacity* recognizes that the maximum current a conductor can carry continuously varies with the conditions of use as well as with the temperature rating of the conductor insulation. For example, ambient temperature is a condition of use. A conductor with 60° insulation installed near a furnace so that the ambient temperature is 60° continuously has no current carrying capacity. Any current flowing through the conductor will raise its temperature beyond the 60° insulation rating. The ampacity of this conductor, regardless of its size is therefore zero.[2]

The normal ambient temperature of a cable installation is the temperature the cable would assume at the installed location with no load being carried on the cable.[3] Ampacity limits for various combinations of cables and ambient temperatures are given in the National Electrical Code (ANSI/NFPA 70). It is important to note, however, that in addition to ambient temperature many other external factors can affect the ampacity of an electrical conductor. Examples include cable tray fill, heat generated by the conductor as a result of load current flow, heat generated by adjacent cables (e.g., within the same cable tray), and any insulating material that may surround the cable (e.g., fire protective wrapping over a cable tray). Such factors must be taken into consideration when selecting conductors for a specific application.

In the U.S., cables are manufactured in accordance with a standard known as *American Wire Gauge* (AWG) where "gauge" refers to the diameter of the metallic conductor (without insulation). The higher the gauge number, the smaller the diameter of the wire conductor. For example, wiring used to power receptacles in most U.S. households is AWG number 12 or 14 while telephone wire is usually AWG number 22, or 24. Because it has less electrical resistance over a given length, thick wire (i.e., small AWG number) can carry more current than thin wire (large AWG number). For example, a copper AWG Number 12 conductor is approximately 0.08 inches in diameter and can carry about 20 amperes of current. Conversely, an AWG Number 1 conductor has a diameter of approximately 0.30 inches and can carry about 150 amperes of current. Conductors of power cables may range from 0.08 inches in diameter (12 AWG) to over one inch. Because they carry less current, control cables commonly range from 16 AWG up through 10 AWG and instrumentation cables are generally 16 AWG or smaller.

The largest diameter conductor specified in the AWG system is 0000 or 4/0 (pronounced “4-ought”). Wire sizes larger than those covered in the AWG system are specified in circular mills (cmill). By definition a circular mill is the area of a circle whose diameter is one mil (one one-thousandth of an inch). Because this unit t is so small the prefix "M" is normally used in denoting wire sizes. For example, a conductor that is 250,000 circular mils is normally denoted 250 MCM.

---

[2] The National Electric Code Handbook, P. J. Schram, Editor, 1997

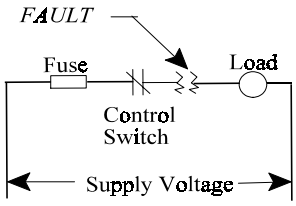
[3] ANSI/IEEE Std 141-1986

In most applications the size of a cable is expressed in terms of the gauge (AWG) of its individual conductor(s) and the number of conductors it contains. For example, a cable that contains three, number 12 AWG conductors would be described as a “three conductor number 12" or “3/C, 12AWG" cable

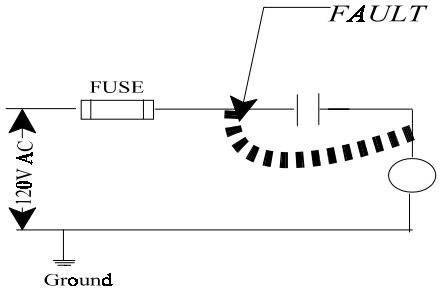
3.3 Circuit Failure Modes and Mechanisms

As discussed previously, cables are comprised of one or more electrical conductors. The individual conductors are electrically isolated from each other and from other possible diversion paths (e.g., ground), by a layer of electrical insulation material. When exposed to the effects of fire and its related perils (e.g., fire-fighting activities), insulation and other protective materials (e.g. jacket) may be subjected to a broad range of potentially damaging stressors or *failure mechanisms.* For example, heat could cause a significant reduction in the quality of electrical isolation provided by the conductor insulation material or in certain cases cause it to completely melt away. Heat, combined with smoke and products of combustion could initiate faults in electronic components and printed circuit boards. The addition of fire suppression agents could further exacerbate the effects of already damaged insulation and mechanical forces, such as those that may be inflicted during fire-fighting activities (e.g., impact of a fire hose stream), could cause a further reduction in the physical and electrical integrity of cables and circuits. As a result, cables and circuits that are exposed to the effects of fire are expected to experience one or a combination of following fault conditions *or failure modes:*

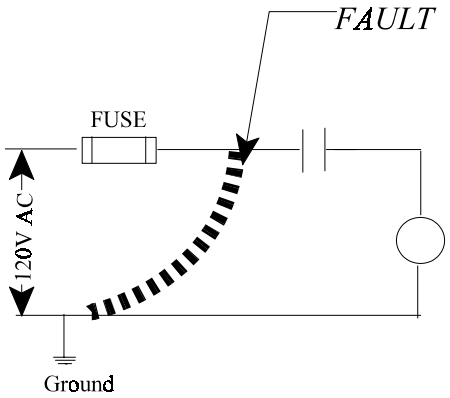
- *Open Circuit* - The loss of electrical continuity.(i.e., the conductor is broken and the signal or power does not reach its destination).



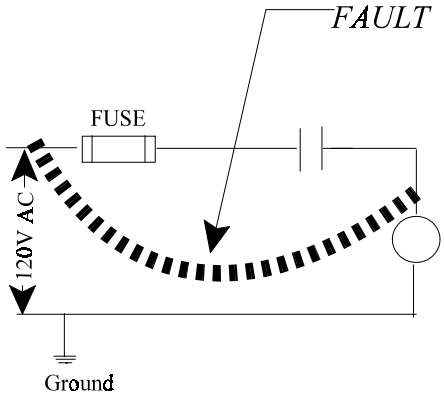
- *Short Circuit* - An abnormal connection of relatively low impedance between two points of different potential.



- *Shorts to Ground* - A conductor comes into electrical contact with a grounded conducting medium such as a cable tray, conduit, or a grounded conductor.



- *Hot Short* - A special type of short circuit condition that causes a previously un-energized conductor to become energized. As a result of this fault, the voltage, current, or instrument signal present in the energized conductor(s) is impressed on the previously un-energized conductor(s). As illustrated below, a hot-short could bypass circuit protective features and cause the unintentional actuation of equipment.



- *High-impedance Fault* - A special type of short circuit condition in power cables where the fault contains some element of resistance to current flow. An *arcing fault* is a specific type of high-impedance fault. Rather than having direct contact offering minimal resistance to fault current (i.e., "bolted" fault condition) the arcing fault current must flow through or "arc over" a small air gap or water. *"Because of the resistance of the arc and the impedance of the return path, current values are substantially reduced from the "bolted fault level"*[4] For analytical purposes, high-impedance fault current is postulated to be a value that is just below the trip point of the individual circuit protective device (fuse/circuit breaker).

3.4 The Browns Ferry Fire

On March 22, 1975, a severe fire involving electrical cables occurred at Unit 1 of the Browns Ferry nuclear power station, operated by the Tennessee Valley Authority (TVA). The Browns Ferry plant consists of three boiling water reactors each designed to produce 1067 megawatts of electrical power. At the time of the fire, Units 1 and 2 were operating at 100% capacity while Unit 3 was still under construction.

---

[4] ANSI IEEE Standard 242-1986, *"IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems"*

The fire began in a bank of cable trays in an area of the Unit 1 cable spreading room where the trays passed through a penetration in a wall separating the cable spreading room from the reactor building. At Browns Ferry, the reactor building functions as the secondary containment for the nuclear steam supply systems. To preclude uncontrolled and unmonitored releases of airborne radioactivity, the reactor building is designed (and required by license condition) to be maintained at a negative pressure (0.25 inches of H_2O / 62.3pa) in relation to the remainder of the plant and the outside environment. The penetration seal inspection process in place at the time of the fire used this differential pressure as a means of identifying defective seals. If the penetration seal was defective, smoke from a candle would be drawn toward the seal. When workers used this method to test a newly installed penetration seal, however, the flame of the candle was drawn into the penetration, igniting the polyurethane foam used as a sealant material. The pressure differential between the cable spreading room and the reactor building then served to fan the fire, causing it to rapidly spread to a large number of cables located in trays on the opposite side of the wall.

Due to a number of contributing factors including the large amount of combustible cable insulation involved in the fire, the inaccessibility of fire in cable trays located approximately twenty feet above the floor, dense smoke, limited availability of breathing apparatus and the operator's reluctance to use water to extinguish an electrical fire, the fire continued to burn for over seven hours. Although the fire had a significant impact on plant operations, only a relatively small area of the plant was actually involved. In the cable spreading room, damage was limited to a 25 square foot area adjacent to the penetration where the fire started. The major amount of fire damage occurred on the opposite side of this penetration in an area of the Reactor Building measuring approximately 40 feet by 20 feet. Although damage was limited to a relatively small area of the plant, temperatures as high as 1500°F caused damage to more than 1600 cables routed in 117 conduits and 26 cable trays. Of those, 628 cables were safety related and their damage caused the loss of a significant number of plant safety systems, including redundant trains of Emergency Core Cooling Systems (ECCS) and electric power and control systems. Fire-induced damage to cables located in the area, also impeded the functioning of normal cooling systems, and degraded the capability to monitor the status of the plant.

As discussed in Section 3.3 above, when conductors of circuits and cables are exposed to the effects of fire and/or fire fighting activities, their electrical integrity and, hence, their ability to properly function will be compromised. The Browns Ferry fire demonstrated the impact fire-induced cable faults can have on the operability of redundant plant safety systems. Some of the more salient consequences this failure mechanism imposed on the operation of Unit 1 are depicted in Table 1 below. It should be noted that for the purpose of discussion the consequences of cable fire damage described in Table 1 are limited to those that were observed on Unit 1 operations. Although not as severe, the fire also impacted Unit 2 operations for approximately six hours following fire initiation. Examples of abnormalities noted by Unit 2 operators include the loss of electrical power supplied from various 4kV and 480V shutdown boards, closure of the MSIVs, loss of the manual actuation capability of all safety relief valves, and loss of High Pressure Coolant Injection (HPCI) due to spurious closure of torus suction valves.

While certain operational consequences developed as the fire progressed, a review of the documented chronology of the event indicates that many abnormalities, including spurious ECCS system alarms, false instrument indications, reduction in power level (due to a run back of the Reactor Recirculation pumps for no apparent reason), and spurious starts and stops of Residual Heat Removal (RHR), Core Spray (CS), Reactor Core Isolation Cooling (RCIC) and High Pressure Coolant Injection (HPCI) pumps, were observed to occur rather quickly, during the first twenty to thirty minutes following the ignition of polyurethane sealant material. The Browns Ferry fire was a clear demonstration of the impact a fire involving redundant trains of electrical cables and circuits can have on the ability of operators to monitor and control important plant parameters.

Consequence of Fire Damage	Attributed Cause
Loss of power supplied from 480V Shutdown Boards 1A and 1B	- Fire-induced **hot-short** in circuit breaker trip indicating light caused voltage to be backfed to the breaker trip coil keeping it energized - Power Cable faults
Spurious closure and inability to reopen Main Steam Isolation Valves	Fire damage to MSIV control circuits
Spurious trip of Reactor Feedwater Pump "A"	False high reactor water level signal to feedwater pump controller (Note remaining feed pumps B and C were manually tripped at time of scram)
Inoperability of High Pressure Coolant Injection System (HPCI)	Fire-induced faults to cables associated with 250VDC MOV Board 1A which powers HPCI valve controls, and cables associated with 480V MOV Board 1A which powers the steam isolation valve
Inoperability of redundant RHR Systems (1A, 1B, 1C, and 1D)	Fire-induced failure of 480V MOV Boards 1A and 1B caused loss of power to valves. Also, fire-induced loss of power supplied from 4kV Shutdown Board C caused a loss of RHR pump 1B.
Inoperability of redundant Core Spray Systems (1A, 1B, 1C, and 1D)	Fire-induced failure of 480V MOV Board 1A and 1B caused loss of power to valves. Also, fire-induced loss of power supplied from 4kV Shutdown Board C caused loss of CS pump 1B.
Inoperability of redundant trains of Standby Liquid Control Systems (1A, 1B)	Fire-induced loss of power from redundant 480V Shutdown Boards 1A and 1B to pump motors and valves
Inoperability of Reactor Core Isolation Cooling System (RCIC)	Inability to electrically operate steam isolation valve due to cable fault and loss of power on 480V MOV board 1B
Loss of ability to operate all Relief Valves	Spurious closure and inoperability of 7 of 11 relief valves attributed to loss of power supplied from redundant 250VDC boards 1A and 1B. Subsequent spurious closure of drywell air compressor flow control valve cut off air supply to remaining 4 relief valves rendering them inoperable for four hours.
Abnormal behavior of instrumentation - Observed alarms on ECCS system were contrary to status of systems - Random lights on ECCS panel began glowing alternately bright and dim	Fire damage to ECCS instrumentation circuits
Loss of operability of Emergency Diesel Generator "C" and loss of remote control capability of EDG "B" and EDG "D"	Fire damage to EDG control and instrumentation circuits

Table 1 - Consequences of Cable Fire Damage at Browns Ferry Unit 1[5]

[5] "Hearings Before the Joint Committee on Atomic Energy, Congress of the United States, First Session," September 16, 1975

3.5 Insights and Observations Resulting From the NEI Fire Test Program

To further investigate the effects of fire conditions on circuit integrity and the potential for fire-induced spurious actuations, during the period of January 8 to June 1, 2001, the Nuclear Energy Institute (NEI) sponsored a series of eighteen (18) cable fire tests at Omega Point Laboratories, located in Elmendorf, Texas. All tests were conducted within a 10 ft. by 10 ft. by 8 ft. high steel enclosure having a single natural ventilation opening in one wall. Since the primary objective was to assess the potential for fire to cause undesired spurious actuations of equipment, the test included only control and control power (120Vac) cables. Ungrounded DC circuits and power cables (480Vac and 4160Vac) were not included in the test. As a result, the potential for fire to cause certain types of power circuit-fault conditions, such as "high-impedance faults" were not fully evaluated. Three types of cables were tested including: a specific type of multi-conductor armored cable having thermoset insulation; several types of thermoplastic cable; and several types of thermoset cable. The tested cables were connected to a single control circuit whose spurious actuation was the object of the study. The control circuit was a specific motor starter (a NEMA-1 starter) for a motor operated valve. Some of the salient findings and observations resulting from these tests include[6]:

- The most obvious conclusion of the whole exercise is that hot shorts leading to spurious actuations cannot be regarded as of negligible importance if the fire under consideration produces cable temperatures above the thresholds identified herein.

- For the majority of the tests there was at least one device actuation observed, and for several tests multiple actuations were observed.

- Overall, the likelihood of spurious actuation given failure was found to be somewhat higher than I might have assumed prior to conduct of the tests.

- *Thermoplastic* cable appears to be more likely to degrade to the point of allowing leakage currents large enough to cause device actuations or blown fuses than either armored cable or thermoset cable for the same exposure conditions.

- It appears that 400°F is the approximate degradation temperature of the thermoplastic cable used in these experiments and 700°F is the approximate degradation temperature of the thermoset cable used in these experiments. Beyond these degradation temperatures, the potential for the loss of insulation resistance and consequent electrical activity is likely to depend on a number of factors that are difficult to characterize based on the 18 tests conducted for this project.

- Water spray on damaged cables can cause spurious actuations to occur.

---

[6] EPRI Technical Report 1006961, *Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of Expert Elicitation*, Final Report, May 2002, EPRI Palo Alto, CA

- The available test data as a whole demonstrates that at least four factors are critical to the assessment of spurious actuation likelihood: armored versus non-armored cables; cables in trays versus cables in conduits; cable-to-circuit wiring configuration; and circuits without Control Power Transformers (CPTs) versus circuits with CPTs.

- The tested configuration used a 150VA CPT on a nominal 120V circuit. This application may bound, for example, NEMA size 1 starters which are limited to typically a maximum 7.5 HP motor. For circuits with a higher range, it is suggested to use the non-CPT values.

- Spurious actuations due to hot shorts between different cables were also observed with fair frequency. For some configurations, as many as one in three failed cable bundles experienced at least one spurious actuation attributed to cable-to-cable hot shorts. In two cases, a single cable bundle actually experienced two device actuations each attributed to separate inter-cable hot shorts.

- It appears that the fact that all the NEI/EPRI tests involved one explicitly grounded conductor was also significant...For the multi-conductor cables, the fact that one conductor in the MOV circuit was always grounded likely had a strong influence on the number of fuse blows versus actuations seen. While it is anticipated that this will, indeed, be the predominant configuration for actual circuits, it would appear inappropriate to apply these same results directly to cases where there is no ground conductor present in the cable...If one were to take away the explicitly grounded conductor from the MOV circuit, the likelihood of spurious actuation would certainly increase.

- No open-circuit type of failures were observed which places an upper bound on such an end-point in the range of a 1% probability, given the number of possible open circuits. (*Ed. Note:* The inability to establish this failure mode may be attributable to several factors including the following: The maximum temperature achieved during the test [approximately 1200° F] was less that the melting point of copper (approximately 1984° F) and the cables were not subjected to any of the physical insults that may be reasonably expected to occur in an actual plant fire event [e.g., impact of 100 lb. hose stream, falling debris, and physical impacts resulting from fire-fighting activities])

- Shorting to another conductor within the same cable is much more likely than shorting to a conductor in another cable.

- The probability that a given conductor in a failed cable will short to another conductor within the same cable (conductor-to-conductor short) is <u>very high</u>, in the range of 70% to 80%. The uncertainty on this estimate is perhaps ±10% to ± 15% to encompass a high confidence range.

- The presence of a grounded conductor in a multi-conductor cable seems to decrease the probability by about half that the source conductor will find a non-grounded conductor to which to short.

- The probability that a source conductor in a multi-conductor cable will short to an adjacent (different) single conductor cable (cable-to-cable short) is generally lower than the probability that a conductor-to-conductor short will occur within the multi-conductor cable. If there is no conductor-to-conductor short, the cable-to-cable short probability is in the range of 20%. The uncertainty in this 20% estimate is significant, perhaps ±5% to ±15% to encompass a high confidence range. For thermoplastic cables, this probability is somewhat higher, perhaps 1.5 to 2 times higher.

- For a given damaged 7-conductor cable, there is no reason in practice why one of its conductors might or might not short to another conductor in the same cable, while a different conductor in the same cable might short to a conductor in an adjacent (different) cable. All of these outcomes are feasible, are generally independent of each other and depend on configuration and electrical details that can be described probabilistically.

- Given cable damage, if a short to another non-grounded conductor occurs first, the time interval before an eventual short to ground is typically quite short, seldom more than a few minutes.

- For the cable configuration tested, the data indicate that a single-conductor cable will usually short to ground before shorting to another single conductor cable. For *thermoset* cables the probability is about 85% to 90%. For *thermoplastic* cables the probability is about 70% to 75%.

- The data recorded a significant number of spurious actuations, given cable damage.

- In a configuration in which one source conductor exists together with one or two target conductors within the same cable (specific conductor-to-conductor shorts within a multi-conductor cable) and one of the conductors within the cable is grounded the probability of spurious actuation is estimated with high confidence to lie between 0.10 and 0.50, with a best estimate point value near 30. The wide range is an indication that ther is considerable uncertainty in the numerical values. (*Ed. Note*: Having one of the conductors in the multi-conductor cable grounded is likely to typify most plant configurations. However, it appears that the absence of a grounded conductor could significantly alter the stated numerical values of probability. As stated above, the presence of a grounded conductor in a multi-conductor cable was observed to decrease the probability that a source conductor will find a non-grounded conductor to which to short by about half.)

- Undesired spurious actuations were caused by a single conductor cable shorting to an adjacent single conductor cable without grounding (cable-to-cable short). The probability for this case is estimated to fall between 0.05 and 0.30 with a best estimate point value near 0.20.

- Undesired spurious actuations were caused by an interaction between an energized conductor within a multi-conductor cable having one grounded conductor and an adjacent single conductor cable. The probability for this case is estimated to fall between 0.05 and 0.20 with a best estimate point value near 0.10.

- Undesired spurious actuations were caused by cable-to-cable faults involving adjacent multi-conductor cables that had one of their conductors grounded . Since the failures were observed to occur late into the tests (more than 2 hours) the report concludes that such interactions are unlikely "since actual nuclear plant fires are unlikely to burn that long."

- Several instances of multiple spurious actuations were observed in the same test, sometimes involving different conductors in the same multi-conductor cable.

- For armored, multi-conductor, thermoset, cable having its armor shield maintained at ground potential, the probability of conductor-to-conductor shorts is estimated to be in the 20% to30% range. This is significantly lower than the 70% to 80% range estimated for unarmored cable.

- The opportunity for armored cable shorting to another cable (cable-to-cable short) was observed to be nil. The report concludes that this probability should be zero.

4. REQUIREMENTS

4.1 Safety Objective

The fundamental safety objective of the NRC regulatory program is to ensure the protection of the health and safety of the public. This means that the risk to the public from normal operation, anticipated transients, and accidents must be acceptably low and that the likelihood of accidents more severe than those postulated for design purposes must be extremely small. To achieve this high level of safety, redundant (identical or diverse) safety systems are incorporated into the design of all nuclear power plants operating in the U.S.. Redundancy provides assurance that failures affecting one system will not have a significant impact on plant safety because a "back-up" system has been provided in the plant design. Separation of the redundant subsystems is typically accomplished by dividing safety equipment and cables into separate divisions. The provision of separate and redundant divisions of safety systems provides confidence that the failure of components or cables within one division will not adversely affect the plant's ability to accomplish required safety functions. In the absence of suitable protection features, such as separation distance or structural barriers, however, redundant trains of cables and equipment could be susceptible to a phenomenon known as "common-mode" failure, where multiple failures in redundant systems may occur as a result of a common cause[7]. If a single event, could induce failures in more than one of the redundant elements, the safety and reliability benefits afforded by this essential design feature could be negated. Examples of events having the potential to initiate common-mode failures in redundant safety systems are flooding, earthquakes and fire.

As discussed in Section 3, a major fire that occurred at Unit 1 of the Browns Ferry plant on March 22, 1975 illustrated the impact common-mode failures due to fire may have on the operation of a commercial nuclear power plant. Shortly after that event, on March 26, 1975 the NRC established a Special Review Group (SRG) to investigate the cause of the fire and initiate an evaluation of the need for improving the fire protection programs at all nuclear power plants. The SRG found serious design inadequacies regarding fire protection at Browns Ferry. In its report, "Recommendations Related to Browns Ferry Fire" (NUREG-0050, February 1976), the SRG provided over fifty recommendations for improving fire prevention and control in existing facilities. The SRG specifically noted that the independence of redundant equipment at Browns Ferry was negated by not having a suitable level of separation between cables associated with redundant trains of safety equipment, and recommended that a suitable combination of electrical isolation, physical distance, barriers, and sprinkler systems be applied to maintain independence of redundant safety equipment, and therefore, the availability of safety functions, in spite of postulated fires. In view of its findings, the SRG called for the development of specific guidance for implementing fire protection regulations, and for a comparison of that guidance with the fire protection program at each operating plant.

---

[7] IEEE Std. 100-1988

The Browns Ferry fire was of sufficient significance to warrant major changes in the fire protection programs of nuclear power plants operating in the U.S.. In the years following the fire the NRC and the nuclear industry expended considerable resources in developing and implementing fire protection guidelines and regulatory requirements directed at minimizing both the probability of occurrence and the possible consequences of postulated fires. As a result of this effort, each operating plant currently has an approved fire protection program that is anchored in the long established defense-in-depth safety principle of providing multiple barriers of protection to prevent and mitigate accidents. With regard to fire protection, these barriers consist of administrative controls and personnel training necessary to reduce the potential for fire to start and plant design features needed to rapidly detect and promptly extinguish those fires that may occur. In addition, because of the potentially unacceptable consequences an unmitigated fire may have on plant safety, each operating plant must demonstrate that in the event a fire were to initiate and continue to burn (in spite of prevention and mitigation features) the performance of essential shutdown functions will be preserved and radioactive releases to the environment will be minimized.

Requirements for protecting structures, systems, and components (SSC) important to safe shutdown in the event of fire have been shown to have safety benefit. Plant design changes required by the regulation (10 CFR 50 Appendix R) have been effective in preventing a recurrence of a fire event of the severity experienced at Browns Ferry.[8] In 1989, Sandia National Laboratories issued the "Fire Risk Scoping Study." According to this study, plant modifications made as a result of Appendix R to 10 CFR Part 50 reduced core damage frequencies (CDFs) at some plants by a factor of ten. The study also suggests that improper implementation of the regulatory requirements and degradation of fire protection defense in depth could be risk significant. The study concluded, for example, that weaknesses in either manual fire fighting effectiveness or control systems interactions could raise the estimated fire-induced CDF by an order of magnitude.

In Generic Letter No. 88-20, Supplement 4, the NRC requested each licensee to perform an Individual Plant Examination of External Events (IPEEE) for plant-specific severe accident vulnerabilities initiated by external events and to submit the results to the NRC. Under the IPEEE program, the licensees systematically assessed the fire risk for each operating reactor. The results of the IPEEE fire analyses provide important insights regarding reactor fire risk and confirm the results of the "Fire Risk Scoping Study." For example, the IPEEE results show that fire events are important contributors to the reported CDF for a majority of plants, ranging on the order of 1E-9/yr to 1E-4/yr, with the majority of plants reporting a fire CDF in the range of 1E-6/yr to 1E-4/yr. The reported CDF contribution from fire events can in some cases approach (or even exceed) that from internal events.[9]

---

[8] NEI-00-001, Industry Proposed Method for Resolving Fire-induced Circuit Failure Regulatory Issues, Draft Rev. C, October 2001

[9] SECY 99-140, Recommendation for Reactor Fire Protection Inspections, May 20, 1999

4.2 Background

Appendix A to 10 CFR 50 establishes the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components (SSC) important to safety. With regard to fire protection, General Design Criterion 3 (GDC 3) requires that structures, systems, and components important to safety be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials are required to be used wherever practical, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability are required to be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. GDC 3 also requires that firefighting systems be designed to ensure that their failure, rupture, or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.

During the initial implementation of the U.S. nuclear reactor program, regulatory acceptance of fire protection programs at nuclear power plants was based on the broad performance objectives of GDC 3. Due to a lack of detailed implementation guidance available at that time however, the level of fire protection was generally found to be acceptable if the facility complied with local fire codes and received an acceptable rating from its fire insurance underwriter. Thus, the fire protection features installed in early U.S. nuclear power plants were very similar to those of conventional, fossil-fueled, power generating stations.

The lessons learned from the Browns Ferry fire brought fundamental change to fire protection and its regulation in the U.S. nuclear power industry. As described in Section 3.4, the fire was started by plant workers using the flame of a candle to test for air leakage through a penetration in a wall that separated the cable spreading room from the the reactor building. Although most of the fire damage was contained to a relatively small area of the reactor building (approximately 800 square feet), more than 1600 cables, routed in 117 conduits and 26 cable trays, were affected of which 628 were important to safety. The resulting damage impeded the functioning of both normal and standby reactor cooling systems, significantly degraded the operator's ability to monitor important plant parameters, and forced operators to initiate emergency repairs in order to restore systems needed to place the reactor in a safe shutdown condition.

The Brown's Ferry fire demonstrated that the occupant safety and property protection concerns of the major fire insurance underwriters did not sufficiently encompass nuclear safety issues, particularly with regard to the potential for fire to cause the failure of systems and components important to safe shutdown of the reactor. Investigations of the cause and possible consequences of this event revealed several significant fire protection vulnerabilities, including:

- the apparent ease with which the fire started,
- the hours that elapsed before it was fully extinguished, and
- the unavailability of redundant trains of plant safety equipment.

Based on these findings the NRC concluded that additional specific guidance for implementing its existing fire protection regulation (GDC 3 to 10 CFR 50) was necessary. In recognition of the potential consequences of fire, and to assure that an adequate level of fire safety is incorporated into the overall design and operation of all nuclear power plants operating in the United States, the NRC determined that established safety principles of defense-in-depth should be applied in defense against fires.

Defense-in-Depth

Defense in depth is a fundamental safety philosophy which provides multiple layers of protection (i.e., barriers) to prevent and mitigate accidents. With regard to fire protection, this concept achieves the required degree of safety by using echelons of administrative controls, fire protection systems and features, and safe shutdown capability. These defense- in-depth principles are aimed at achieving the following objectives:

a. To prevent fires from starting;
b. To detect rapidly, control and extinguish promptly those fires that occur; and
c. To provide protection for structures, systems and components important to safety so that a fire that is not promptly extinguished by the fire protection activities will not prevent the safe shutdown of the plant.[10]

The multiple levels of protection that are embodied in the defense-in-depth philosophy assure fire safety throughout the life of the plant by minimizing both the probability and consequence of fires. While it is recognized that no one level can be perfect or complete by itself, and strengthening any one level can compensate in some measure for known or unknown weaknesses in the others, each level of protection must meet certain minimum requirements.

Consistency with the defense-in-depth philosophy is maintained if:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided.
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved.

[10] 10CFR50 Appendix R , Section II, General Requirements, Paragraph A, Fire protection program

- The intent of the General Design Criteria in Appendix A to 10 CFR Part 50 is maintained.[11]

4.3 Development of Fire Protection Program Requirements

To assist licensee's in the enhancement of their fire protection programs, the NRC staff incorporated recommendations it received from the Browns Ferry Special Review Group into a single guidance document and in May 1976 issued Auxiliary and Power Conversion Systems Branch, Branch Technical Position 9.5-1 (BTP 9.5-1) "Guidelines for Fire Protection for Nuclear Power Plants." As part of this action, the staff requested each licensee to provide an analysis that divided the plant into distinct fire areas and demonstrates that redundant trains of equipment required to achieve and maintain cold shutdown conditions were adequately protected from fire damage. The guidance contained in BTP 9.5-1, however, was only relevant to plants which filed an application for construction after July 1, 1979. In an effort to establish a suitable fire protection program without significantly affecting the design, construction, or operation of "older" plants that were either already operating or well past the design stage and into construction, in September of 1976 the NRC modified the guidelines in BTP APCSB 9.5-1, and issued Appendix A to BTP 9.5-1 "Guidelines for Fire Protection for Nuclear Plants Docketed Prior to July 1, 1976". This guidance provided acceptable alternatives in areas where strict compliance with BTP 9.5-1 would require significant modifications. Additionally, the NRC informed each plant that the guidance in Appendix A would be used to analyze the consequences of a postulated fire within each area of the plant, and requested licensees to provide results of the fire hazards analysis performed for each unit and the technical specifications for the present fire protection systems.

Early in 1977 each licensee responded with a fire protection program evaluation that included a fire hazard analysis. These analyses were reviewed by the staff using the guidelines of Appendix A to APCSB 9.5-1. The staff also conducted inspections of operating reactors to examine the relationship of structures, systems, and components important to safety with the fire hazards, potential consequences of fires, and the fire protection features. Based on the results of its reviews the staff determined that additional guidance on the management and administration of fire protection programs was necessary, and in mid-1977, issued Generic Letter 77-002, "Nuclear Plant Fire Protection Functional Responsibilities, Administrative Controls, and Quality Assurance." This document provided criteria used by the staff in its review of specific elements of a licensee's fire protection program, including organization, training, combustible and ignition source controls, firefighting procedures and quality assurance.

By the late 1970s, the majority of operating plants had completed their analyses and had implemented most of the fire protection program guidance of Appendix A to the BTP. Many fire protection issues were resolved during the BTP review process, and agreements were included in the NRC-issued safety evaluation reports (SERs). In certain instances, however, licensee's refused to adopt some of the specified fire protection recommendations, such as the requirements for fire

[11] REGULATORY GUIDE 1.174, An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis, July 1998

brigade size and training; water supplies for fire suppression systems; alternative or dedicated shutdown capability; emergency lighting; qualifications of penetration seals used to enclose places where cables penetrated fire barriers; and the prevention of reactor coolant pump oil system fires. Following deliberation, the Commission determined that, given the generic nature of some of the disputed issues, a rulemaking was necessary to ensure proper implementation of NRC fire protection requirements. Accordingly, the NRC amended its regulations, and in November 1980 issued 10 CFR 50.48, "Fire Protection" (which specified broad performance requirements) and Appendix R, "Fire Protection Program for Nuclear Power Plants Operating Prior to January 1, 1979"(which specified detailed regulatory requirements for resolving the disputed issues).

As originally proposed (Federal Register, Vol. 45, No. 1&5, May 22, 1980), Appendix R would have applied to all plants licensed to operate prior to January 1, 1979, including those for which the staff had previously accepted the fire protection features as meeting the provisions of Appendix A to APCSB 9.5-1. However, after analyzing comments on the proposed rule, the Commission determined that only three of the fifteen items in Appendix R were of such safety significance that they should apply to all plants (licensed prior to January 1, 1979), including those for which alternative fire protection actions had been approved previously by the staff. These items are fire protection of safe shutdown capability (including alternative or dedicated shutdown systems), emergency lighting, and the reactor coolant pump oil system. The final rule required all reactors licensed to operate before January 1, 1979, to comply with these three items even if the NRC had previously approved alternative fire protection features in these areas (Federal Register, Vol. 45, Nov. 19, 1980). In addition, the rule provided an exemption process that can be requested by a licensee provided that a required fire protection feature to be exempted would not enhance fire protection safety in the facility or that such modifications may be detrimental to overall safety.

By letter dated November 24, 1980 the Commission informed all power reactor licensees with plants licensed prior to January 1 1979, of new fire protection regulations contained in Section 10 CFR 50.48 (to ensure each plant had a fire protection program) and Appendix R to 10 CFR 50 (to ensure satisfactory resolution of disputed items). In its letter the Commission stated that the provisions of Appendix R can be divided into two categories:

(1) Those provisions of the Appendix that are required to be backfit in their entirety by the new rule, regardless of whether or not alternatives to the specific requirements of these sections have been previously approved by the NRC staff . These requirements are set forth in Sections III.G, Fire Protection of Safe Shutdown Capability, III.J, Emergency Lighting, and III.O, Oil Collection Systems for Reactor Coolant Pump.

(2) Requirements concerning the “open items” of previous NRC staff fire protection reviews. (An “open item” is defined as a fire protection feature that has not been previously approved by the staff as satisfying the provisions of Appendix A to Branch Technical Position 9.5-1, as reflected in a fire protection safety evaluation report).

Attached as enclosures to this letter were a copy of the Federal Register Notice 45 FR 76602 (Enclosure 1), and a summary of open items identified by the staff during its evaluation of the plant's implementation of Appendix A to BTP 9.5-1(Enclosure 2).

It is important to note that with the exception of Sections III.G, J, L, and O, (which were backfit to all plants operating prior to January 1, 1979 regardless of previous approvals granted by the staff), those portions of Appendix A to the BTP that were previously accepted by the staff remained valid. Therefore, Appendix R does not, by itself, define the fire protection program of any plant. For plants licensed before January 1, 1979 (pre-79 plants) the fire protection program is defined by Appendix A to the BTP, the applicable portions of Appendix R (i.e. open issues from BTP 9.5.1 Appendix A reviews), and any additional commitments made by the licensee, as stated in the conditions of its operating license.

Fire Protection Guidelines for Plants Licensed After January 1, 1979

As stated above, Appendix R is only required to be implemented by plants licensed to operate before January 1, 1979. Fire protection programs at plants licensed after this date were typically reviewed by the staff during their initial licensing process. Certain plants in this category were required to implement specific sections of Appendix R (typically sections III.G., III.J. and III.O) as specified in their "Fire Protection" license condition. Consequently, there was no need to "backfit" Appendix R to plants licensed after January 1, 1979. Additionally, only paragraphs (a), requiring plants to have a fire protection plan that satisfies Criterion 3 of Appendix A to 10 CFR 50, and (b) requiring plants to complete all fire protection modifications needed to satisfy Criterion 3 of Appendix A to 10 CFR 50 in accordance with the provisions of their operating licenses, of the fire protection rule (10 CFR 50.48) apply to plants licensed after January 1, 1979.

Guidelines acceptable to the staff for implementing GDC 3 at plants licensed after January 1, 1979 are presented in NUREG-0800, "Standard Review Plan" (SRP) Section 9.5.1, "Fire Protection Program." This document consolidates the guidance of BTP APCSB 9.5-1, Appendix A to BTP APCSB 9.5-1, Nuclear Plant Fire Protection Functional Responsibilities, Administrative Controls and Quality Assurance (originally issued in August 1977), and the criteria of Appendix R to 10 CFR 50. Since NUREG-0800, SRP 9.5.1, consolidates previous guidance issued by the staff, it may be considered as a single reference document which describes the features of an acceptable fire protection program.

4.4 Requirements, Guidelines, and Clarifications Related to Post-fire Safe Shutdown Capability

The NRC's regulatory framework for nuclear plant fire protection programs is contained in a number of regulations and supporting guidelines, regulatory guides, generic communications (e.g., Generic Letters, Bulletins, and Information Notices), NUREG reports, the Standard Review Plan (NUREG-0800) and associated Branch Technical Positions and industry standards. The comprehensive fire protection guidance and regulatory criteria described in these documents address the broad range of features that comprise an acceptable fire protection program. Consistent with the

objective of this report, however, only those requirements, guidelines, and generic communications (clarification documents) that are specifically related to post-fire safe shutdown capability and the performance of a safe shutdown analysis are discussed in this section.

Regulatory requirements of primary interest include: General Design Criteria 3, 5, 19 and 23 of Appendix A to 10 CFR50, 10 CFR 50.48, and Sections III.G and III.L of 10 CFR 50 Appendix R. While it is recognized that Appendix R is not applicable to plants licensed to operate after January 1, 1979, the technical requirements of Sections III.G and III.L were subsumed into review guidance developed for plants licensed to operate after this date (i.e., Position C.5.b of the Standard Review Plan Section 9.5-1). It is important to note that not all the regulations and guidelines described below are applicable to each plant. Therefore, the reviewer must refer to the plant-specific fire protection licensing bases when determining the applicability of a specific regulation or guideline to a specific plant.

Appendix A to 10 CFR Part 50 "General Design Criteria for Nuclear Power Plants"

Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50 establishes for those plants for which its provisions apply, the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety. The following subsections summarize criteria having specific application to fire protection of nuclear power plants.

- GDC 3, Fire Protection

  GDC 3 requires that structures, systems, and components important to safety be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and heat resistant materials are required to be used wherever practical, particularly in locations such as the containment and control room. Fire detection and fighting systems of appropriate capacity and capability are required to be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. GDC 3 also requires that firefighting systems be designed to ensure that their failure, rupture, or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.

- GDC 5, Sharing of Structures, Systems, and Components

  GDC 5 requires that structures, systems, and components important to safety not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

- GDC 19, Control Room

  GDC 19 requires that a control room be provided from which actions can be taken to operate the nuclear power unit under normal and accident conditions, while limiting radiation exposure to control room personnel under accident conditions for the duration of the accident. GDC 19 also

requires that equipment and locations outside the control room be provided with the design capability to accomplish hot shutdown of the reactor and with a potential capability for subsequent cold shutdown of the reactor. It should be noted that GDC 19 design criteria were largely based on environmental / habitability concerns within the control room. As a result, this criterion does not specifically consider the effect of equipment damage occurring as a result of fire.

- GDC 23, Protection System Failure Modes

  GDC 23 requires that the protection system be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, radiation) are experienced.

10 CFR 50.48 "Fire Protection"

Section 50.48(a) of 10 CFR Part 50 requires that each operating nuclear power plant have a fire protection plan that satisfies General Design Criterion 3 of Appendix A to 10 CFR Part 50. It specifies what should be contained in such a plan and lists the basic fire protection guidelines for the plan. Section 50.48 (b) requires that all plants with operating licenses prior to January 1, 1979, satisfy the requirements of Sections III.G, III.J, and III.O, and other sections of Appendix R to 10 CFR Part 50, where approval of similar features had not been obtained prior to the effective date of Appendix R. Plants licensed to operate after January 1, 1979, must meet the provisions of 10 CFR 50.48(a) The required schedules for licensees to comply with the provisions of Appendix R were established in 10 CFR 50.48(c). Provisions were also included in the rule to allow licensees to file exemptions from Appendix R requirements on the basis that the required modifications would not enhance fire protection safety in the facility or would be detrimental to overall facility safety. These exemptions, upon approval by the staff, become a part of the fire protection licensing basis. The provisions of 10 CFR 50.48(c) have since expired and have been deleted from the regulations. Future exemptions should be requested in accordance with 10 CFR 50.12, as discussed below.

In accordance with 10 CFR 50.48, each operating nuclear power plant must provide the means to limit fire damage to structures, systems, and components important to safety so that the capability to safely shut down the reactor is ensured. A safe shutdown analysis should be developed that demonstrates the capability of the plant to safely shut down for a fire in any given area (see Section 6).

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

One of the principal goals of regulatory requirements and staff guidance issued since the Browns Ferry fire is to ensure that in the event of fire in any area of the plant, one train of equipment needed to achieve and maintain safe shutdown conditions in the reactor will remain free of fire damage. To achieve this objective, Paragraph 50.48(b) of 10 CFR Part 50, which became effective on February 17, 1981, required all licensed nuclear power plants operating prior to January 1, 1979 to meet the requirements of Sections III.G, "Fire Protection of Safe Shutdown Capability," of

Appendix R to 10 CFR 50, regardless of any previous approvals by the NRC for other design features. Compliance with this criterion required each licensee to reassess all areas of the plant and demonstrate for each area that suitable fire protection features (as specified in Section III.G.2 of Appendix R) are provided for redundant trains of cables and equipment necessary to achieve and maintain hot shutdown conditions. As part of this evaluation, licensees were also required to consider the potential effects of fire on associated non-safety circuits and cables that could prevent operation or cause maloperation of required shutdown systems (see Sections 3 and 6). It should be noted that with regard to the fire protection of safe shutdown capability, facilities that commenced operation on or after January 1, 1979 are subject to essentially the same criteria as those contained in Appendix R which have been imposed through license conditions or through licensing commitments.

In developing the regulation, the Commission decided that the overall interest of public safety is best served by establishing some conservative level of protection and assuring that level of compliance. The objective for fire protection of safe shutdown capability is to assure that at least one means of achieving and maintaining safe shutdown conditions will remain available during and after any postulated fire in the plant. Because it is not possible to predict the specific conditions under which fire may occur and propagate, the design basis protective features are specified rather than the design basis fire. The fire protection features specified in Section III.G are not unique to the nuclear industry. Rather, they are based upon principles long accepted within that portion of American industry that has been classified by their insurance carriers as "Improved Risk" or "Highly Protected Risk."[12]

Section III.G.1 of Appendix R requires fire protection features be provided for structures systems and components (SSC) important to safe shutdown. These features must be capable of limiting fire damage so that:

(a) One train of systems necessary to achieve and maintain hot shutdown conditions from either the control room or emergency control station(s) is maintained free of fire damage; and

(b) The extent of fire damage to redundant trains of systems and equipment necessary to achieve and maintain cold shutdown is limited so that at least one train can be repaired or made operable within 72 hours using onsite capabilities.

It should be noted that the fire areas falling under the requirements of III.G.1.b are those for which an alternative or dedicated shutdown capability is not being provided. For these fire areas, Section III.G.1.b requires only the capability to repair the systems necessary to achieve and maintain cold shutdown from either the control room or emergency control station(s) within 72 hours, not the capability to repair and achieve cold shutdown within 72 hours as required for the alternative or dedicated shutdown modes by Section III.L.[13]

---

[12] SECY-80-438A, Rule on Fire Protection Program for Nuclear Power Plants Operating Prior to January 1, 1979, Enclosure A, September 30, 1980

[13] Generic Letter 86-10, Enclosure 1, Paragraph 2, "Repair of Cold Shutdown Equipment"

Section III.G.2, provides various options for protecting the capability to achieve and maintain hot shutdown conditions. Specifically, this section of the regulation states:

> *"Where cables or equipment, including associated non-safety circuits that could prevent operation or cause maloperation due to hot shorts, open circuits or shorts to ground of redundant trains of systems necessary to achieve and maintain hot shutdown conditions are located within the same fire area outside of primary containment, one of the following means of ensuring that one of the redundant trains is free of fire damage shall be provided:*
>
> *a. Separation of cables and equipment and associated non-safety circuits of redundant trains by a fire barrier having a 3-hour rating. Structural steel forming a part of or supporting such fire barriers shall be protected to provide fire resistance equivalent to that required of the barrier; or*
>
> *b. Separation of cables and equipment and associated non-safety circuits of redundant trains by horizontal distance of more than 20 feet with no intervening combustibles or fire hazards. In addition, fire detectors and an automatic fire suppression system shall be installed in the fire area; or*
>
> *c. Enclosure of cable and equipment and associated non-safety circuits of one redundant train in a fire barrier having a 1-hour rating. In addition, fire detectors and an automatic fire suppression system shall be installed in the fire area.*
>
> *Inside non-inerted containments one of the fire protection means specified above or one of the following fire protection means shall be provided:*
>
> *d. Separation of cables and equipment and associated non-safety circuits of redundant trains by horizontal distance of more than 20 feet with no intervening combustibles or fire hazards; or*
>
> *e. Installation of fire detectors and an automatic fire suppression system in the fire area; or*
>
> *f. Separation of cables and equipment and associated non-safety circuits of redundant trains by a noncombustible radiant energy shield."*

<u>Note</u>: Since fire areas are frequently described in terms of the section of III.G that they meet, additional clarification is warranted with regard to the use of this terminology. For a fire area to "meet III.G.1" at least one train of shutdown systems and equipment must be completely independent (physically and electrically) of the fire area. A "III.G.2 Fire Area" contains redundant trains of shutdown equipment, however, one train has been assured to remain free of fire damage (per the criteria contained in this section of the regulation). A "III.G.3 Fire Area" contains redundant trains of shutdown equipment or cables and one train has <u>not</u> been assured to remain free of fire damage (per III.G.2 criteria) or redundant trains are vulnerable to damage as a result of fire suppression activities or the inadvertent actuation of fire suppression systems.

Interpretation 3 of GL-86-10 defines the term "free of fire damage" in Section III.G.1.a. This interpretation was provided to clarify Section III.G.1.a, during the exemption process, for licensee's attempting to justify the lack of III.G.2 separation features for redundant trains within a single fire area. It was never intended that "other methods proposed by licensees" would be reviewed and approved at the Appendix R validation inspection. For any fire area an approved exemption is required where neither alternative safe shutdown nor the separation features of Section III.G.2 are provided. (Reference: BWROG Generic Guidance for Post-fire Safe Shutdown Analysis Assessment, Rev. G, June 24, 1998, pg. 3-48 , and NRC Internal Memo (Whitney to MnKee) 8/11/86, Enclosure 2, SECY 85-306 Meeting Minutes of 5/7/86).

As indicated in the above text, Appendix R utilizes the term *"free of fire damage."* In promulgating Appendix R, the Commission has provided methods acceptable for assuring that necessary structures, systems and components are free of fire damage (see Section III.G.2a, b and c), that is, the structure, system or component under consideration is capable of performing its intended function during and after the postulated fire, as needed.[14]

Where the protection of systems whose function is required for hot shutdown does not satisfy the requirement of paragraph G.2, or where redundant trains of systems required for hot shutdown located in the same fire area may be subject to damage from fire suppression activities or from the rupture or inadvertent operation of fire suppression systems, Section III.G.3 of Appendix R requires an alternative or dedicated shutdown capability and it associated circuits be provided that is independent of cables, systems or components in the area, room, or zone under consideration. In addition, Section III.G.3 further requires that fire detection and a fixed fire suppression system be installed in the area, room, or zone under consideration. Specific criteria for implementing this capability are contained in Section III.L of Appendix R, " Alternative and Dedicated Shutdown Capability."

Although 10 CFR 50.48(b) does not specifically include Section III.L with Sections III.G, J, and O of Appendix R as a requirement applicable to all power reactors licensed prior to January 1, 1979, the Appendix, read as a whole, and the Court of Appeals decision on the Appendix, Connecticut Light and Power, et al. v. NRC, 673 F2d. 525 (D.C. Cir., 1982), demonstrate that Section III.L applies to the alternative safe shutdown option under Section III.G if and where that option is chosen by the licensee[15].

Section III.G recognizes that the need for alternate or dedicated shutdown capability may have to be considered on the basis of a fire area, a room or a fire zone. The alternative or dedicated capability should be independent of the fire area where it is possible to do so. When fire areas are not designated or where it is not possible to have the alternative or dedicated capability independent of the fire area, careful consideration must be given to the selection and location of the alternative

---

[14] Generic Letter 86-10, Enclosure 1, Paragraph 3, "Fire Damage"

[15] Generic Letter 86-10, Enclosure 2, Q 5.1.3

or dedicated shutdown capability to assure that the performance requirement set forth in Section III.G.l is met. Where alternate or dedicated shutdown is provided for a room or zone, the capability must be physically and electrically independent of that room or zone. The vulnerability of the equipment and personnel required at the location of the alternative or dedicated shutdown capability to the environments produced at that location as a result of the fire or fire suppressant's must be evaluated. These environments may be due to the hot gas layer, smoke, drifting suppressants, common ventilation systems, common drain systems or flooding. In addition, other interactions between the locations may be possible in unique configurations. If alternate shutdown is provided on the basis of rooms or zones, the provision of fire detection and fixed suppression is only required in the room or zone under consideration. Compliance with Section III.G.2 cannot be based on rooms or zones[16]. While "independence" is clearly achieved where alternative shutdown equipment is outside the fire area under consideration, this is not intended to imply that alternative shutdown equipment in the same fire area but independent of the room or the zone cannot result in compliance with the regulation. The "room" concept must be justified by a detailed fire hazards analysis that demonstrates a single fire will not disable both normal shutdown equipment and the alternative shutdown capability.[17]

The remote shutdown systems recommended under Chapter 7 of the SRP are needed to meet GDC 19. These remote shutdown systems need to be redundant and physically independent of the control room in order to meet GDC 19. For GDC 19, damage to the control room is not considered. Alternate shutdown systems for Appendix R need not be redundant but must be both physically and electrically independent of the control room.[18]

Generic Communications

To aid in developing a common understanding between licensees and NRC reviewers and inspectors, a number of clarification documents have been promulgated by the staff, principally in the form of generic letters and information notices. When considering guidance contained in generic communication documents the following points must be noted:

1. It is the Commission's position that regulatory guidance by itself cannot alter the specific regulatory requirements contained in the Commission's fire protection regulations,[19] and

---

16 Generic Letter 86-10, Enclosure 2, Q 3.1.5

17 Generic Letter 86-10, Enclosure 1, Paragraph 6, "Alternative or Dedicated Shutdown"

18 Generic Letter 86-10, Enclosure 2, Q 5.3.11

19 Letter dated April 6, 2001, from: J. Hannon NRC, to: A. Marion, Nuclear Energy Institute; Subject: Adoption of NFPA Standard 805

2. NRC generic letters legally cannot create a new requirement for a specific course of action to resolve an issue. Generic communications have been used, however, to provide new or clarified interpretations of existing requirements.[20]

Salient generic communications related to post-fire safe shutdown capability are summarized in the table below.

Generic Communication Document	Description
Generic Letter 77-002	Provided supplemental guidance to Appendix A BTP 9.5-1 regarding a licensee's fire protection organization, training of the fire brigade, control of combustibles and ignition sources, fire fighting procedures and quality assurance.
Generic Letter 81-12 and Clarification of GL 81-12	In these letters, the staff identified the information necessary to perform their reviews of licensee compliance with the alternative or dedicated shutdown requirements of Section III.G.3 of Appendix R. These letters defined safe shutdown objectives, reactor performance goals, necessary safe shutdown systems and components, and associated circuit identification and analysis methods. Generic Letter 81-12 also requested that technical specifications be developed for safe shutdown equipment that was not already included in the existing plant technical specifications.

[20] Statement submitted by the United States Nuclear Regulatory Commission to the Subcommittee on Clean Air, Wetlands, private property, and nuclear safety committee on environment and public works United States Senate concerning United States Nuclear Regulatory Commission programs and nuclear safety regulatory issues presented by Shirley Ann Jackson, Chairman July 30, 1998

Generic Communication Document	Description
Generic Letter 83-33	Provided the following staff positions on certain requirements of Appendix R to 10 CFR 50: (a) Detection and Automatic Suppression; (b) Fire Areas; (c) Structural Steel Related To Fire Barriers; (d) Fixed Suppression System; (e) Intervening combustibles; (f) Transient Fire Hazards. It should be noted that certain licensee's disagreed with, or found it difficult to implement, the interpretations provided in this Generic Letter. To pursue the matter with senior NRC management industry formed the Nuclear Utility Fire Protection Group. To "...examine all licensing, inspection and technical issues and to make policy recommendations for expediting Appendix R implementation and for assuring consistent levels of fire protection at all plants," by direction of the Executive Director for Operations, the staff formed the Steering Committee on Fire Protection Policy. Disagreements in the implementation of interpretations provided in Generic Letter 83-33 were ultimately resolved by issuance of Generic Letter 86-10, "Implementation of Fire Protection Requirements" on April 24, 1986.

Generic Communication Document	Description
Information Notice 84-09	Provided guidance for conducting analyses and/or making modifications to implement requirements of 10 CFR 50, Appendix R with respect to the following issues: (a) Fire areas; (b) Fire Barrier Testing and Configuration; (c) Protection of Equipment Necessary To Achieve Hot shutdown; (d) Licensee's Reassessment for Conformance with Appendix R; (e) Identification of Safe Shutdown Systems and Components; (f) Combustibility of Electrical Cable Insulation; (g) Detection and Automatic Suppression; (h) Applicability of 10 CFR 50, Appendix R, Section III.L; (i) Instrumentation Necessary for Alternative shutdown; (j) Procedures for Alternative Shutdown Capability; (k) Fire Protection Features for Cold Shutdown Systems; (l) RCP Oil Collection Systems.
Information Notice 85-09	Issued to alert licensee's of potential deficiencies in the electrical design of isolation / transfer switches which do not provide redundant fuses upon transfer.

Generic Communication Document	Description
Generic Letter 86-10	Provides additional guidance on acceptable methods of satisfying NRC regulatory requirements. Although this document was issued by the staff, it had the review and approval of the Commission. Specific topics addressed include: (a) Scheduler Exemptions (b) Documentation Required to Demonstrate Compliance (c) Applicable Quality Assurance Requirements (d) NRC Notification of Deficiencies (e) Incorporation of Fire Protection Program into FSAR (f) Standard Fire Protection License Condition Through the implementation and adoption of a standard license condition, a licensee is allowed to make changes to its fire protection program without prior notification to the NRC in accordance with the provisions of 10 CFR 50.59, provided the changes did not adversely affect the plant's ability to achieve and maintain post-fire safe shutdown. The licensee, upon modification of the license to adopt the standard condition, could also amend the license to remove the fire protection technical specifications. (g) Interpretations of Appendix R: • Process Monitoring Instrumentation • Repair of Cold Shutdown Equipment • Fire Damage • Fire Area Boundaries • Automatic Detection and Suppression • Alternative or Dedicated Shutdown Capability (h) Appendix R Questions and Answers To assist the industry in understanding the NRC's requirements, and improve the staff's understanding of the industry's concerns, a series of workshops were conducted in each NRC Region. This section presents the NRC's position as responses to the questions posed by the industry during these workshops.
Generic Letter 88-12	Provided additional guidance for implementation of the standard license condition and removal of the technical specifications associated with fire detection and suppression, fire barriers, and fire brigade staffing. The technical specifications associated with safe shutdown equipment and the administrative controls related to fire protection audits were to be retained under the guidance of the generic letter.

Generic Communication Document	Description
Information Notice 99-17	Issued to to alert licensee's to potential problems associated with post-fire safe-shutdown circuit analysis that could could prevent the operation or lead to malfunction of equipment necessary to achieve and maintain post-fire safe shutdown.

4.5 Fire Protection Licensing and Design Basis

With the issuance of the fire protection rule (10 CFR 50.48, and Appendix R to 10 CFR 50), the applicability of certain fire protection requirements, including those within the rule, was established on the basis of the licensing date for a given plant being before or after January 1, 1979. However, the progression of regulatory guidelines and requirements outlined above coupled with a broad range of plant specific attributes (design features, operating preferences, and exemptions to certain technical requirements) has created a unique set of circumstances for nearly each plant. Design and construction factors such as plant type (PWR vs. BWR), age, size, NSSS supplier (Westinghouse, Combustion Engineering, Babcok and Wilcox, GE), architect / engineer, degree of separation provided for redundant shutdown systems in the initial plant design, type of cabling used (e.g., thermoset vs. thermoplastic insulation) and the individual preferences of a utility for system and equipment configurations can significantly influence the type and quantity of fire protection features needed to provide an acceptable level of protection. The influence factors such as these may have on the protection of safe shutdown capability is considered by the staff and documented in plant-specific Safety Evaluation Reports (see below). As a result of these plant-specific differences, fire protection features imposed on one plant may be found to differ considerably from those at another.

Plants Licensed Prior to January 1, 1979

The primary licensing basis for plants licensed to operate prior to January 1, 1979, is comprised of the plant license conditions, Appendix R and any approved exemptions, and the staff's Safety Evaluation Reports (SERs) on the fire protection program.

Plants Licensed After January 1, 1979

Plants licensed after January 1, 1979, are subject to the requirements of 10 CFR 50.48(a) only, and as such must meet the provisions of GDC 3 as specified in their license conditions and as accepted by the NRC in their SERs. These plants are typically reviewed to the guidance of SRP Section 9.5-1. For these plants, where commitments to specific guidelines cannot be met, or alternative approaches are proposed, the differences between the licensee's program and the guidelines are documented in deviations.

Safety Evaluation Reports

Safety Evaluation Reports (SERs) document the staff acceptance of the plant fire protection program or elements thereof. For plants licensed to operate prior to January 1, 1979, the staff's SERs also establish the extent to which the requirements of Appendix R to 10 CFR Part 50 apply. Plants whose fire protection features were accepted by the NRC as satisfying the provisions of Appendix A to Branch Technical Position (BTP) APCSB 9.5-1, or were accepted in comprehensive SERs issued prior to publication of Appendix A to BTP APCSB 9.5-1 in August 1976, were only required to meet the provisions of Sections III.G (III.L), III.J, and III.O of Appendix R.

Exemptions and Deviations

When it promulgated Appendix R, the Commission recognized that there would be plant conditions and configurations where strict compliance with specified fire protection design features would not

significantly enhance the level of fire safety already provided by the licensee. Therefore, in cases where a fire hazard analysis could adequately demonstrate that alternative fire protection features provided an equivalent level of fire safety to that required by the regulation the licensee could apply for an exemption from the prescriptive requirements of Appendix R. Thus, the exemption process provided a means of allowing flexibility to meet the performance objectives of Appendix R through alternative means. For plants that began operation after January 1, 1979, guidance for the plants' fire protection programs is provided in Branch Technical Position (BTP) CMEB 9.5-1. For these newer plants, the staff approved "deviations" from the guidance during the licensing process. Since Appendix R requirements are included in BTP CMEB 9.5-1, this report uses the term "exemptions" to refer to both BTP CMEB 9.5-1 deviations as well as Appendix R exemptions.

Through the performance of a detailed fire hazards analysis of plant-specific conditions a licensee may demonstrate that certain configurations which do not meet the technical requirements of the regulation will provide an adequate level of fire safety. For example, the evaluation of a fire area at a certain plant may find that although redundant shutdown components are adequately separated (>20 feet of horizontal separation) the area between the components contains a small quantity of intervening combustibles in the form of cables routed in cable trays. Although this configuration does not satisfy the technical requirements of the rule (which specifies that the separation area be free of intervening combustibles or fire hazards), when other protection features are considered (such as the use of armored sheathed cables, adequacy of installed fire detection systems, automatic and manual suppression capabilities and the quantity ant type of combustibles in the area), it may be shown that strict compliance with the technical requirements would not enhance fire safety. When plant-specific conditions such as this are encountered, licensee's may request NRC approval of an exemption from technical requirements of the regulation under 10 CFR 50.12. Under this provision, the Commission may grant exemptions from the requirements of the regulations in 10 CFR Part 50, which are:

1. Authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security.
2. The Commission will not consider granting an exemption unless special circumstances are present. Special circumstances are present whenever:
    - Application of the regulation in the particular circumstances conflicts with other rules or requirements of the Commission; or
    - Application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule; or
    - Compliance would result in undue hardship or other costs that are significantly in excess of those contemplated when the regulation was

adopted, or that are significantly in excess of those incurred by others similarly situated; or

- The exemption would result in benefit to the public health and safety that compensates for any decrease in safety that may result from the grant of the exemption; or

- The exemption would provide only temporary relief from the applicable regulation and the licensee or applicant has made good faith efforts to comply with the regulation; or

- There is present any other material circumstance not considered when the regulation was adopted for which it would be in the public interest to grant an exemption. If such condition is relied on exclusively for satisfying criteria (2) above, the exemption may not be granted until the Executive Director for Operations has consulted with the Commission.

As stated previously, plants licensed after January 1, 1979 have fire protection programs that were typically reviewed and approved under the guidance contained in NUREG-0800, SRP Section 9.5.1, and therefore, are not subject to the specific regulatory requirements of 10 CFR 50.48 and Appendix R. For these plants, a license amendment, or NRC staff approval of a deviation from a specific NRC guideline, is necessary when an alternate approach is used to satisfy the requirements of GDC 3. As with an exemption, however, the licensee must submit a sound technical justification for the alternate approach for NRC review and approval, along with its license amendment or deviation request.

Standard Plant License Condition

Most operating plant licenses contain a section on fire protection. License conditions for plants licensed prior to January 1, 1979, typically contain a condition requiring implementation of modifications committed to by the licensee as a result of the fire protection program review with respect to the branch technical position. These license conditions were added by amendments issued between 1977 and February 17, 1981, the effective date of 10 CFR 50.48 and Appendix R. As a result of numerous compliance, inspection, and enforcement issues associated with the various plant license conditions, the staff developed a standard licensing condition. The standard license condition, and the NRC's recommendation that it be adopted by licensees, was transmitted to licensees in Generic Letter 86-10 (see below). Additional guidance regarding removal of the fire protection requirements from the plant technical specifications was provided to licensees in Generic Letter 88-12. The changes were promulgated to provide licensees greater flexibility in the management and implementation of the fire protection program and to clarify the fire protection licensing basis for the specific facility.

If the licensee has adopted the standard license condition and incorporated the fire protection program in the FSAR, the licensee may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire as documented in a safety evaluation. In addition to planned changes, a safety evaluation may also be required for nonconforming conditions. Generic Letter 86-10 recommended that licensees incorporate the fire protection program in the facility Final Safety Analysis Report (FSAR). Incorporation of the fire protection program and major commitments, including the fire hazards analysis, by reference into the FSAR for the facility places the fire protection program, including the systems, the administrative and technical controls, the organization, and other plant features associated with fire protection on a consistent status with other plant features described in the FSAR. Generic Letter 86-10 further recommended the adoption of the standard license condition, requiring licensees to comply with the provisions of the approved fire protection program as described in the FSAR and establishing when NRC approval for changes to the program is required. The licensee should maintain, in auditable form, a current record of all such changes, including an analysis of the effects of the change on the fire protection program, and should make such records available to NRC Inspectors upon request. All changes to the approved program should be reported, along with the FSAR revisions required by 10 CFR 50.71(e).

If the fire protection program committed to by the licensee is required by a specific license condition and is not part of the FSAR for the facility, licensees may be required to submit amendment requests even for relatively minor changes to the fire protection program.

The standard license condition for fire protection was transmitted to licensees in April 1986 as part of Generic Letter 86-10 with information on its applicability to specific plants. The standard license condition reads as follows:

> Fire Protection
>
> (Name of Licensee) shall implement and maintain in effect all provisions of the approved fire protection program as described in the Final Safety Analysis Report for the facility (or as described in submittals dated ----------) and as approved in the SER dated ---------- (and Supplements dated ---------) subject to the following provision:
>
> The licensee may make changes to the approved fire protection program without prior approval of the Commission only if those changes would not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire.

The adoption of the standard license condition in conjunction with the incorporation of the fire protection program in the FSAR for the facility provides a more consistent approach to evaluating changes to the facility, including those associated with the fire protection program.

Within the context of the standard fire protection license condition, the phrase "not adversely affect the ability to achieve and maintain safe shutdown in the event of a fire," means to maintain sufficient safety margins. See Regulatory Guide 1.174 for additional information.

If a proposed change involves a change to a license condition or technical specification that was used to satisfy NRC requirements, a license amendment request should be submitted. When a change that falls within the scope of the changes allowed under the standard fire protection license condition is planned, the evaluation is made in conformance with the standard fire protection license condition to determine whether the change would adversely affect the ability to achieve and maintain safe shutdown. The assessment should include the effect on the fire hazard analysis and the consideration of whether circuits or components, including associated circuits, for a success path of equipment needed for safe shutdown are being affected or a new element introduced in the area. If this evaluation concludes that there is no adverse affect, this conclusion and its basis should be documented and be available for future inspection and reference. If the evaluation finds that there is an adverse affect, or that it is outside the basis for an exemption (or deviation) that was granted (or approved) for the area involved, the licensee should make modifications to achieve conformance, justify and request an exemption, or seek a license amendment from the NRC.

5. Post-Fire Safe Shutdown Capability

5.1 Objective

The purpose of a reactor plant fire protection program is to prevent fires and to ensure the capability to shutdown the reactor and to minimize radioactive releases to the environment in the event a fire were to occur. The underlying purpose of regulatory requirements and staff guidance promulgated since the Browns Ferry fire is to ensure that in the event of fire in any area of the plant, one train of equipment used to achieve and maintain safe shutdown conditions in the reactor will remain free of fire damage.

Redundancy is a fundamental safety feature incorporated into the design of all commercial nuclear power plants operating in the U.S.. Separation of the redundant subsystems is typically accomplished by dividing safety equipment and cables into redundant divisions. The provision of separate and redundant divisions of safety systems provides confidence that the failure of components or cables within one division will not adversely affect the plant's ability to accomplish required safety functions. In essence, redundancy ensures that failures affecting one system will not have a significant impact on plant safety because a "back-up" system is provided in the plant design. To a certain extent, this design feature also provides a measure of safety against the possible consequences of fire. The level of confidence achieved through redundancy, however, is highly dependent on the degree of separation and independence provided for the redundant elements. In the absence of suitable separation distance or other protection features, redundant trains of cables and equipment could be susceptible to a phenomenon known as "common-mode" failure, where multiple failures in redundant systems may occur as a result of a common cause[21]. If a single event could induce failures in more than one of the redundant elements, the safety and reliability benefits afforded by this design feature could be negated. As demonstrated by the equipment perturbations that occurred during the Browns Ferry fire, common-mode failures due to fire may cause equipment to fail and/or interact in ways that are not readily predictable.

The need to fully consider the potential consequences of fire damage to redundant divisions of safety equipment was emphasized by the Special Review Group (SRG) established by the NRC to investigate the Browns Ferry fire event:

> *"The chronicle of the Browns Ferry fire includes many examples of unavailability of redundant equipment. Evidently the independence provided between redundant subsystems and equipment was not sufficient to protect against common mode failures".*

[21] IEEE Std. 100-1988

As discussed in Section 4.2 above, minimizing the potential for fire to cause common-mode failures in redundant divisions of shutdown equipment, is a essential element of the "defense in depth" philosophy for fire protection. Achieving this objective requires plant safety systems to be designed so that in the event a fire should start (in spite of the fire prevention program) and continue to burn for a considerable period of time, the capability of accomplishing safe shutdown functions will not be prevented.

5.2 Fire Damage Limits

Achieving safe shutdown conditions is a sequential process that relies on the operation of various plant systems to accomplish shutdown functions necessary to achieve and maintain both hot and cold shutdown conditions. While certain shutdown functions, such initial reactivity control must be immediately available, other functions, such as long-term decay heat removal, may not be needed for an extended period of time following a reactor trip. This sequential process creates a qualitative hierarchy of fire risk. That is, fire damage to equipment and systems that are needed to perform Hot Shutdown functions (i.e., those needed immediately after a reactor trip), pose a greater threat to safety than damage to equipment whose operation is only needed to achieve and maintain Cold Shutdown (i.e., may not be needed for some time into the event). The need to assure an adequate level of fire protection for systems and equipment needed to perform Hot Shutdown functions was underscored by the Commission in its comments on Appendix R. In its Statements of Considerations on the Fire Protection Rule (SEC -80-438A) the Commission states:

> *"When considering the consequences of a fire in a given fire area, in evaluating the safe shutdown capabilities of the plant, we must be able to conclude that one train of equipment that can be used immediately to bring the reactor to hot shutdown conditions remains unaffected by that fire."*

The relationship between the specific shutdown functions performed (i.e., hot or cold shutdown) and the potential consequences of their failure is acknowledged in the regulation. Specifically, Section I of Appendix R establishes the following fire damage limits based on the safety function of the structure, system or component:

Safety Function of Structure, System or Component	Fire Damage Limit
Hot Shutdown:	One train of equipment necessary to achieve hot shutdown from the control room or emergency control station(s) must be maintained free of fire damage by a single fire, including an exposure fire.
Cold Shutdown:	Both trains of equipment necessary to achieve cold shutdown may be damaged by a single fire, but damage must be limited so that at least one train can be repaired or made operable within 72 hours using onsite capabilities.
Design Basis Accident:	Both trains of equipment necessary for mitigation of consequences following design basis accidents may be damaged by a single exposure fire.

Additionally, Paragraph 50.48(b) of 10 CFR 50, requires all licensed nuclear power plants operating prior to January 1, 1979 to meet the requirements of Sections III.G, "Fire Protection of Safe Shutdown Capability," of Appendix R to 10 CFR 50, regardless of any previous approvals by the NRC for other design features. Compliance with this criterion requires each licensee to demonstrate that in the event of an exposure fire in any single area of the plant, one of the redundant trains of cables and equipment necessary to achieve and maintain hot shutdown conditions will remain free of fire damage. Although hot shutdown equipment must remain free of fire damage, equipment required to achieve and maintain cold shutdown may be damaged provided the necessary repairs can be completed within the time restrictions established in the regulation. (*Note:* Facilities that commenced operation on or after January 1, 1979 are subject to essentially the same criteria as those contained in Appendix R which have been imposed through license conditions or through licensing commitments).

It should also be noted that not all safety class equipment requires the same level of protection from fire. Structures, systems and components (SS&C) that are only used to mitigate the consequences of design basis accidents do not require the same level of fire protection as those needed to accomplish post-fire safe shutdown. The basis for this position is provided in, Section I, Introduction and Scope, of Appendix R to 10 CFR 50:

> *"Because fire may affect safe shutdown systems and because the loss of function of systems used to mitigate the consequences of design basis accidents under post fire conditions does not per se impact public safety, the need to limit fire damage to systems required to achieve and maintain safe shutdown conditions is greater than the need to limit fire damage to those systems required to mitigate the consequences of design basis accidents."*

5.3 Evaluation Process Overview

Assuring the ability of achieve and maintain safe shutdown conditions in the event of fire, requires a comprehensive assessment of the potential effects of fire and its related perils (direct flame impingement, hot gases, smoke migration, fire fighting water damage, etc.) in each fire area. The overall objective of this evaluation, which is frequently referred to as a "Safe Shutdown Analysis" or "SSA" is to identify potential fire vulnerabilities and develop protection measures that are consistent with established requirements.(e.g., Section III.G of Appendix R). This is a technically complex process, involving personnel having expertise in fire protection, plant operations, electrical engineering and mechanical systems engineering disciplines.

Information developed during performance of the Fire Hazards Analysis (FHA) provides the initial input for the SSA. For example, in addition to identifying the plant fire areas, the FHA will contain important information related to fire barrier ratings, equipment locations, fire detection and suppression capabilities, etc. This information is then supplemented by facility design and engineering data, additional analysis and studies, and data developed by direct observation or walk-down of facility spaces and systems.

Each facility performing a fire SSA designs or specifies the analysis methodology to be used. Although differences in plant design have resulted in many variations in plant-specific approaches, the overall process remains fairly consistent between plants. As illustrated in Figure 5.1 below, the determination of post-fire safe shutdown capability will typically include two principal assessments, a "Systems Analysis" and a "Fire Area Analysis." As part of the systems analysis, required shutdown functions are defined and redundant trains or "paths"of plant systems capable of accomplishing each of these functions are identified. Equipment, cables, and circuits needed to assure the operation of these systems or whose damage due to fire may adversely affect the shutdown capability are then determined. Once the equipment and cabling needed to assure safe shutdown is identified, their physical location (by fire area) may be determined. A "Fire Area Analysis"is then performed to assess the potential consequences a postulated fire in each fire area

may have on the plant's ability to achieve and maintain safe shutdown conditions. An overview o this process is illustrated in Figure 5.1 below. Refer to Section 6 for a more detailed discussion of this process.

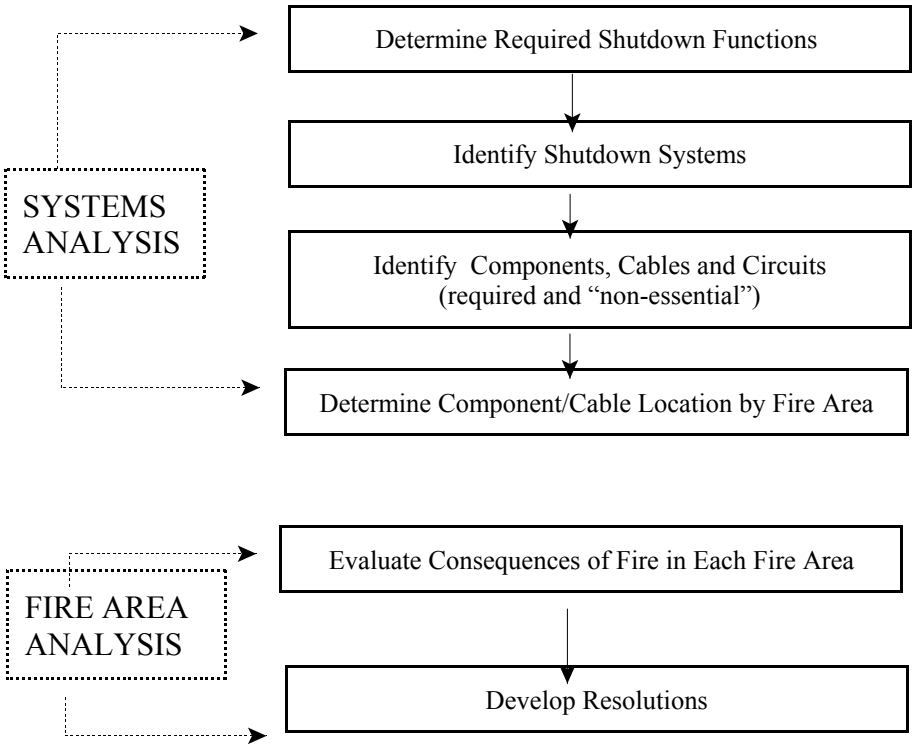


Figure 5-1 Overview of Safe Shutdown Evaluation Process

Because the SSA will be based on large quantities of information and data, computer programs are frequently used to sort, manage, and analyze the information necessary develop a safe shutdown capability for the facility.

Conducting a SSA is an iterative process. As changes to the SSA data base are implemented and facility modification are installed, additional analysis must be performed to demonstrate that the changes have not compromised the previous analysis.

5.4 Analysis Assumptions

The following set of fundamental principles and assumptions establish the "ground rules" for performing acceptable SSA:

Fire Hazards Analysis

It is assumed that a Fire Hazards Analysis (FHA) has been performed by qualified individuals which divides the plant into distinct fire areas and identifies fire hazards and major equipment located within each of those areas.

Shutdown Functions, Systems and Equipment

The systems and equipment needed for post-fire safe shutdown are those systems necessary to perform the shutdown functions defined in Section III. L of Appendix R. These functions are reactivity control, reactor coolant makeup, reactor heat removal, process monitoring, and associated support functions. The acceptance criterion for systems performing these functions is also defined in Section III. L:

> *During the post-fire shutdown, the reactor coolant system process variables shall be maintained within those predicted for a loss of normal a.c. power, and the fission product boundary integrity shall not be affected; i.e., there shall be no fuel clad damage, rupture of any primary coolant boundary, or rupture of the containment boundary*.

These guidelines apply to the systems needed to satisfy both Section III.G and III.L of Appendix R.[22]

[22] NRC Information Notice 84-09, 2/13/84, Section V, p. 4

Exposure Fire

The evaluation of safe shutdown capability is based on the occurrence of a single *exposure fire* in an area containing (or presenting a fire hazard to) components, equipment or cabling relied on for post-fire safe shutdown. An exposure fire is defined as a fire in a given area that involves either in situ (permanently installed) or transient combustibles, but is external to any structures, systems, or components (SSC) located (or adjacent to) that same area. The effects of such fire (e.g., heat, smoke, or ignition) can adversely affect SSC 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 either redundant train may constitute an exposure fire to both redundant trains located in the same fire area. Each fire area must be analyzed for the effects of an exposure fire.

Damage Expectations

In general, all cables and equipment that are exposed to the effects of fire (i.e., do not meet protection criteria of Appendix R Section III.G.2) should be assumed to experience damage unless a plant-specific exemption to these requirements has been reviewed and approved by the staff. Credit can not be taken for fire to cause a loss of function if such a loss would serve to simplify the shutdown scenario. For example, assuming that fire causes a loss of offsite power may be non-conservative.

Cause of Failures

The only failures considered are those that are directly attributable to the fire and/or fire suppression activities. No other failures or independent events are assumed to occur concurrently with the fire.

Availability of Shutdown Systems

At the onset of the postulated fire all safe shutdown systems (including applicable redundant trains) are assumed operable and available for post-fire safe shutdown. Systems are assumed to be operational with no repairs, maintenance, testing LCOs etc. in progress. The unit is assumed to be operating at full (100%) power under normal conditions and normal lineups with a 3-month 100% power history.

Use of Low Pressure Injection Systems at BWRs

The use of safety-relief valves (SRVs) in conjunction with low-pressure injection systems (LPS) meets the requirements of a redundant means of post-fire safe shutdown under Section III.G.2 of 10CFR Part 50, Appendix R. When this methodology (SRV/LPS) is employed,

the shutdown performance criteria identified in Section III.L do not apply. Rather, licensees who designate SRV/LPS as a redundant means of post-fire safe shutdown must show that SRV/LPS can achieve and maintain hot shutdown in accordance with Sections III.G.1 and III.G.2 of Appendix R.[23]

Availability of Off-site and On-site Power Sources

For the case of redundant shutdown, offsite power may be credited if demonstrated to be free of fire damage. 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.

Safety Class of Shutdown Systems

For redundant train shutdown, equipment comprising one of the normal means of accomplishing shutdown functions will be assured to remain available (Ref: GL 86-10). For alternate shutdown capability, safe shutdown systems can be either safety related or non-safety related.

Multiple Unit Sites

Unrelated fires in two or more units are not postulated to occur simultaneously. However, where a single fire can impact more than one unit of a multi-unit site, the ability to achieve and maintain safe shutdown conditions in each of the affected units must be demonstrated.

Automatic Equipment Operation

Automatic equipment operation may or may not occur during a fire. Credit can not be taken for fire to cause a loss of automatic functions if such a loss would serve to simplify the alternative shutdown scenario. For fire areas requiring alternative shutdown capability the "worst case" scenario should be considered. For other fire areas, automatic operation of components and logic circuits may be credited in the analysis if the circuitry associated with

[23] Letter from S. Richards (NRC) to J. Kenny (BWROG), December 12, 2000

the automatic operation is demonstrated to remain unaffected by the postulated fire (i.e., satisfies established fire protection/separation criteria).

Relay/Switch Contact Positions

All relay, position switch, and control switch contacts in control circuits are in the position or status that correspond to the normal operation of the device. Test and transfer switches in control circuits are in their normal position.

Repairs

Repair activities (e.g., wiring changes, fuse replacement, use of pneumatic or electric jumpers or other modifications) are not permitted for systems required to achieve and maintain hot shutdown conditions. Modifications and repair activities are permitted for cold shutdown systems provided: (a) For areas not requiring an alternative shutdown capability it can be demonstrated that all repair activities can be accomplished within 72 hours or, (b) For areas requiring an alternative shutdown capability all needed repairs can be performed and cold shutdown achieved within 72 hours.

Cable and Circuit Failure Modes

It is not deemed possible to accurately predict the manner in which damaged cables or circuits may fail. Various types of electrical failure modes (e.g., hot-shorts, open circuits, or shorts to ground) must be assumed to occur as a result of fire damage.

Manual Actions

The use of manual operator actions does not satisfy regulatory requirements governing the protection of hot shutdown systems and equipment (i.e., Section III.G.2 of Appendix R). See Section 5.5 below.

Single Failure Criterion

Because it is only one of several levels of defense, the shutdown capability does not have to meet the single failure criterion.

Redundant vs. Alternative Shutdown Systems and Equipment

For the purpose of analysis to Section III.G.2 criteria (i.e., redundant train shutdown capability), the safe shutdown capability is defined as one of the two normal safe shutdown trains. If the system is being used to provide its design function, it generally is considered

redundant. If the system is being used in lieu of the preferred system because the redundant components of the preferred system do not meet the separation criteria of Section III.G.2, the system is considered an alternative shutdown capability (Ref: GL 86-10) .

Post-fire Operating Procedures

The only requirement for post-fire operating procedures is for those areas where alternative shutdown is required. For other areas of the plant, shutdown would be achieved utilizing one of the two normal trains of shutdown system. Shutdown in degraded modes (one train unavailable) should be covered by present operator training and abnormal and emergency operating procedures. If the degraded modes of operation are not presently covered, the operation staff should determine the need for additional training or procedures (Ref: GL 86-10).

5.5 Redundant Shutdown Capability

As experienced during the Browns Ferry fire, SS&C that are exposed to the effects of fire may be damaged, and this damage may lead to unexpected consequences in the operation of plant safety systems. On February 20, 1981 the NRC forwarded Generic Letter 81-12 (GL 81-12). This document restated the regulatory requirement for each licensee to reassess areas of the plant containing cables or equipment, including associated non-safety circuits, of redundant trains of systems necessary to achieve and maintain hot shutdown conditions.

Failing to adequately identify circuits, components, and systems required to achieve and maintain safe shutdown and protect them from the affects of fire could result in damage to redundant trains of shutdown systems and significantly impair the ability to safely shutdown the plant in the event of fire. Consequently, one of the key outcomes of the SSA evaluation process is the identification of plant locations (fire areas) that contain redundant trains of SS&C important to safe shutdown. As described in Section 4.3 above, when redundant trains of cables or equipment, including associated non-safety circuits necessary to achieve and maintain hot shutdown are found to be located in the same fire area, the fire protection requirements of Section III.G.2 of Appendix R must be satisfied. If not, an *alternative or dedicated shutdown capability* must be provided or an exemption requested if there is some technically justifiable basis.

Areas of the plant that meet the separation requirements of Section III.G.2 are frequently referred to as *"Redundant Shutdown"* fire areas.

5.6 Alternative Shutdown Capability (III.G.3)

In certain areas of the plant redundant trains of equipment required for hot shutdown may be located in close proximity. Typical examples include the Main Control Room and Cable Spreading Room where redundant trains of shutdown equipment may be separated by only a few inches. In cases such as this, compliance with fire protection features specified in Section III.G.2 of Appendix R can not be readily achieved. When areas such these are identified an alternative or dedicated shutdown capability must be provided that is both physically and electrically independent of the area under consideration.

Alternative Shutdown Capability is provided by rerouting, relocating, or modifying existing systems. An example of an alternative shutdown capability would be the case where isolation switches are installed to isolate safety-related circuits from fire damage. Alternative shutdown capability can also be provided by implementation of procedures specifying "alternative" methods of operation such as manual operations and/or evacuation of the normal control station(s) such as the control room.

Dedicated Shutdown Capability is provided by installing new structures and systems for the sole function of post-fire shutdown. Examples of dedicated shutdown capability include installation of emergency generators, process instrumentation, or other equipment which is intended to be used only for safe shutdown purposes (i.e. dedicated to safe shutdown).

The alternative or dedicated shutdown capability may be unique for each area, or it may be one unique combination of systems for all fire areas requiring this capability. For those areas requiring alternative or dedicated shutdown capability, fire detection and a fixed fire suppression system must also be installed in the fire area of concern.

The design basis event for considering the need for alternative or dedicated shutdown capability is a postulated fire in a specific fire area containing redundant safe shutdown cables/equipment in close proximity where it has been determined that fire protection means cannot assure that safe shutdown capability will be preserved. Two cases should be considered:(1) offsite power is available; and (2) offsite power is not available (Ref: GL 86-10) .

The SSA must demonstrate that during a post-fire shutdown reactor coolant process variables will be maintained within those predicted for a loss of normal ac power and the integrity of the fission product boundary will not be affected. That is (a) no fuel clad damage; (b) no rupture of any primary coolant boundary; and (c) no rupture of the containment boundary.

The alternative or dedicated shutdown capability shall be able to achieve and maintain sub-critical conditions in the rector, maintain reactor coolant inventory, achieve and maintain hot standby conditions (hot shutdown for a BWR) for an extended period of time, achieve cold shutdown conditions within 72 hours and maintain cold shutdown conditions thereafter.

Performance goals for the shutdown functions identified in the SSA are as follows:

- 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 decay heat removal.

- The process monitoring function should be capable of providing direct readings of the process variables necessary to perform and control the above functions.

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 for the portions of these systems that interface with or impact existing safety systems.

It should be noted that safe shutdown performance goals and functions to be performed are specified in the regulation (Appendix R Section III.L). However, specific methods for achieving these objectives are left to the individual plants to determine and demonstrate.

Implementation of an alternative or dedicated shutdown capability will require operators to perform many activities at local control stations outside the main control room. All operator activities should be prescribed in abnormal operating procedures which have been integrated into the overall plant operator training and qualification program. As alternative/dedicated shutdown procedures are developed, timely performance of all operator actions in the process must be assured. Verification that time-dependent actions are satisfied in the written procedures is accomplished by performing a thermal hydraulic timeline analysis where various types of transients are analyzed to determine how much time the operating crew has to implement each of the safe shutdown functions before exceeding the established performance criteria. These transients may involve a fire induced spurious equipment operation or the generation of a false signal, with an assumed concurrent loss of offsite power. It should be noted that the spurious operation or false signal generation is not limited to safe shutdown equipment. Non-safe shutdown equipment has to be included, since electrical cables for this equipment may also be routed through the area containing the fire and could be subject to fire damage. Therefore, the single worst-case spurious operation or signal could involve this equipment. Typical examples include the loss of main feedwater in a PWR or inadvertent opening of the turbine bypass valves in a BWR that could cause over-pressurization of the main condenser due to loss of circulating water (The loss of circulating water would be due to the concurrent loss of offsite power). In summary, this analysis and verification will include:

- Confirmation that the procedural steps or actions can be performed by verifying that operators will have access to required equipment
- Confirmation that the analysis criteria are satisfied. For example, the performance of time sensitive steps within allotted times (derived from the results of the plant's thermal-hydraulic analysis)
- Confirmation that required support equipment such as ladders and valve handles are available (pre-positioned and administratively controlled) for use when needed

Other alternative/dedicated shutdown implementation considerations include:

- Confirmation that the minimum shift complement of operators, exclusive of operators that are part of the fire brigade, is adequate to properly implement the safe shutdown procedures.

- Job performance measures covering the major tasks in the post-fire safe shutdown procedures have been integrated into the overall plant operator training and qualification program.

- Emergency Lighting - Because alternative/dedicated shutdown procedures frequently require the performance of manual operator actions throughout the plant, the availability and adequacy of emergency lighting must be confirmed. Section III.J of Appendix R requires that fixed emergency lighting units be provided for locations in the plant associated with post-fire safe shutdown implementation, including the ingress and egress routes of the operators to those locations. C

- Communications - Most alternative and dedicated shutdown strategies rely heavily on the operators ability to confirm/verify the operation of plant equipment and then report this information back to another operator stationed at central location (typically the Remote Shutdown Panel). The communication system relied on to assure this capability provides a vital shutdown support function. In addition to remaining free of fire damage, the designated method of communications should not be affected by a loss of offsite power, interfere with any in-plant instrumentation, or have dead zones in areas where communications is vital to the shutdown process.

5.7 Specific Considerations

5.7.1 Manual Operator Actions

In the early 1990's significant performance deficiencies began to be identified with Thermo-lag fire protective material. At that time, this material was used extensively by industry to meet the protection requirements specified in Section III.G.2 of Appendix R for cable trays, conduits and other enclosures containing circuits required to achieve and maintain hot shutdown conditions. During the subsequent Thermo-lag resolution process, licensee's attempted to minimize the use of this material by re-analyzing their plants and developing alternate protection strategies. While many approaches, such as cable rerouting, use of different equipment, or using fire-protective barriers of

different material are clearly acceptable, the use of manual operator actions does not provide prima-facie evidence of equivalency to the level of fire protection required by the regulation (i.e., a required barrier).

As discussed in Section 5.6 above, manual actions are permitted to accomplish Alternative Shutdown in accordance with Appendix R Section III.G.3, provided the required actions are incorporated into post-fire operating procedures, verified to be physically possible, capable of being performed within the time constraints defined by a thermal-hydraulic analysis developed for the specific shutdown scenario (e.g., fire in control room with one worst-case spurious actuation), and sufficient staffing, communications and emergency lighting are assured to remain available.

In recent inspections, the teams have noted that licensee's are using manual actions to accomplish shutdown in redundant shutdown areas. Licensee representatives state that this is because Generic Letter 86-10 defines free of fire damage as "capable of performing its intended function". Thus, by this definition they consider that manual actions at a remote location will satisfy Appendix R Section III.G.1 requirement that one train is "free of fire damage". This interpretation does not meet the requirements of Section III.G.2 which specifies barrier or spatial separation between redundant trains to prevent maloperations from occurring. Section III.G.2 does not permit the use of a manual action to recover from or to prevent a maloperation. Indeed, a reading of the GL 86-10 paragraph in its entirety would read that an exemption was required for a licensee to not meet the III.G.2 criteria.

Since human performance typically has some associated failure probability, replacing a passive, rated, fire barrier or an automatic suppression system with manual operator actions would appear to increase risk. For some simple actions, the risk increase associated with human performance may be minimal and thus meet the requirements of 10 CFR 50.12 to satisfy the underlying purpose of the rule. For other actions, however, risk may be significantly increased. NFPA 805, also notes that where manual operator actions are relied on to provide the primary means of recovery in lieu of providing fire protection features, risk may be increased The increased risk associated with manual operator actions is also recognized in NFPA 805, "Fire Protection for Light Water Reactor Electrica Generating Plants"2001 Edition, which states that where recovery actions are used in lieu of protection risk can be increased.

It should be noted that the regulation (10 CFR 50.48 and Appendix R) does not forbid the use of manual operator actions. Specific examples of acceptable manual actions include:

- The operation of equipment for which cables are located in fire areas that meet Section III.G.1of Appendix R where cables, equipment and associated non-safety circuits relied on for post-fire safe shutdown are located in a different fire area. One example of a III.G.1-compliant fire area, is one that contains only the cables, equipment, and associated circuits

for only one of the redundant trains of shutdown equipment. Since the cables and equipment for the other (redundant) train are located in a different fire area they would remain unaffected by a postulated fire. Since Appendix R did not require protection of automatic functioning of systems, manual actions may be taken in this case to operate the unaffected train of equipment from the control room or emergency control station(s). However If redundant fire protection safe shutdown cables or equipment are in the same fire area, the requirements of Section III.G.2 or III.G.3 are applicable.

- Staff-approved deviations and exemptions for specific manual actions in lieu of meeting the criteria of Section III.G.2 of Appendix R to 10 CFR Part 50

- Manual operation of equipment used to meet the requirements of Section III.G.3 for Alternative or Dedicated Shutdown of Appendix R to 10 CFR Part 50.

- Manipulation of controls within the control room

- Operation of switches and manually operated valves that are manipulated during a normal shutdown sequence

In summary, the use of manual actions does not satisfy the technical requirements of Section III.G.2 of Appendix R. In certain cases manual actions have been reviewed and approved by the staff, on a plant-specific basis. These approvals are documented in plant-specific Safety Evaluations (SEs) and incorporated into the plants fire protection licensing basis. One example is an exemption granted to Alabama Power Company for the Joseph M. Farley Nuclear Plant, dated November 19, 1985 (NUDOCS Accession No. 8512060395).

Where the use of manual actions has been previously approved by the staff, inspection teams are expected to verify that they can be safely and effectively performed in a sufficiently timely manner to facilitate the accomplishment of required shutdown functions.

Factors to be considered when determining the acceptability of manual operator actions include:

- The number and complexity of manual operator actions with respect to minimum shift staffing levels, operator training, and safe shutdown time constraints

- The effects of fire (e.g., heat, suppression system discharge, products of combustion, etc.) on personnel performance

- Habitability - The effects of environmental factors (e.g., temperature, humidity, etc.) on personnel performance

- Location of actions (No actions are required to be performed in the fire affected area)

- Access and egress (Operators are not required to traverse a fire affected area)

- Accessability of equipment requiring manual manipulation

- Feasibility of performing the specified actions - operator can physically perform the action specified using normal effort

- Availability and adequacy of fixed emergency lighting units and communications systems

- All actions can be completed within time constraints established in the SSA to support required shutdown functions (i.e., operator action time-line).

- The time available to travel to each location and perform all specified actions has been verified by walk-through assessments performed by the plant operations staff

- Manual actions do not include repair activities needed to achieve and maintain hot shutdown conditions

- Required support equipment such as ladders and valve handles are available (pre-positioned and administratively controlled) for use when needed

- For cases where, manual actions are relied on to mitigate the effects of fire damage, sufficient diagnostic instrumentation has been assured to remain available to ensure activity was successful.

Additional guidance is provided in Appendix A of this document.

5.7.2 Repairs

Section III.G.1 of Appendix R states that one train of systems needed for hot shutdown must be free of fire damage. Thus, one train of systems needed for hot shutdown must be operable during and following a fire. Operability of the hot shutdown systems, including the ability to overcome a fire or fire suppressant induced maloperation of hot shutdown equipment and the plant's power distribution system, must exist without repairs. In general, fuse removal for the purpose of preventing the mal-operation of equipment is not considered a repair provided the action is routine and can be performed in a manner that does not subject the operator to an undue safety hazard (e.g., reaching in an energized 4kV switchgear). However, the replacement of fuses is considered a repair.

Repairs for cold shutdown systems are allowed. However, the time requirements for completing repairs is dependent on the shutdown method employed. For areas provided with an alternative or dedicated shutdown capability, Section III.L.5 of Appendix R states that,*"equipment and systems comprising the means to achieve and maintain cold shutdown conditions shall not be damaged by fire; or the fire damage to such equipment and systems shall be limited so that the systems can be made operable and cold shutdown can be achieved within 72 hours."* This time limit should not to be confused with the requirements for completing repairs for areas that do not require an alternative shutdown capability. For these areas, Section III.G.1.b requires only the capability to repair the systems necessary to achieve and maintain cold shutdown from either the control room or emergency control station(s) within 72 hours, not the capability to repair and achieve cold shutdown within 72 hours as required for the alternative or dedicated shutdown modes by Section III.L.

Procedures for repairing damaged cold-shutdown equipment should be prepared in advance with replacement equipment stored onsite.

All repairs should be of sufficient quality to assure safe operation until the plant is restored to an operating condition.

5.7.3 Diagnostic Instrumentation

Certain post-fire shutdown strategies rely on the operator to take mitigating actions in response to fire-induced mal-operations of equipment. For example, the spurious opening of a discharge valve of a required water storage tank may be detected by level instrumentation and then defeated by

manual operator actions to close the affected valve. Since the success of this approach is largely dependent on the operator's ability to "detect" the maloperation, instrumentation relied on to provide this capability must be identified on the Safe Shutdown Equipment List and assured remain free of fire damage (i.e., meet Appendix III.G.2 separation criteria). This type of instrumentation is known as "diagnostic instrumentation." As stated in Generic Letter 86-10, "diagnostic instrumentation" is instrumentation, beyond that identified in Attachment 1 to I&E Information Notice 84-09, needed to assure proper actuation and functioning of safe shutdown equipment and support equipment (e.g., flow rate, pump discharge pressure). The specific diagnostic instrumentation needed depends on the design of the shutdown capability. When the shutdown strategy relies on the use of procedures to direct operator actions in response to equipment upsets that may occur as a result of fire, sufficient diagnostic instrumentation must be assured to remain available (i.e., free of fire damage) so that the success of operator activities can be readily confirmed.

6. Deterministic Analysis Process For Appendix R Compliance

The Brown's Ferry event was of sufficient significance to warrant major changes in fire protection design features of a nuclear power plant. On February 17, 1981 10 CFR50.48 and its attachment, Appendix R to 10 CFR 50 became effective. One of the key demands of this regulation was to backfit all nuclear power plants licensed to operate prior to January 1, 1979 to meet the requirements of Sections III.G, "Fire Protection of Safe Shutdown Capability" which, as described in Section 4, establishes minimum acceptable fire protection design features necessary for assuring that safe shutdown can be attained in the event of fire in any area of the plant. The fundamental objective of this section of the regulation is to extend the concept of defense-in-depth to fire safety by obtaining reasonable assurance that in the event a fire were to start (in spite of fire prevention measures) and continue to propagate (in spite of fire suppression features), one train of structures, systems and components (SSC) needed to achieve and maintain safe shutdown conditions will remain available. An example of how fire damage to cables (circuits) may adversely affect the shutdown capability is illustrated below in Figure 6.1

Compliance with 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 structures, system and components (SSC) whose failure (or mal-operation) 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 an approved exemption). For locations of the plant where compliance with 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 cable spreading room), Section III.G.3 requires an alternative or dedicated shutdown capability be provided that is independent (both physically and electrically) from the fire area under consideration. For either case, 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 which will be depended upon to perform essential shutdown functions must be identified in the safe shutdown analysis (SSA) for the plant. Any circuits or cables in the fire area which could: (a) adversely affect the operability of identified shutdown systems and equipment or (b) 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, must be evaluated and such disabling conditions must be prevented or appropriately mitigated. Otherwise, reliance on the identified safe shutdown equipment can not be ensured. Since 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 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. In summary, such evaluations are expected to be based on the following deterministic premise:

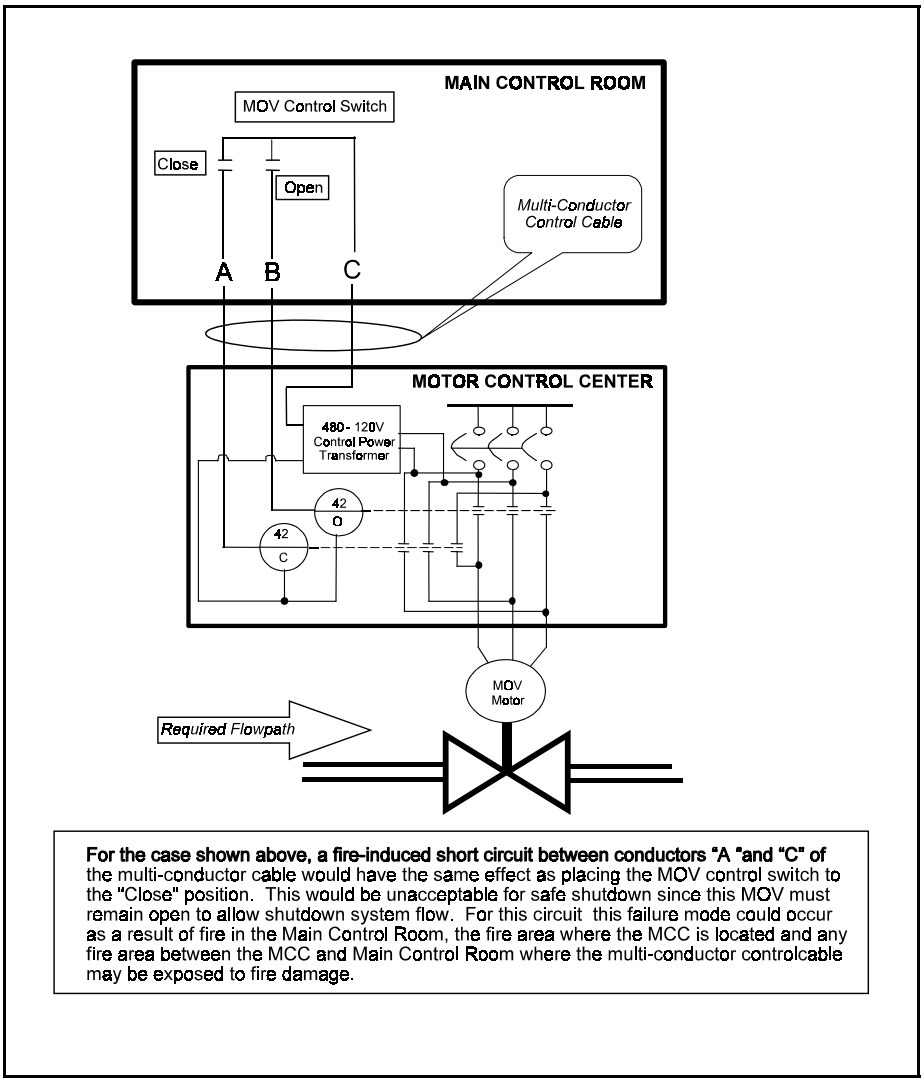


Figure 6.1 Potential Effect of a Fire-induced Circuit Failure

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.

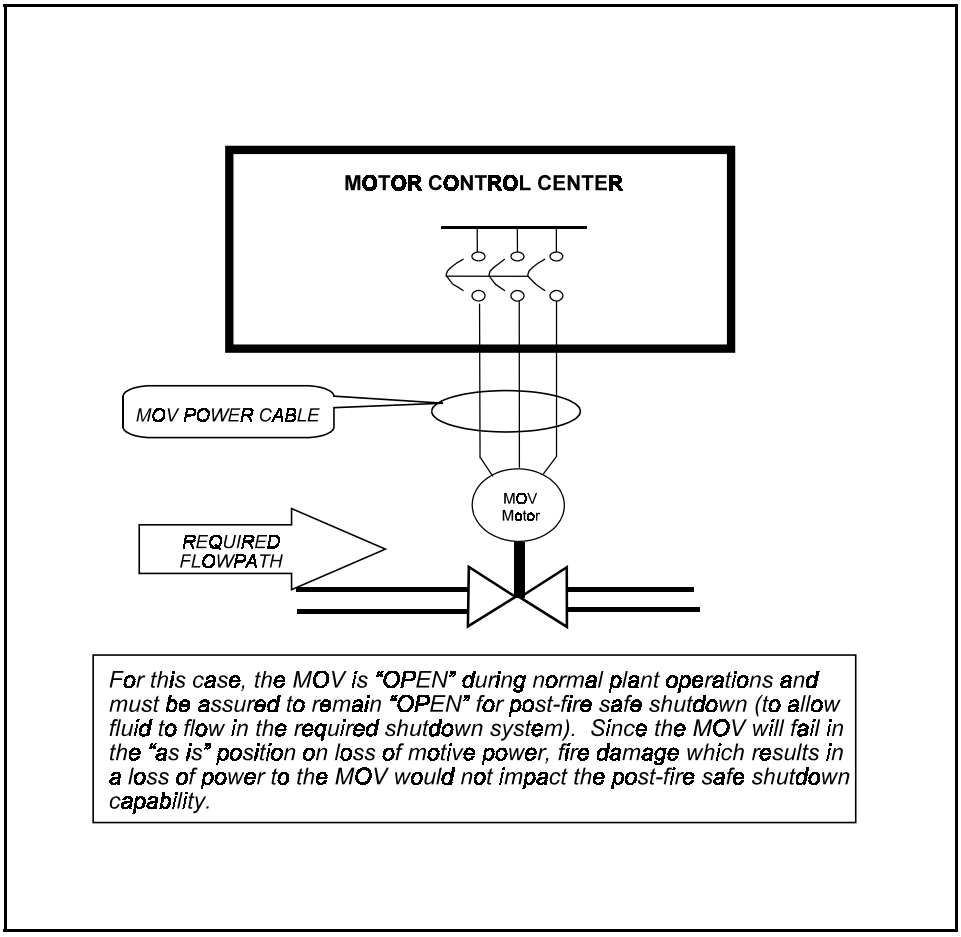


Figure 6.2 Fire Damage to Certain Circuits of Required Shutdown Equipment May Not Pose a Threat to the Shutdown Capability

It is important to recognize that not all circuit (cable) failures that may occur as a result of fire will necessarily have an adverse impact 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 nuclear power station are composed of a diverse array of electrical circuits (cables), and fire damage to many (if not most) of these circuits will not have any 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 analyses 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 since 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. In this case, a motor-operated valve is open during normal plant operations. To assure the successful accomplishment of safe shutdown conditions, the MOV must remain open to allow fluid to flow through the desired 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 an equivalent level of safety 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 by the staff in its clarification of Generic Letter 81-12: *"Our interest is only with those circuits (cables) whose fire-induced failure could affect shutdown."*

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 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 since the guidelines contained in SRP 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 language is not intended to infer 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 post-fire safe shutdown capability of plants licensed after this date was typically reviewed by the staff during the initial licensing process for conformance to guidelines contained in Position C.5.b of SRP 9.5.1 .

6.1 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 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 safe shutdown analysis (SSA), and the NRC does not prescribe or endorse any one specific approach. The SSA should be a bounding analysis which identifies the range of possible fire impacts within each fire area and assures 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 will define a 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 assure that each system will be capable of accomplishing its intended shutdown function.

Because the approach used by a particular plant operating organization will vary in response to plant specific conditions such as design, construction, cable configuration, equipment lay-out and operating preferences, it is not possible (or necessarily prudent) 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 assuring the availability of at least one shutdown *"success path"* (i.e., the minimum set of structures, systems, and components 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. An overview of this approach is depicted in Figure 6.3.

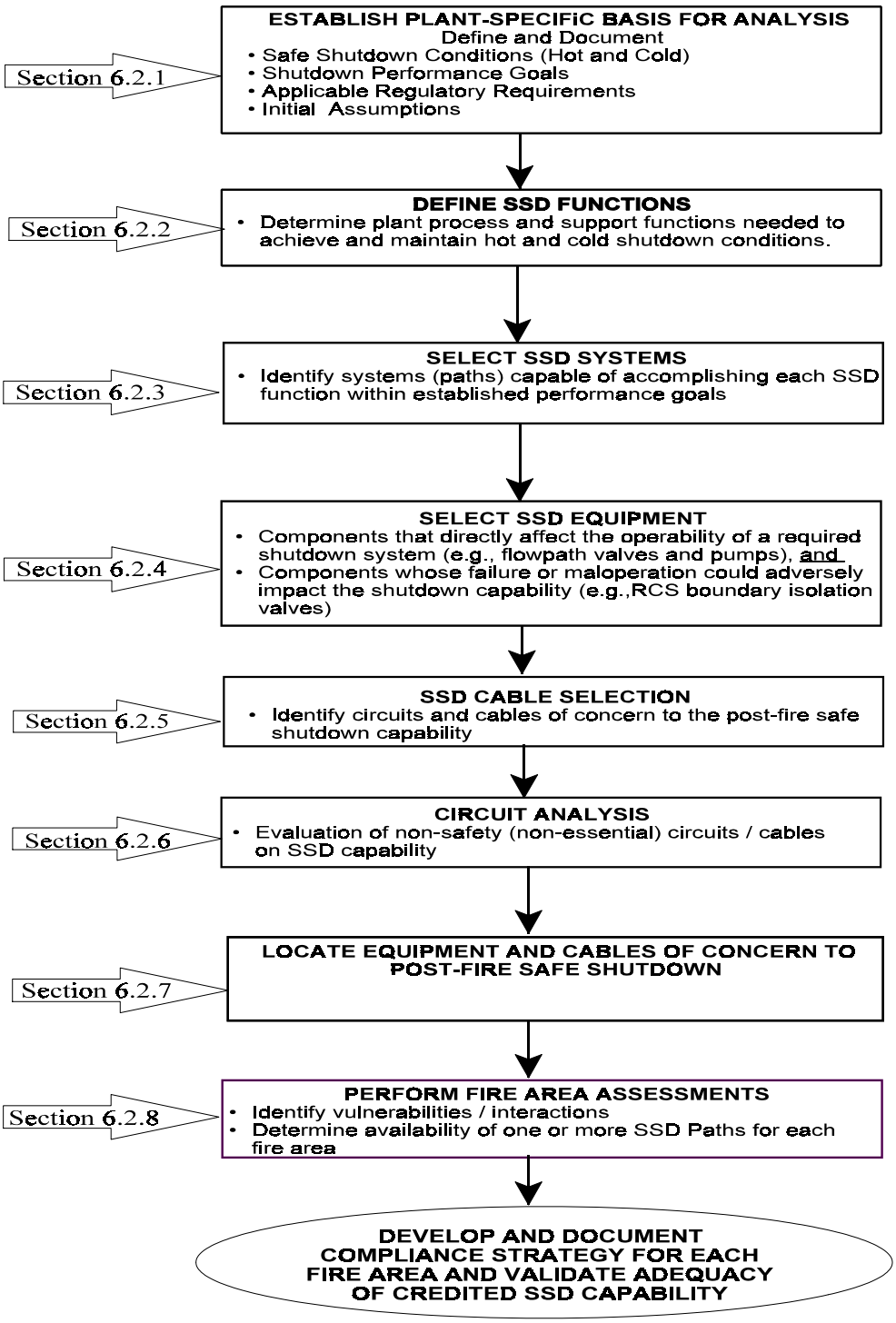


Figure 6.3 - Overview of Post-fire Safe Shutdown Analysis Process

It should be noted that for the purpose of this discussion it is assumed that a comprehensive Fire Hazards Analysis (FHA) has already been performed by qualified fire protection engineers which divides the plant into separate and distinct fire areas that are separated from other fire areas by rated fire barriers adequate for the fire hazard. As depicted in Figure 6.4, the fire area boundaries represent the extent of fire spread assumed in the safe shutdown analysis (SSA).

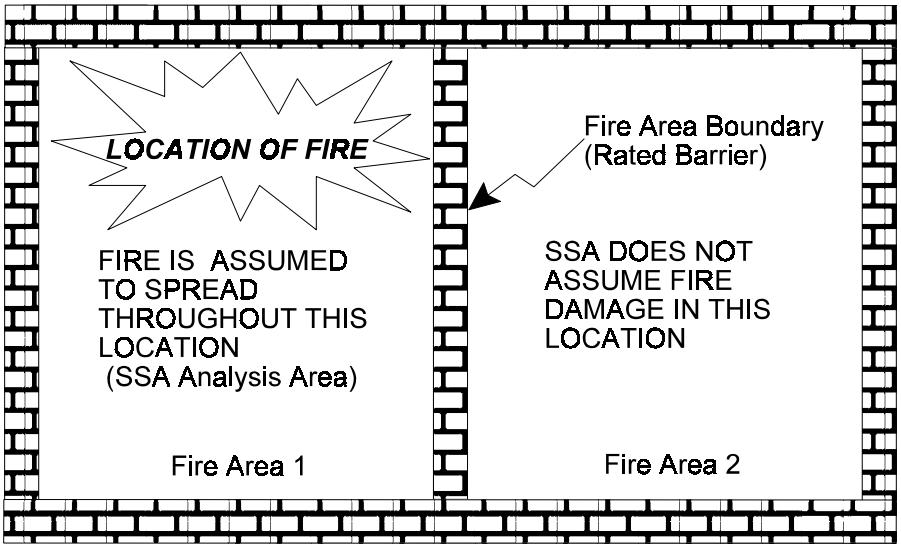


Figure 6.4 Fire-rated Boundaries Determine Extent of Fire Spread Assumed in SSA

6.2 Methodology

In demonstrating the safe shutdown capability of the plant, the SSA integrates the following evaluations:

1. **Safe Shutdown System Selection / Path Development**- Identification of redundant systems capable of accomplishing shutdown safety functions (e.g., reactivity control, reactor coolant makeup, decay heat removal etc.).

2. **Plant Configuration** - Equipment location and cable routing compared with the fire area boundary information established in the FHA.

3. **Safe Shutdown System Performance** - Demonstration 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** - Demonstration that a fire can not through its effects on non-essential / non-safety electrical circuits, prevent safe shutdown systems and equipment from accomplishing their intended function or initiate an event that is beyond the capability of the safe shutdown systems.

6.2.1 Establish the Plant-specific Technical and Licensing Basis for Post-fire Safe Shutdown

6.2.1.1 Assemble Plant-specific Information

Review available documentation to obtain an understanding of the available plant systems and the functions required to achieve and maintain safe shutdown. Documentation typically needed to perform the SSA includes:

- *Fire Protection Licensing Basis Documents* - These include the FSAR, plant operating license conditions, Technical Specifications, applicable regulatory requirements (Appendix R or SRP 9.5.1), and fire protection safety evaluations issued by the staff.

- *Fire Hazards Analysis* - In addition to identifying the fire areas, the FHA characterizes the hazards and describes the fire protection features within each fire area.

- *Plant System Descriptions* - these are the detailed descriptions of the functions and capabilities of each plant system, including those systems capable accomplishing the safe shutdown functions. They should contain both front line and support systems necessary for the operation of the system. Support systems do not directly provide safety functions, but are required to ensure that the front line systems can provide safety functions as required. Examples of support systems include cooling water, electrical power distribution, instrument air, and HVAC.

- *Plant System Design Drawings* Piping and Instrumentation Diagrams (P&IDs) are needed to identify the components that make up a system and the flow-path of that system, and to identify any interconnections to other systems that could degrade the system under certain conditions of fire damage. 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* (Normal, Emergency and Abnormal)

6.2.1.2 Define and Document Safe Shutdown

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 specific parameters for each of these conditions is defined in the Technical Specifications for the plant.

6.2.1.3 Define and Document the Safe Shutdown Performance Goals

Guidance for determining the functional and performance requirements of systems relied on to accomplish both redundant (III.G.2) and alternative (III.L) shutdown was initially provided by the NRC in Information Notice 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 (<u>both</u> redundant and alternative) are those systems necessary to perform the safe shutdown functions defined in Section III.L of Appendix R. The acceptance criteria for systems performing these functions are defined in Section III.L as:

- During the 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 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 modified the guidance initially provided in IN 84-09. Specifically, in its review of the applicability of Appendix R Section III.L requirements, the staff concludes: *"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 re-evaluation of its previous position, performance criteria for shutdown systems are now defined in Regulatory Guide 1.189 as:

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 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 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 decay heat removal.
- The process monitoring function should be capable of providing direct readings of the process variables necessary to perform and control the above functions.

Regulatory Guide 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.

6.2.1.4 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" which 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 set of 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 structures, systems or components located in (or adjacent to) that same fire area. The effects of such fire (e.g., smoke, heat or ignition) can adversely affect those structures, systems or components important to safety. Thus, a fire involving one train of safe shutdown equipment may constitute an exposure fire for the redundant train located in the same 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 LOOP the emergency diesel generators will normally start automatically on undervoltage. However, in developing the alternative shutdown capability operation of this automatic start feature can not 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 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% 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.

6.2.2 Define Required Shutdown 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 6.2.1.3). Successful accomplishment of each of the shutdown functions described below is necessary to preclude the occurrence of an unrecoverable plant condition (e.g., uncontrolled primary depressurization, loss of decay heat removal capability or breach of the Reactor Coolant System 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 Pressurized Water Reactors (PWR) there must be 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 of ensuring that sufficient make-up inventory is provided to compensate for reactor coolant system fluid shrinkage during cooldown and to replace any coolant that may escape due to leakage 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[24] and within the level indication of the pressurizer for PWRs.

[24] Short-term core uncovery may be permissible when using low-pressure injection systems at BWRs (see NRC Letter (Richards to BWROG) dated 12/12/00)

• *Reactor Coolant Pressure Control*

Pressure control is required to ensure that the reactor coolant system (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 decay heat removal 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 modify 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 Generic Letter 81-12, "Fire Protection Rule," and Information Notice 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.(Note 2)

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 exit core thermocouples, and cold leg temperature.

c. Steam generator pressure and level (wide range).

d. Source range flux monitor. (Note 1)

e. Diagnostic instrumentation for shutdown systems. (Note 2)

f. Level indication for all tanks used (e.g., CST).

Note 1: 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 ASD instrumentation in PWRs. Additionally, Enclosure 1 of GL 86-10 states that alternative methods of instrumentation are not excluded if justified by a technical evaluation. For example, the Generic Letter specifically cites the use of boron concentration measurements in lieu of source range instrumentation

Note 2: Diagnostic instrumentation is instrumentation, beyond that identified above, that is needed to assure the proper actuation and functioning of safe shutdown equipment and associated support equipment (e.g., flow rate, pump discharge 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 assured 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.

Enclosure 1 of Generic Letter 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 Emergency Operating Procedures) 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 assured 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 mal-operations that may occur as a result of fire damage, sufficient diagnostic instrumentation must be available for operators to detect the mal-operations and initiate appropriate responses in a timely manner, without resorting to complex and potentially hazardous troubleshooting activities.

When sufficient diagnostic instrumentation is not assured to remain unaffected by fire, reliance on the operators ability to detect fire-induced mal-operations that may occur and perform activities needed to defeat them before an unrecoverable condition is achieved can not be assured. For example, during a fire an operator observes the assured method of monitoring pressurizer level to be decreasing. Since many possible mal-operations 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 diagnostic instrumentation is eliminated.

• *Auxiliary Supporting Functions*

To assure 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).

6.2.3 Identify Shutdown Systems

Using the initial assumptions defined in Section 6.2.1.4 above, 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 6.2.3). This may be accomplished by a review the design documentation, such as system descriptions, system drawings, and plant procedures, described in Section 6.2.1.1. Once identified, these systems can be combined into safe shutdown success paths and a unique designation (e.g., SSD Path 1, SSD Path 2, etc.)may be assigned to each path. A description of each path should then be documented. For example, shutdown paths for a BWR may be described as:

Path 1: Control Rod Drive System; Division I train of ADS, Division I Core Spray in Alternate 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 Core Spray in Alternate 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.

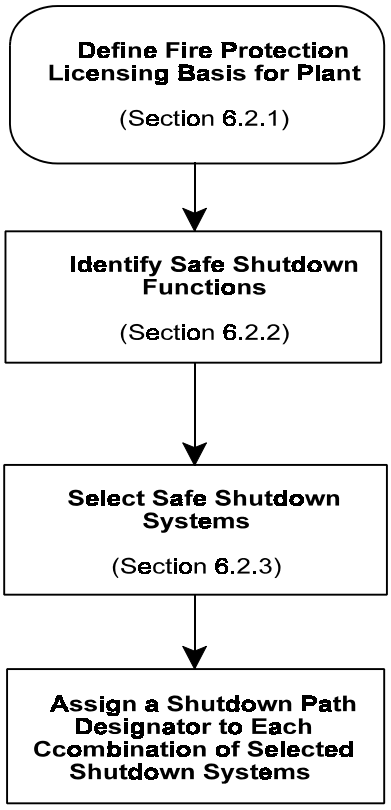


Figure 6.4a Safe Shutdown System Selection and Path Development

6.2.4 Identify 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. 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 result in an impact to 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. Criteria specifically applicable to the selection of safe shutdown equipment include:

- 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” or “Required Components” will be generated for each system. This list should include any component that is required to operate or whose mal-operation could degrade the shutdown capability. This latter set of components are typically classified as “spurious operation components” that are described below in Section 6.2.5.2. Typical examples of required components include:

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 (emergency diesel generators, battery banks, inverters, battery chargers, switchgear, motor-control centers, 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 (Safe Shutdown Equipment List, or SSEL) establishes the basis for identifying identifying *required circuits and cables* (i.e., circuits and cables needed to support operation of the identified Shutdown Paths) as well as *associated non-safety circuits* whose damage due to fire could impact (adversely effect) the achievement of safe shutdown conditions.

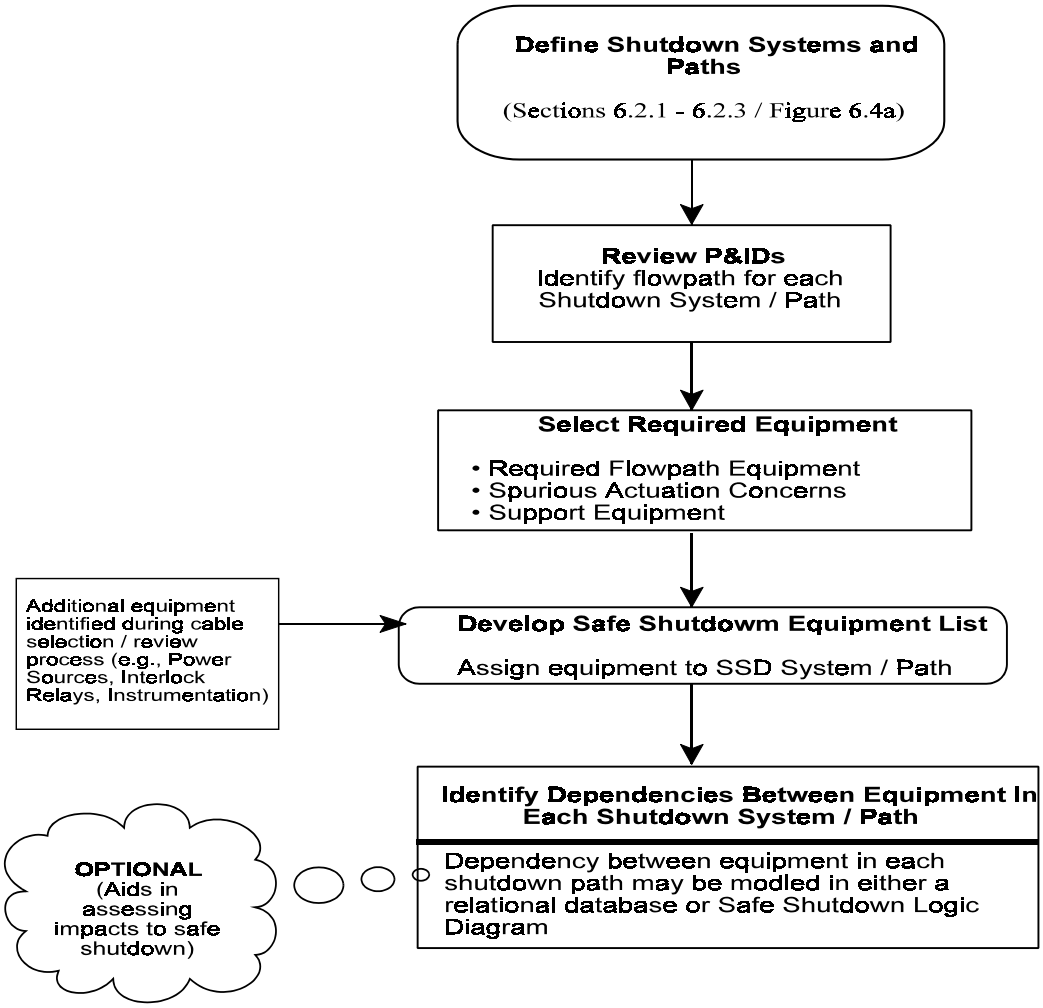


Figure 6.4b Safe Shutdown Equipment Selection

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. From an analysis perspective, components of interest are those whose operation can be adversely affected by fire. In general, these components are those that are controlled or powered by electrical circuits (cables). Typical examples of components to be included in the SSEL include:

- *Valves and **HVAC** dampers that constitute system boundaries* should be included if a fire-induced fault could cause them to change position. Associated valve operators should also be included as part of the valve. These components are included to ensure that the process is not diverted from its safe shutdown function.(Valves V7 and V8 on 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 on 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 on Figure 6.5 are is 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. (On 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)

1. *Power supplies* or other electrical components that support operation of required shutdown components should be included (switchgear, emergency diesel generator, motor control centers, load centers, inverters, batteries, relays, control switches, flow switches, pressure switches, level switches, transmitters, controllers, transducers, and signal conditioners)

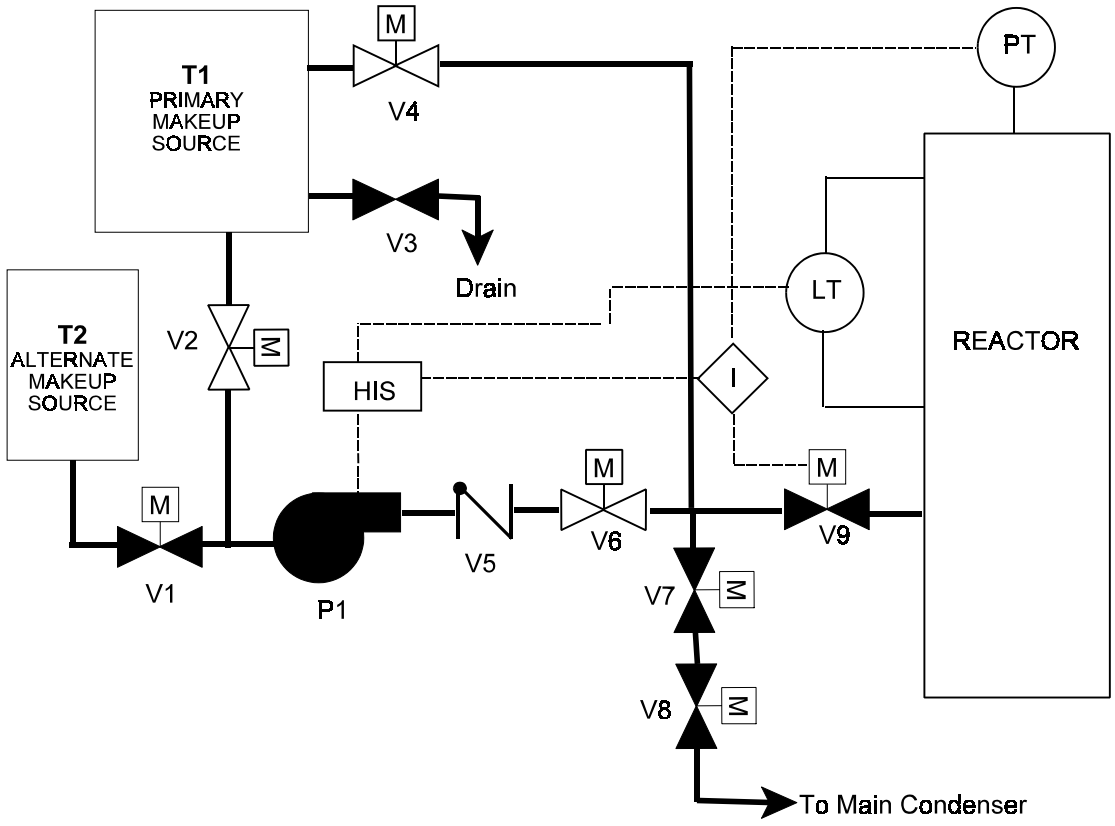


Figure 6.5 Example System

6.2.5 Identify and Locate Required Cables and Circuits

As discussed above, to achieve safe shutdown conditions certain *shutdown functions* (e.g., reactivity control, decay heat removal, 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. Systems identified as being capable of accomplishing these functions are classified as *"required shutdown systems*." Similarly, components that must operate or be prevented from mal-operating in order for the required shutdown system(s) to accomplish their intended shutdown function(s), are considered *"required components."* Once identified, required components are listed on the Safe Shutdown Equipment List (SSEL). The Safe Shutdown Equipment List (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 non-safety circuits* whose damage due to fire could impact (adversely effect) the achievement of safe shutdown conditions.

For each safe shutdown component, all circuits (cables) that are required for the operation or which could cause the maloperation of the component must be identified. After the required components are developed for each shutdown path, the cables/circuits needed to support the operation of these components are identified and evaluated. 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 cables/circuits needed to assure 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, or, 3) a connection to equipment whose *spurious operation* or mal-operation may adversely affect the shutdown capability (Note: as discussed above in Section 6.2.4 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 of an operating reactor for the condition of an exposure fire. The objective of the cable selection criteria is to ensure that cables and circuits of required shutdown equipment are identified and that these cables are properly related to the equipment whose functionality they could affect. Through this cable-to-equipment relationship, cables become associated with the safe shutdown path assigned to the equipment affected by the cable.

6.2.5.1 Cable Selection Criteria

- *Scope:* The list of cables whose 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 assure 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 cables and circuits 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 SRUs (signal resistor units) 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 assured 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 emergency diesel generators to the safe shutdown equipment. This equipment should then be added to the Safe Shutdown Equipment List (SSEL). This information will be needed to support the *Associated Circuits - Common Power Source Analysis* described in Section 6.2.5.2.

- *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 not adversely affect any post-fire safe shutdown system function.

6.2.5.2 Associated Circuits

The overall objective of the Safe Shutdown Analysis (SSA), is to demonstrate that in the event of an exposure fire in any single area of the plant, structures, systems and components important to safe shutdown will remain available to accomplish required shutdown functions (e.g., reactivity control, reactor coolant makeup, and pressure control, decay heat removal, etc.) as needed. Because cables and circuits of the required shutdown systems frequently share certain physical or electrical configurations with cables of non-essential 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 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 non-essential equipment and cables may adversely affect the operability of required shutdown systems, in performing the SSA the analyst must consider the affect of fire on both the primary, or "front-line" shutdown equipment (e.g., reactor coolant makeup pump) and any non-essential equipment and cabling whose damage due to fire may affect the operability of required shutdown systems. The point here is that the scope of the evaluation must extend beyond the limited set of equipment that comprises the defined shutdown paths. A

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.

6.2.5.2.1 Associated Circuit Configurations of Concern to Post-fire Safe Shutdown

Section III.G.2 of Appendix R to 10CFR50 requires that separation features be provided for equipment and cables, including associated non-safety circuits that could prevent the operation or cause the mal-operation due 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*

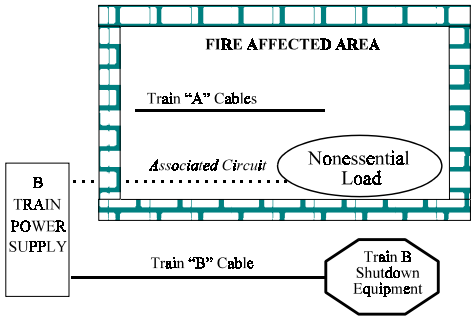


Figure 6.6 Associated Circuit

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 non-essential / non-safety 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 which share a **common power source** (e.g., switchgear, Motor Control Center, Fuse Panel) with circuits of equipment required to achieve safe shutdown; or,

- Circuits which share a **common enclosure**, (e.g., raceway, conduit, junction box, etc.) with cables of equipment required to achieve safe shutdown; or,

- Circuits of equipment whose **spurious operation** or mal-operation 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. In the event of a 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.

Electrical power supplies (e.g., switchgear, motor-control centers, 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 6.2.4). Once identified, the analyst must then assure that in the event of fire, the required power supplies will remain available as needed to ensure that the continuity of service to essential shutdown loads is maintained.

The Common Power Source associated circuit concern is illustrated in Figure 6.7.

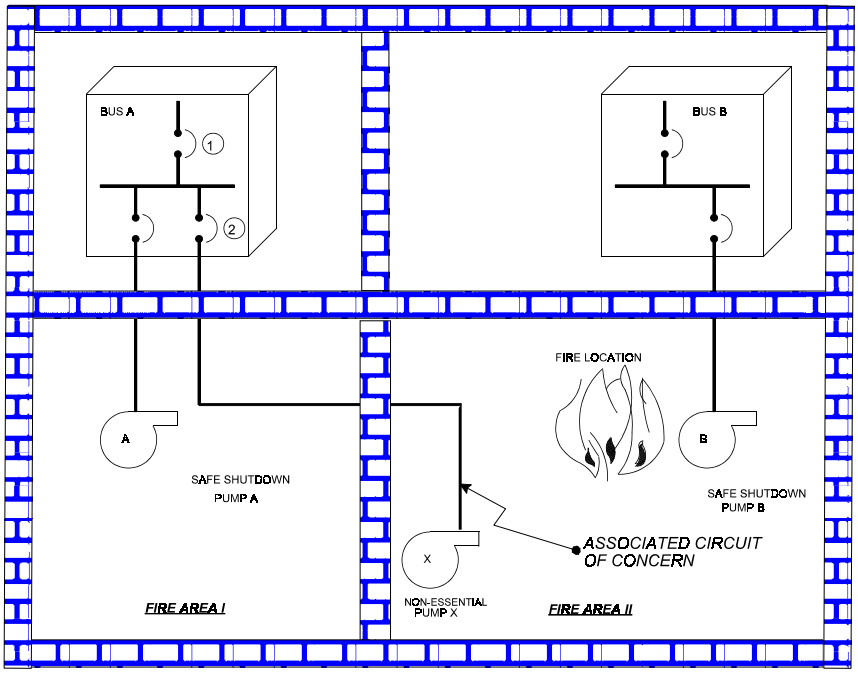


Figure 6.7 Associated Circuits - Common power source

The Common Power Source Associated Circuit Concern consists of two items:

1. Coordination of Electrical Protective Devices (Circuit Breakers, relays, fuses, etc.) and,
2. Multiple High Impedance Faults (MHIFs)

Coordination of Electrical Protective Devices

Although the term "coordination" is often used it is somewhat ambiguous since it is sometimes interpreted to mean a "degree of coordination," where more than one protective device is allowed to open under a given short circuit condition. A clearer term that more precisely addresses post-fire safe shutdown concerns is "selectivity" or "selective coordination". Selectivity means positive coordination over the entire range of possible fault currents, assuring 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 is illustrated in Figures 6.7a and 6.7b. In the Non-selective system a branch fault causes protective devices D, C and B to open, resulting in a loss of power to all loads supplied from by the system. In the fully selective system shown in Figure 6.7b, however, the fault is isolated by protective device D and the remainder of the system remains undisturbed.

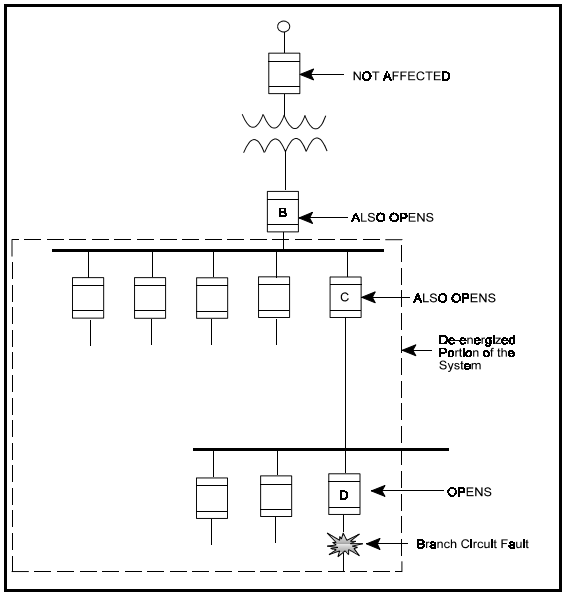


Figure 6.7a Non-Selective Coordination

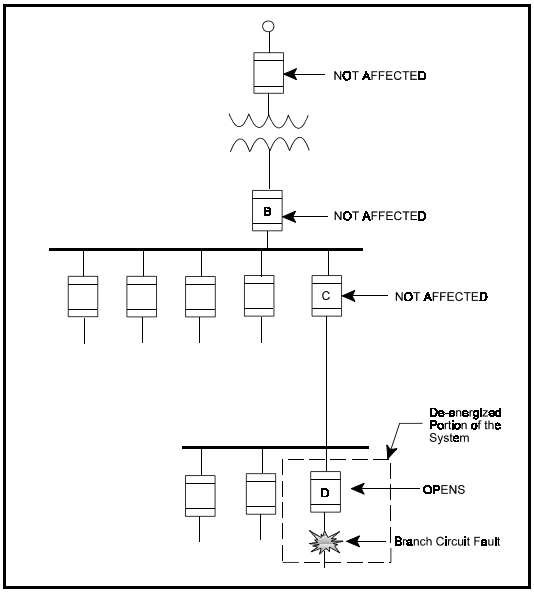


Figure 6.7b Selective Coordination

For the example shown in Figure 6.7, a fire is postulated to occur in Fire Area II. In this case, Train A safe shutdown equipment, located in Fire Area I and powered by safe shutdown Bus A, is relied on to accomplish safe shutdown. Note, however, that a Train A *associated circuit cable* (a cable not required for safe shutdown) is also routed through the fire area of concern (Fire Area II). If a fire initiated fault on this cable is not rapidly isolated by the individual branch load breaker at Bus A (Circuit Breaker No.2), the resulting fault current may propagate to cause a trip of the feeder breaker to the required power supply (Circuit Breaker No.1). Because they would result in a loss of electrical power to all shutdown equipment powered from safe shutdown Bus A, failures of this type are unacceptable.

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) or a conductor of a different phase (phase-to-phase 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 a "high-impedance" fault to be initiated. In almost every case, this type of fault occurs between one phase and ground. 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 protection 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 480v system, tests and calculations have indicated that this sustained current can be as low as 20% of the available bolted three phase current.[25] A coordination problem will exist if, instead of multiple simultaneous low level fault currents tripping the downstream breakers closest to each fault, the cumulative effect of the high-impedance faults trips the upstream breaker, causing a loss of power to the entire electrical bus and, hence, a loss of power to required shutdown equipment being fed from the affected power source. Therefore, in order to fully demonstrate that a required power source will not be impacted by fire damage to its connected cabling, high impedance faults must also 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 high-impedance fault (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, and,

[25] *"Good Design Prevents High Impedance Fault,"* Actual Specifying Engineer, Vol. 17, No.4, 1967

- 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. and,

- The total load current to be considered is the sum of all high-impedance faults plus the normal operating load current on the bus.

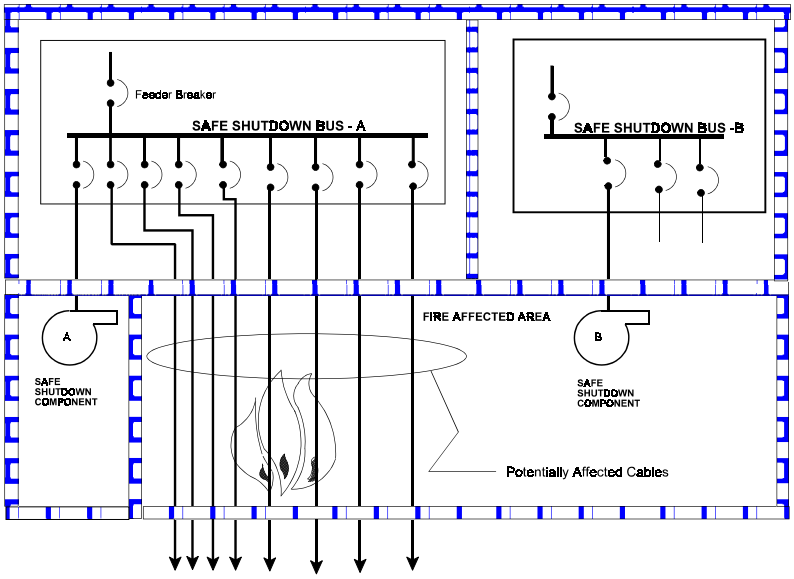


Figure 6.8 Multiple High Impedance Fault Concern

In many cases, only a few of the components powered from of a power supply identified in Section 6.2.4 as being "required" for safe shutdown are actually needed to accomplish required shutdown functions. While providing power to the remaining equipment may not be necessary to accomplish safe shutdown, it must be assured that fire initiated faults on the power cables to this equipment will not affect the shutdown capability by causing a trip of a protective device (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 6.2.4. 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 protection devices.

Circuits Associated by Common Enclosure

The concern with common enclosure associated circuits is fire damage to a cable whose failure could propagate to other safe shutdown cables in the same enclosure either because the circuit is not properly protected by a suitably sized isolation device (circuit breaker / fuse), or by the fire propagating along the cable and into an adjacent fire area. Fire spread to an adjacent fire area could impact safe shutdown equipment or cables located in that fire area, thereby resulting in a condition that exceeds the criteria and assumptions of this methodology (i.e., multiple fires and fire spread beyond area under consideration).

Circuits that share enclosures (e.g., cable trays, conduits, junction boxes, panels, etc) with safe shutdown circuits must be analyzed to determine the potential effect 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 by means of fire propagation, and

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 non-essential 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 non-essential cables may cause a secondary fire to occur within the common enclosure, thereby damaging required cables.

A diagram illustrating the common enclosure concern due to "cable ignition"is provided in Figure 6.9. As shown in this diagram, a fire in the fire area containing Instrument B cables (Fire Area II) 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 propagates 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, resulting in the loss of redundant trains of shutdown equipment.

Case 2: Common Enclosure - Fire Propagation

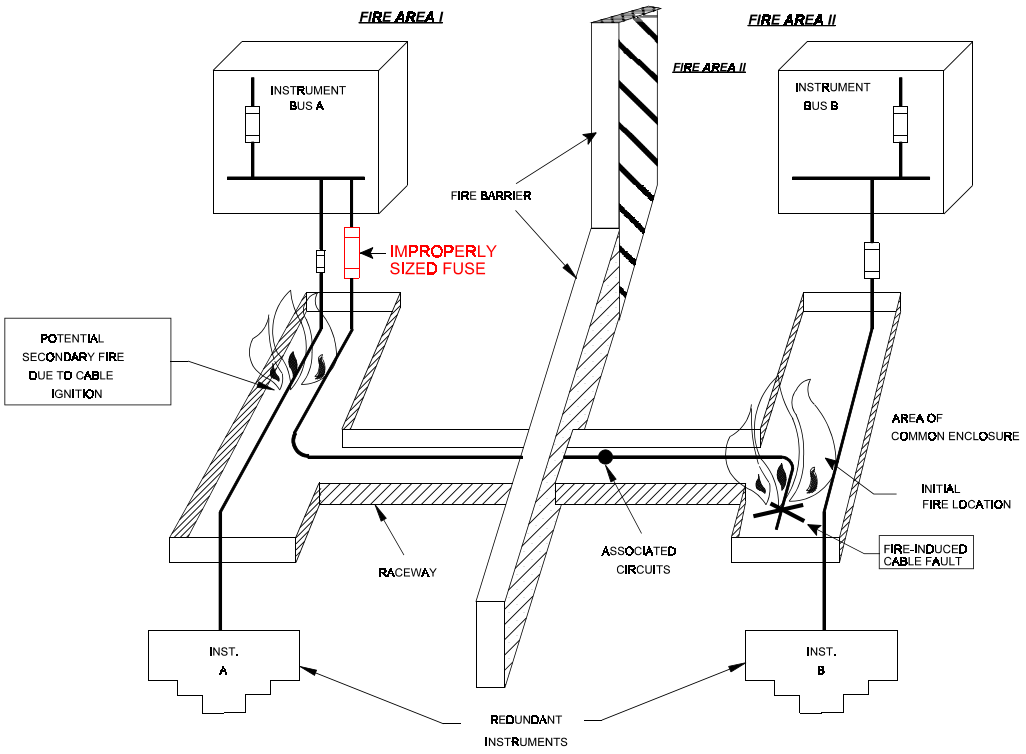


Figure 6.9 Common Enclosure - Case 1: Cable Ignition

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 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 and impact the redundant instrument (Train "A") located in the adjacent fire area.

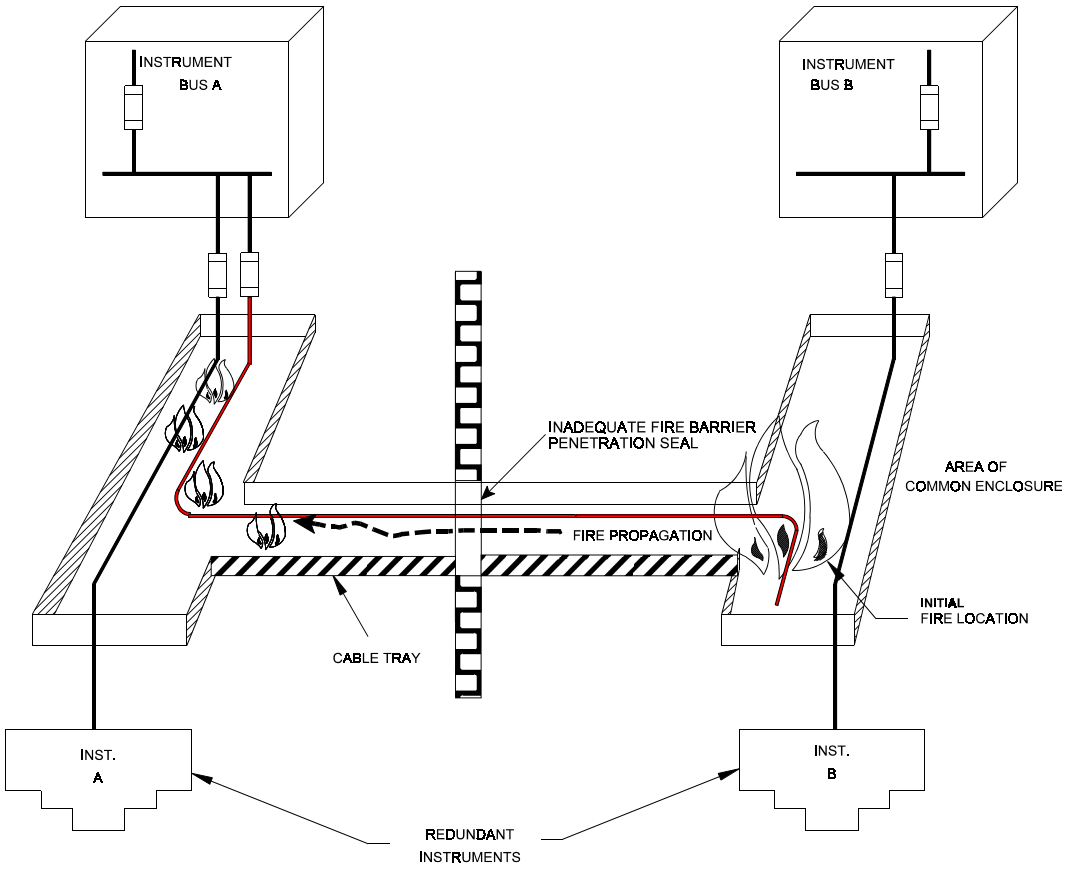


Figure 6.10 Common Enclosure Associated Circuit Case 2: Fire Propagation

Spurious Actuations and Signals

Cable damage due to fire or its related perils (e.g., fire fighting and fire suppression activities) can cause connected equipment to operate in an undesirable and frequently unexpected manner. For example, a fire-induced short circuit on control wiring of a normally open motor-operated valve (MOV), could cause the valve to spuriously 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, Motor-Operated Valve 1 (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 (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 below in Section 6.3, due to 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.

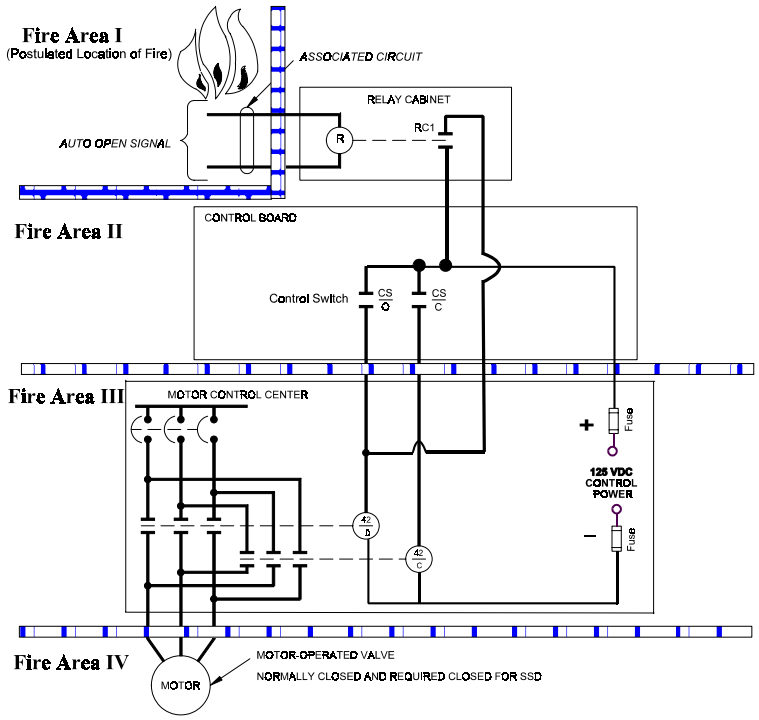


Figure 6.11 Example of the Spurious Actuation Associated Circuit Concern

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 have an immediate 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 6.2.4, 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 whose inadvertent operation could prevent the system from performing its intended shutdown function are identified and included in the Safe Shutdown Equipment List. This list should include components of non-essential systems whose 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.

6.2.6 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 9.5-1. It is explicitly required in Appendix R." (Reference: SECY-80-438A, September 30,1980, Commission Approval of the Final Rule on Fire Protection Program).

6.2.6.1 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 which will be depended upon to perform essential shutdown functions must be identified in the fire hazards analysis (FHA) and/or the safe shutdown analysis (SSA) for the plant. It follows that any circuits or cables in the fire area which could:

(a) adversely affect the operability of identified shutdown equipment and systems, or

(b) 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 can not 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 6.2.4 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 non-safety 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 non-safety circuits such that a postulated fire involving associated circuits will not prevent safe shutdown.

Associated circuits of concern are defined as cables (circuits) whose failure due to fire damage may affect the safe shutdown capability and/or prevent the achievement of post-fire safe shutdown conditions. Associated circuits may be safety related or non-safety 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 6.2.5.

6.2.6.2 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. Since it is not possible to 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 fire fighting activities), analytical approaches for demonstrating 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 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 6.2.6).

2) Short circuits between individual conductors of a multi-conductor cable (see Section 6.2.6).

3) Short circuits between conductors of different cables (see Section 6.2.6).

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 6.2.6)

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

6) Direct "bolted" low-impedance short circuits of energized conductors to grounded reference potentials. (see Section 6.2.5)

7) Arcing (high impedance) short circuits of energized conductors. (see Section 6.2.5)

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 and unless potentially affected structures, systems and components (SSC) are provided with suitable fire protection features (per Section III.G.2) the fire must be assumed to impact the performance of all SSC in the fire area.

- Credit can not be taken for the proper function of any electrical circuit that has not been fully analyzed.

- Credit may 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 can not be taken for automatic signals if the equipment or circuits that generate the automatic signals are exposed to fire damage.

- It can not 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 are 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).

- 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. Due to 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.

a. 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 can not 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. All potential spurious actuations that may occur as a result of fire in a single fire area must be addressed and either prevented or the effects of each actuation appropriately mitigated on a one-at-time basis. That is, in the evaluation of non-high/low pressure interface components, the analyst must assume that "any and all" spurious actuations that could occur, will occur, but on a sequential, one-at-a-time, basis. While it is not assumed that all potential spurious actuations will occur instantaneously at the onset of fire, the analyst must consider the possibility for each spurious actuation to occur sequentially, as the fire progresses, on a one-at-a-time basis. Analysis approaches that arbitrarily limit the number of spurious actuations that may occur (such as assuming that only one spurious actuation will occur) as a result of fire damage are inconsistent with regulatory requirements.

- 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 cables and circuits lack sufficient technical basis and are not 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.

- 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 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 Main Control Room and assume control of the plant at a remote location (e.g., Remote Shutdown Panel). Therefore, spurious operations must be postulated on circuits that can be isolated as well as circuits that can not 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 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 assure 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 can not be predicted. That is, the instrument may fail full scale high, full scale low or at some intermediate point. It can not 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 the equipment / components under consideration as described in Information Notice 92-18.

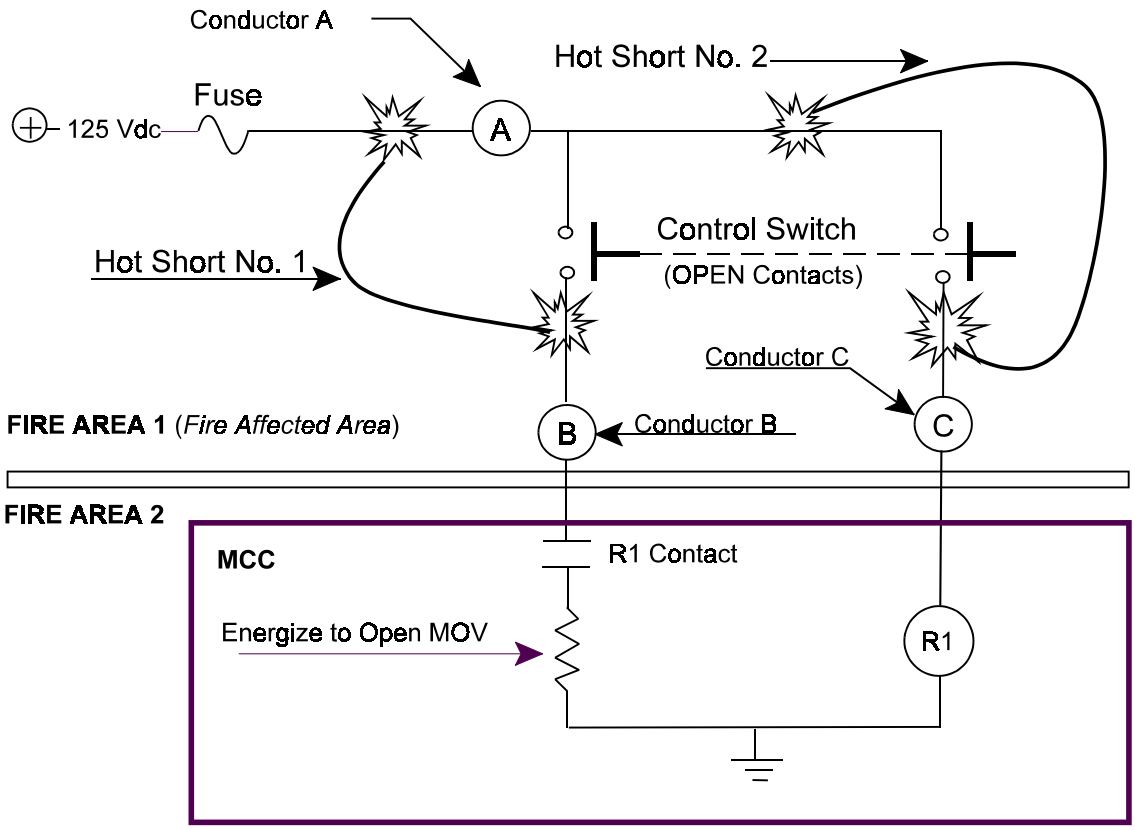


Figure 6.11a Considration of Multiple Hot-Shorts

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 spurious opening of the MOV. Multiple hot shorts of this nature are not considered credible Except

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.

6.2.6.3 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.

6.2.6.3.1 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:

- 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

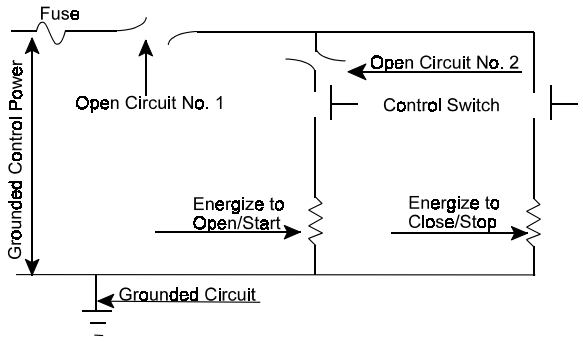


Figure 6.12 Open Circuit Example

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.

6.2.6.3.2 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. Typically, 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 6.2.5.2.1, 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.

6.2.6.3.3 Shorts to Ground - Ungrounded Circuits

In the case of an ungrounded circuit (such as most 125VDC 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

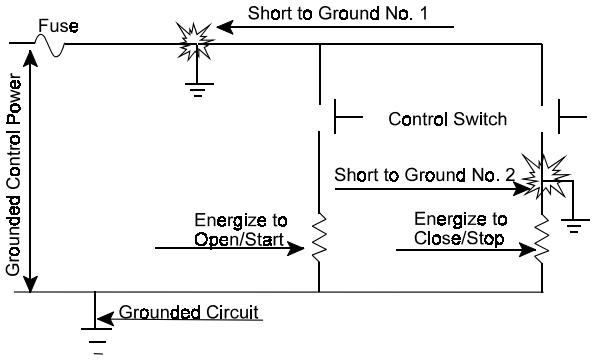


Figure 6.13 Shorts to Ground - Grounded Circuit

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)

As described above, a single short to ground on any part of an ungrounded circuit may not result in

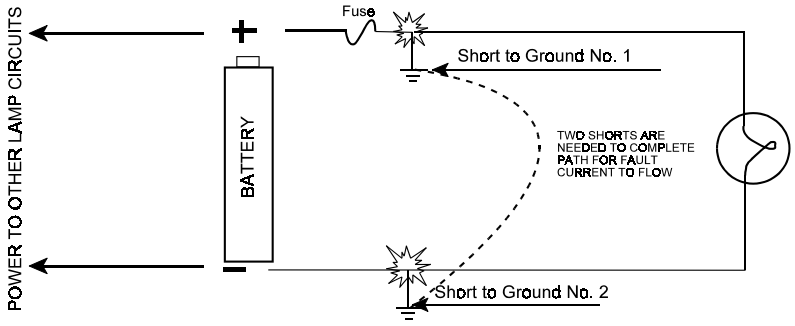


Figure 6.14 Ungrounded Circuit Illustration

tripping the circuit isolation device (fuse, circuit breaker). Another short to ground (either on the circuit or another circuit fed from the same power source) needs to exist to cause a loss of power to the circuit. Since it is likely that additional shorts to ground can occur fire damage will cause an ungrounded circuit to become grounded, it should be assumed that ungrounded circuits will become grounded as a result of fire damage.

6.2.6.3.4 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

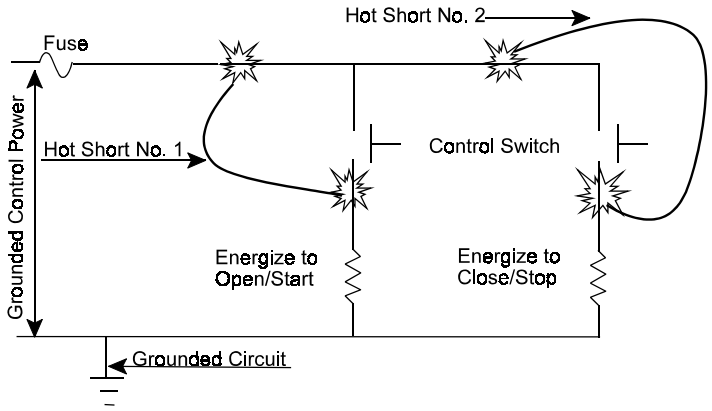


Figure 6.15 Hot Short Example

circuit. This condition would be unacceptable for safe shutdown if the desired operating mode of the affected equipment were Open / Start.

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. Due to 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 can not be ruled out, it should be assumed that ungrounded circuits will behave the same as grounded circuits in their response to hot shorts.

6.2.7 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 6.2.2), *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 6.2.3). With the shutdown paths are defined, the equipment needed to assure the proper operation of each path is identified and documented in the *Safe Shutdown Equipment List* (Sections 6.2.4). The Safe Shutdown Equipment List (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 non-safety circuits* whose damage due to fire could impact (adversely effect) the achievement of safe shutdown conditions (6.2.5). 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 (Section 6.2.6).

As discussed in Section 6.1, the post-fire safe shutdown analysis (SSA) is performed on a fire area basis. With the equipment, cables and circuits 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 lay-out drawings) to the fire area delineations identified in the Fire Hazards Analysis (FHA). The location of this equipment (i.e., fire area) should then be verified as necessary by field walk-downs 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 walk-downs 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 separate 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)

6.2.8 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 6.2.1.4.

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 (Sections 6.2.1 - Section 6.2.5) 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 is to start with the fire area and identify the redundant divisions (trains) of equipment and cables that are actually 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 is then 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 assures 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 necessary to accomplish 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 <u>not</u> 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.

One train of systems necessary to achieve and maintain Hot Shutdown conditions must be free of fire damage (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:

- Enclosing one of the redundant systems, including cables, equipment and associated non-safety circuits, in a three-hour fire rated barrier (III.G.2.a); or

- Separating redundant systems, including cables, equipment and associated non-safety circuits, by a horizontal distance of more than twenty feet with no intervening combustibles or fire hazards. In addition, fire detection and an automatic fire suppression system are required (III.G.2.b); or,

- Enclosing redundant systems including cables, equipment and associated non-safety circuits may in a one-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:

- Separating redundant systems, including cables, equipment and associated non-safety circuits, by a horizontal distance of more than twenty feet with no intervening combustibles or fire hazards. (III.G.2.d); or

- Installing fire detection and an automatic fire suppression systems (III.G.2.e); or,

- Separating redundant systems, including cables, equipment and associated non-safety circuits, by a non-combustible 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.

- Alternative (or dedicated) shutdown equipment must be independent (physically and electrically) of the cables, equipment and associated non-safety circuits of the redundant systems damaged by the fire.

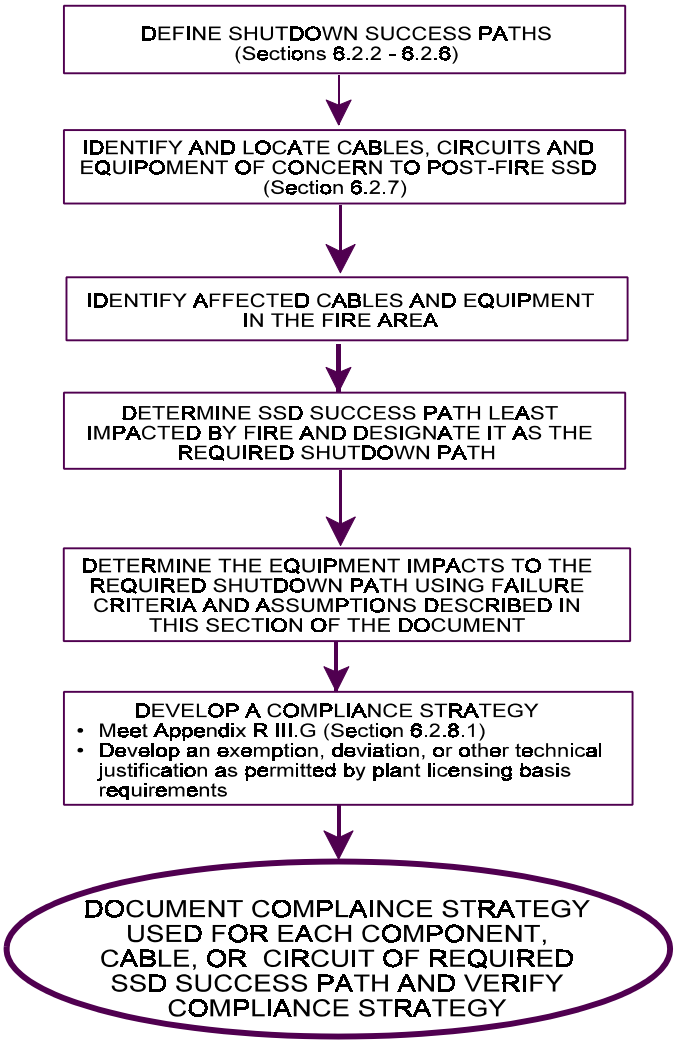


Figure 6.16 Fire Area Assessment Flowchart

7. CONFIGURATION MANAGEMENT FOR POST-FIRE SAFE SHUTDOWN

The post-fire safe shutdown analysis (SSA) is based on a "snapshot" of the configuration of plant structures, systems, components, and cable routing information that existed at the time it was performed (i.e., some single point in time). However, the plant design features and operating practices that form the basis of this 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 the SSA and incertain instances may threaten the 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, be evaluated for their impact on the shutdown capability can be fully assessed.

An example of how even a seemingly straightforward modification involving the installation of non-safety related equipment can impact the shutdown capability is illustrated in Figure 7.1. In this case, a modification is being performed to provide a more efficient means of transferring water between two non-safety related tanks. Key components being added as part of this modification include a pump, piping, a non-safety related switchgear (SWGR 1A-1), motor-operated pump suction and discharge valves, and associated 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). Additional attributes of the proposed design include:

- The pump and the entire system in which it is located is not needed to remain operational to accomplish required shutdown functions;
- Mal-operation 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 non-safety related power source (SWGR 1-1A) that does not power any safe shutdown components. A fire-induced loss if 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; and
- The SSA has demonstrated acceptable coordination between load and feed breakers of required power source 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 the pump 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 assuring that the new circuit breakers installed in SWGR1A (breaker 4) and SWGR 1A-1 (breaker 2) properly coordinate with upstream feed breaker (breaker 1), a fire in Fire Area VI could significantly impact the shutdown capability by causing a trip of the feed breaker to the required Division A power source (breaker 1) and, hence, the loss of equipment (Pump A) that would be relied on to accomplish essential shutdown functions in the event of fire in Fire Area VI. (Refer to Section 6.2.5.2.1 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., a motor-operated valve), re-routing of cables, adding loads to a required power source, replacement of circuit protective devices (fuses, circuit breakers, relays) installation or removal of interlocks, control circuit modifications (e.g., change from manual to automatic control), temporary modifications to facilitate plant maintenance activities (e.g., welding) and changes to the plant operating procedures (normal, abnormal and emergency).

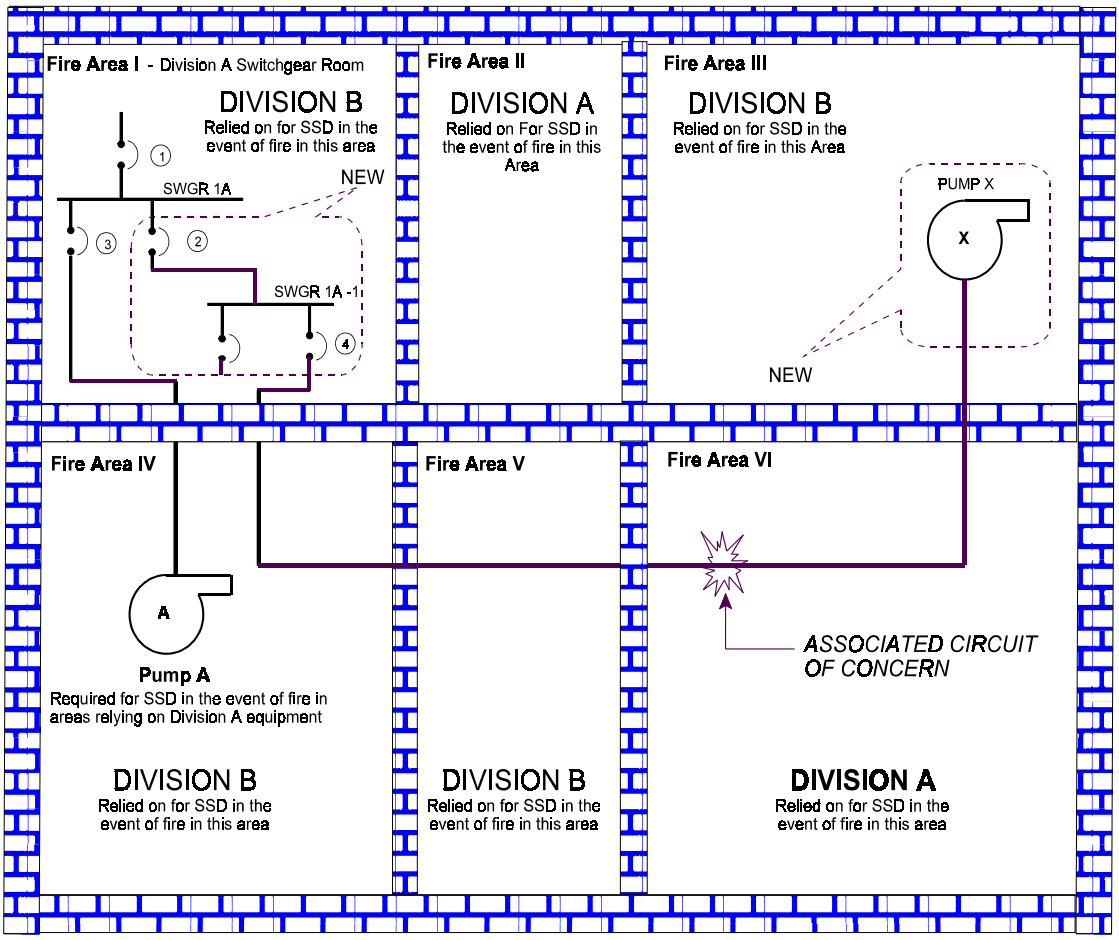


Figure 7.1 Illustration of modification impacting the SSD capability

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

- Modification Review - All modifications (i.e., permanent or temporary additions, deletions or changes) to plant structures, systems or components (SSC) 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 - Fuses, circuit breakers and relays having ratings or settings other than those selected to assure proper coordination for post-fire safe shutdown are not accidentally used. To ensue that circuit breaker and fuse coordination studies referenced in the SSA will not be compromised by future plant changes, the replacement of fuses in power sources required for post-fire safe shutdown should be performed in accordance with approved procedures and the coordination study should be maintained current with the most recent modification of required shutdown power sources.

- Procedure Changes - The review of permanent and/or temporary procedure changes should consider such factors as:

  (a) The effects of the change on 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 both inside control room and from alternative shutdown location(s)

8. INTEGRATION OF DETERMINISTIC CRITERIA AND RISK-INFORMED INFORMATION

8.1 Overview of a Risk-Informed Approach

It is USNRC policy to increase the use of risk information in the regulatory decision-making process [Ref. 8.1]. Risk combines two factors; namely, the likelihood (or frequency) that an event will occur leading to undesired consequences and the severity of those undesired consequences. In this chapter, the event of interest is a fire that challenges nuclear safety, and the potential undesired consequence of such an event is an off-site release of radiative 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, Core Damage Frequency (CDF) and Large-Early Release Frequency (LERF).[1] CDF reflects the frequency (events per reactor year) at 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 leading to a large release of radioactive materials relatively early in the accident sequence. In this context, the term early is measured in the context of 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 considered generally indicative of the potential that public health consequences might occur.

The USNRC Risk-Informed Policy as embodied in Regulatory Guide 1.174 [Ref. 8.2] weighs regulatory compliance findings and issues against both CDF and LERF criteria. To date, the fire protection portions of the regulatory requirements (e.g., 10 CFR 50 Appendix R [Ref. 8.3]) have not been formally risk-informed. However, aspects of the fire protection regulatory process are incorporating risk information. For example, the USNRC staff is currently engaged in a rule-making activity related to the recently adopted National Fire Protection Association standard (NFPA 805) - *Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plant* [Ref. 8.4]. 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 [Ref. 8.5].

The current discussion is intended to provide risk-informed perspectives on the post-fire safe shutdown circuit analysis issues for use by USNRC staff, in particular, those staff members responsible for plant inspection activities. The discussion does not establish any new requirements nor regulatory compliance criteria. Rather, the discussion is intended to assist the USNRC staff in understanding, and potentially assessing, the risk significance of the fire-related safe shutdown circuit analysis issue.

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 nor 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 USNRC Office of Nuclear Regulatory Research (RES). More detailed discussions on this topic can, for example, be found in Reference 8.6.

[1] 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 off-site release and public health consequences.

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 post-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 achieve, but generally 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, very few of which have been performed to date. This section provides a very brief 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 for the purposes of regulatory compliance often differs from the definitions used in a fire PRA. For regulatory purposes 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 [Ref. 8.7]. Fire PRAs are generally based on fire compartments[2], 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 area may be partitioned into two or more fire compartments. Defining the boundaries of a fire PRA compartment is a somewhat judgmental exercise. Partitioning for the fire PRA may credit such features as 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.

The CDF analysis systematically considers the potential risk contribution arising from fires in each fire compartment. The risk contributions may be reported at a scenario level (e.g., for a given fire ignition source), but are more typically reported at a compartment level. Hence, one will often see CDF values cited for each individual compartment (e.g., the Cable Spreading Room). Note that an explicit analysis is also performed to assess the risk contribution for those fires that might impact multiple fire compartments, and these scenarios are often reported separately. It is also common to report a total fire-induced CDF for the plant as a whole - 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 based on the consideration of three factors. Mathematically, this is expressed through a simple three-term expression as follows:

$$CDF = \sum_i f_i \left(\sum_j P_{cd,j|i} \left(\sum_k P_{CD:k|i,j} \right) \right)$$

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 likely involving a number of fire compartments. Fire frequency includes consideration of both fixed (e.g.: fixed electrical

[2] 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.

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; in-service maintenance support materials; welding and cutting operations; refuse; etc.).

Given fire PRA plant partitioning practices as described previously, the fire frequency may be broadly quantified to reflect all possible fire ignition sources in a given fire compartment (e.g, a battery room). However, fire frequency may also 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 switchgear). The fire frequency is typically estimated based on statistical analysis of the existing 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 [e.g., Ref. 8.8, 8.9].

The second term ($P_{cd,j|i}$) reflects that 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 probability of either "component damage" or "critical damage" depending on the analysts' use of terminology. The second summation reflects the observation 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 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 equipment. Damaging some set of plant equipment implies that some subset of the plant systems and/or functions are damaged. 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 Core Damage will result. Again, the summation reflects the possibility that different paths towards safe shutdown are possible, each having a unique likelihood of success/failure. Calculation of this factor 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 those fire compartments that contribute most to the total fire risk; that is, the risk- dominant fire compartments. 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 switchgear 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 critical 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 compartment. For example, a 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 1E-4/ry).

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.[3] 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.

Circuit analysis is complicated in part because electrical cables may experience one or more of several failure modes, and the failure behavior may be dynamic - changing through 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 signal, and spurious actuation. Since the electrical cable failure behavior may be dynamic, the circuit's faulting behavior may also be dynamic. To

[3]Note that some methods used in the Individual Plant Examination External Events (IPEEE) studies credited only the Appendix R systems [Ref. 8.10]. When rigorously applied, such approaches typically yield conservative estimates of fire risk.

illustrate, consider that two of the possible cable failure modes of particular importance are hot shorts and shorts to ground. Conductor-to-conductor shorting 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 cable failure mode, and the anticipated duration of specific failure modes. As multiple circuits come into play in a fire scenario analysis, this introduces further questions such as the likelihood that multiple circuits might experience concurrent spurious actuations.

It is impractical 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 system will have a limited set of specific fault modes that will be unique in the context of fire risk. Depending on the specific system, some fault modes may, indeed, 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 will influence 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 mal-operation 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 systems and system fault modes and to then quantify the potential 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

For the purposes of risk analysis, a mechanistic view of the circuit analysis problem is being developed [Ref. 8.6]. As an entry condition to the 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 int two major pieces; namely, the electrical cable failure mode behavior and the circuit fault mode behavior. The discussions provided in subsequent sections of 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, a cable failure mode 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 where to become involve in the short circuit, e.g. a grounded conductor, then 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 address 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, given failure the electrical cable in and of itself will experience some combination of conductor failure modes. Conductors of a given electrical cable may short to each other, they may short to the conductors of another electrical cable, or they may short to an external ground. This behavior should be to, at least some extent, relatively independent of the nature of the circuit to which the cable is connected. However, the cable failure mode 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 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 through the circuit when the circuit is actuated (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, how the circuit responds to the cable failures, will depend on the shorting failure of each of these conductors as illustrated by the previous example.

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 sustained shorts 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 will not fully simulate the plant installation and fire exposure conditions one might expect to encounter. 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 electrical cable fire tests [Ref. 8.13], even though these tests arguably 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 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 follow, 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” [Ref. 8.11]. From and 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 assured.

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 American Wire Gauge (AWG)), the number of conductors, shielding and/or armoring features, and the insulation/jacket materials used in the construction.

There are four modes of cable failure of potential interest. These failure modes relate to the electrical behavior of the conductors associated with a given electrical cable and are 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)). As 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 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 relating to this discussion of 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 - 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 the conductors within a single multi-conductor electrical cable. Inter-cable conductor-to-conductor shorting implies that the short circuit involves shorting between 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 as discussed further in Section 8.5 below. 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 NRC Office of Nuclear Regulatory Research (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 [Ref. 8.6]. Hence, of particular note is a recently completed set of tests performed by NEI with the explicit participation of the NRC [Ref. 8.12,13]. These tests provide the most explicit data on cable failure modes and effects currently available and will be discussed in some detail.

A total of 18 fire tests was conducted, each involving a cable tray and 4-to-5 monitored cable bundles. The tests explored a limited range of fire exposure conditions, cable types, and routing conditions. The data has 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 a highly a-typical room. The test room was a steel plate box of limited dimension. Given the steel room construction, heat losses from the room were much greater than would be anticipated given a wall material such as concrete. Hence, the relationship between the fire intensity and the room temperature conditions was somewhat distorted.

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 apply to 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 contributed to a higher incidence of shorts to ground and a lower likelihood of spurious actuation.

Finally, the tests use primarily AC power sources so the applicability to DC circuits is unknown. 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 either fuse blows (indicating an energized conductor shorting to ground or to a grounded conductor) versus spurious device 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 estimated conditional probability of this mode of cable failure was estimated as 80% or higher based on these and other tests (conditional on electrical cable failure).

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[4] 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 be assessed for validity, hence, their application to risk analysis remains unproven.

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 - it is not a recommended approach.

There are potential problems with such approaches that have not yet been resolved. First, the shorting behavior of multi-conductor electrical cables is complex and often involves more than two conductors in a shorting group. Second, the shorting behavior of conductors in a given electrical cable 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.

The combinatorial model represents a potentially valuable approach that will likely see further development in the near future. One participant in the recent EPRI expert panel study proposed a more complex combinatorial model that incorporates an advanced view of cable failure behavior (see Appendix B-1 of Ref. 8.14). 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

[4] 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.

galvanized steel) 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 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, what is again of 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% or less of the observed cable failure 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 likely substantially higher (perhaps 50% 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 or not 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, again 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 [Ref. 8.13], 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 nominally 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 if not likely. 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 fire fighting 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

Polymeric insulation materials, thermo-sets and thermo-plastics, dominate the current electrical cable applications in the U.S. nuclear power industry. When these materials are heated, they will loose their electrical insulation value. Based on available equipment qualification test results [Reg. 8.15], the degradation in resistance is logarithmic with linear increases in temperature. An example of this behavior is illustrated in Figure 8.1 [reproduced from Ref. 8.16]. This same mechanism can lead to a loss of insulation resistance failure 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 thermo-plastic material, and below the nominal gross failure threshold of thermo-set 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.

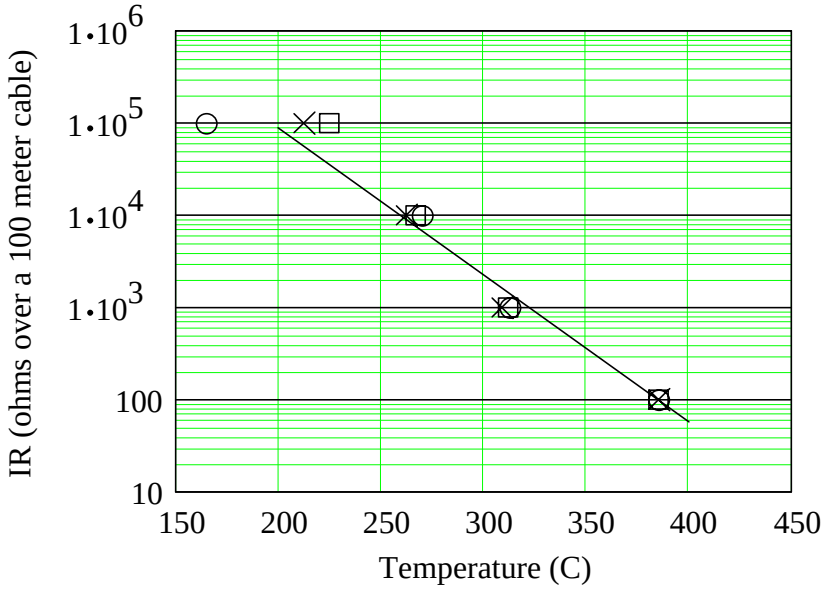


Figure 8.1: Illustration of the IR versus temperature behavior of a typical electrical cable insulation material. This plot shows test data and a linear regression curve fit for a Brand Rex cross-linked polyethylene (XLPE) insulated 12 AWG 3-conductor electrical cable. The data are from Table 4 of NUREG/CR-5655, *Submergence and High Temperature Steam Testing of Class 1E Electrical Cables* (Ref. 8.17). 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.

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 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.

A recent test series examined this behavior for instrument circuits [Ref. 8.12]. In general, a pronounced difference was noted between the behavior of thermo-set and thermo-plastic insulated instrument cables. Thermo-plastic

insulated electrical cables tended to fail abruptly and catastrophically with little or no indication of degraded signals prior to loss of signal. Thermo-set insulated electrical cables illustrated a prolonged period of corrupted signal transmission before a complete loss of signal was observed. Hence, the use of thermo-set insulated electrical cables appears to increase the potential that operators might be misled by a corrupted signal. An offsetting observation was that the thermo-plastic insulated electrical cables failed far more quickly than did the thermo-set insulated electrical cables. This is also consistent with the observation that thermo-set insulated electrical cables are generally more resistant to fire-induced failure than are thermo-plastic 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 - 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 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, it would be expected that 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 failure 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 author's rational for the second part of this conclusion depends on the type of circuit considered:

- 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 due to 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 this failure mode - intra-cable conductor-to-conductor short circuits. This appears to apply to both thermo-set and thermo-plastic 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 thermo-plastic insulated electrical cables than it is given thermo-set insulated electrical cables. The available data on inter-cable shorting is not sufficient to provide firm estimates of conditional likelihoods. However, for thermo-plastic insulated electrical cables, the likelihood of inter-cable conductor-to-conductor short circuits is probably 0.5 or less. For thermo-set 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, thermo-plastic and thermo-set, 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 known to, or thought to, have a significant impact on the likelihood of inter-cable shorting include the following [Ref. 8.12]:

- The nature of the fire exposure: direct flame/plume exposures that heat the cables from below may be more prone to 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 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 show promise 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 potential unique interest for each circuit type are as follows:

- Power circuits:
  - Loss of primary or motive power to a system or component
  - Hot shorts leading to spurious actuation
  - Multiple high impedance faults

- Control/Indication Circuits:
  - Loss of control function or power
  - Spurious actuation in control circuits
  - Loss of control indications
  - False control indications

- Instrumentation circuits:
  - Loss of permissive signals
  - False permissive signals
  - Corrupted instrument gage readings

Each of these circuit types is taken up in detail in the sub-sections which follow.

8.6.1 Power Circuits

Circuit Fault Modes Involving Loss of Primary Motive Power

For power circuits, many electrical cable failures will lead to a loss of primary motive power to plant devices.[5] 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 motor-operated valves 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 or fail-safe condition.

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

[5] Motive power is distinguished from control power - motive power is the source of energy that runs a primary electrical device such as a motor; control power is a separate, though 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.

- phase-to-ground short circuits involving an energized conductor,
- phase-to-phase short circuits involving two or more energized conductors, or
- 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 leading to loss of motive power will be the predominant fault mode given the failure of power cables. It can nominally be assumed that 99% 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.

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 nuclear power plants in the U.S. 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 over-current condition will likely trip the source conductors' protective circuit features mitigating the fault.

Nominally, the probability of such faults given the failure of power cables is probably 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 probably of 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), then the likelihood of a spurious actuation will likely 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 is probably 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. Alternately, 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 only for high consequence applications (e.g., high-low pressure interfaces) appears appropriate. 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 what knowledge we do 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 [Ref. 8.12,17,18]. The data show that electrical cables energized to a non-trivial level (i.e., greater than approximately 50V) 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 implication of the multiple high impedance fault issue are mitigated to some extent given that operator actions 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 due to 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. nuclear power plants, 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 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 associate 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 Ref. 8.6).

Spurious actuation in control circuits

The issue of spurious actuations (or spurious operations) has received much attention. Spurious actuation is one specific type of 'mal-operation' fault as identified in the NRC fire regulations. Spurious actuation involves activation of a functional mode of a system, in this context, caused by fire-induced electrical cable failures. Based on our 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, and some conductor shorting combinations will not cause actuation. Indeed, not all hot shorts will lead to a spurious actuation, so care must be taken is 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; namely, when the spurious actuation occurs and for how long it persists. For example, a spurious actuation may open a 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 a 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 noted previously, 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[6] of this circuit to range from 0.1 to 0.5 due only to intra-cable hot shorts [Ref. 8.14]. Variations from the base case led to other likelihood estimates including the following general effects:

[6] 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.

- 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 two). 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 thermo-set insulated electrical cables, the thermo-plastic 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 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 experience 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. Manual actions would be needed to mitigate the diversion path by closing one or both valves. 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 - the so-called ‘any and all, one at a time’ approach. In the regulatory analyses based on this approach, it is assumed that any spurious actuation fault might occur, but that the impacts are considered due to only one such fault at any given time. The MOV example immediately above would not be captured under this approach.

Two additional considerations related to multiple spurious actuations are the following:

- 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 RES insulation resistance measurements made during the NEI tests as well. In the RES measurements, groups of conductors were observed form dynamic conductor shorting groups, a behavior that could lead to multiple actuations of a circuit due to 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[7] 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.

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

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 test, and that the factors varied were only explored over a limited range. Overall, there is 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 $(0.6)^4$ or 0.13.

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 (thermo-set insulated electrical cables in particular). Experience illustrates that most fires cause 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 problem. For example, if an operator sees both open and closed indicators illuminated for a single valve, they will likely 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 considered this issue explicitly.

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 apposed 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 unsafe actions. 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 actions.

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/USNRC electrical cable fire tests described previously, several instrument cables were tested [Ref. 8.12]. These tests utilized a simulated 4-20mA 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.

- Thermo-plastic 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.

- Thermo-set 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 Circuit Faults

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 actions 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 Circuit Faults

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.

Lost or Corrupted Reactor Status Signal Circuit Faults

As noted previously, the instrument signals are of critical importance to operators and guide the operator 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 unsafe actions. 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 thermo-plastic and thermo-set insulated cables has been observed which is directly relevant to the potential for transmission of corrupted signals. Thermo-plastic insulated cables experienced a sudden failure with no appreciable pre-failure degradation of the transmitted signal. In contrast, thermo-set 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 thermo-set insulated instrument wires. While thermo-set insulated cables are known to be predominant in control and power cable applications in the U.S., the proportion of plants using thermo-plastic versus thermo-set 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 actions to replace or bypass the damaged electrical cables. Spurious actuations due 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 due to 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 unlikely 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 due 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. 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 as 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. Given 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. 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 apparent 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 [Ref. 8.20]:

- During a 1982 fire at the Armenia 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 due to fire damage to the associated control cables. This led to the non-operating generators being connected to the grid and in turn to secondary fires in one of the turbine-generators and in the start-up transformer.
  - One of the diesel generators spuriously disconnected from its emergency loads apparently due to 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 Ignalina NPP, there were a number of cases where equipment was lost due to 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 6kV buses and two essential (non-safety) buses.
  - Control cable damage tripped Transformer 5 and prevented it from taking up the loads for these buses.

- During a 1991 fire at Chernobyl Unit 2, a conductor-to-conductor short in a multi-conductor electrical cable attributed to electrical cable damage from poor cable pulling practices during construction 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 actuation might occur in a given fire. The cases noted previously show spurious actuations impacting up to three independent systems during a single fire event.

8.8 References for Chapter 8

8.1 "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," USNRC, Federal Register, V60, p.42622: Aug. 16, 1995.

8.2 "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis," Regulatory Guide 1.174, USNRC: July 1998.

8.3 The Code of Federal Regulations: Title 10 - Energy, Part 50 - "Domestic Licensing of Production and Utilization Facilities, Appendix R - Fire Protection Program for Nuclear Power Facilities Operating Prior to January 1, 1979."

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

8.5 *Fire Protection Significance Determination Process*, IMC 0609 Appendix F, USNRC: 2000.

8.6 LaChance, J., et.al., "Circuit Analysis - Failure Mode and Likelihood Analysis: A Letter Report to the USNRC," Sandia National Laboratories, Albuquerque, NM, May 8, 2000 (available through the USNRC PDR under USNRC memorandum from T.L. King to M.E. Mayfield and G.M. Holahan dated June 13, 2000).

8.7 *Fire Protection For Nuclear Power Plants*, Regulatory Guide 1.189, USNRC: Apr. 2001.

8.8 Wheelis, W.T., *Users Guide for a Personal-Computer-Based Nuclear Power Plant Fire Data Base*, NUREG/CR-4586, USNRC: August 1986.

8.9 *Fire Events Database for U.S. Nuclear Power Plants: Update Through 1999*, EPRI, Palo Alto, CA: Oct. 2000, 1000894.

8.10 *Perspectives Gained From the Individual Plant Examination of External Events (IPEEE) Program*, NUREG/CR-1742, USNRC: Apr. 2002.

8.11 "Fire Endurance Test Acceptance Criteria for Fire Barrier Systems Used to Separate Redundant Safe Shutdown Trains Within the Same Fire Area," Supplement 1 to Generic Letter 86-10, "Implementation of Fire Protection Requirements," USNRC: Mar. 25, 1994.

8.12 Wyant, F.J., Nowlen, S.P., *Cable Insulation Resistance Measurements Made During Cable Fire Tests*, NUREG/CR-6776, USNRC: June 2002.

8.13 *Characterization of Fire-Induced Circuit Faults: Results of Cable Fire Testing*, EPRI, Palo Alto, CA: 2002. 1003326.

8.14 *Spurious Actuation of Electrical Circuits Due to Cable Fires: Results of an Expert Elicitation*, EPRI, Palo Alto, CA: 2002. 1006961.

8.15 Bennett, P.R., Kolaczkowski, A.M., Medford, G.T., *Summary Report: Electrical Equipment Performance Under Severe Accident Conditions (BWR/Mark I Plant Analysis)*, NUREG/CR-4537, USNRC: Sep. 1986.

8.16 Nowlen, S.P., *Ampacity Derating and Cable Functionality for Raceway Fire Barriers*, NUREG/CR-6681, USNRC: August, 2000.

8.17 Jacobus, M.J., and G.F. Fuehrer, *Submergence and High Temperature Steam Testing of Class 1E Electrical Cables*, NUREG/CR-5655, USNRC: May 1991.

8.18 Nowlen, S.P., *An Investigation of the Effects of Thermal Aging on the Fire Damageability of Electric Cables*, NUREG/CR-5546, USNRC: May 1991.

8.19 M. Kazarians and G. Apostolakis, *Fire Risk Analysis for Nuclear Power Plants*, NUREG/CR-2258, University of California at Los Angeles, Los Angeles, CA, Sept. 1981.

8.20 Nowlen, S.P., Kazarians, M., Wyant, F., *Risk Methods Insights Gained from Fire Incidents*, NUREG/CR-6738, USNRC: September 2001.

PRELIMINARY DRAFT
December 2002

APPENDIX A

SUCCESSFUL IMPLEMENTATION OF APPENDIX R CIRCUIT ANALYSIS

As described in Section 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*); and

2. Circuits/cables of equipment that, if damaged by fire, could impact the shutdown *capability* (*“associated, “non-essential” or “non-safety” circuits of concern*).

The principal staff guidance related to the potential impact of fire-induced circuit failures in “non-essential” or “associated” circuits is contained in Generic Letter 81-12 (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:

- Non-essential circuits which share a **common power supply** (e.g., Switchgear, Motor Control Center, Fuse Panel) with circuits of equipment required to achieve and maintain safe shutdown; or,

- Non-essential circuits which share a **common enclosure**, (e.g., raceway, conduit, junction box, etc.) with cables of equipment required to achieve and maintain safe shutdown; or,

- Cables and circuits that have a connection to equipment whose **spurious operation** would adversely affect the shutdown capability.

With few exceptions, most licensees have successfully resolved *Common Power Supply* and *Common Enclosure* associated circuit concerns on a plant-wide basis through the performance of generic evaluations. When resolved in this manner, the types of cables/circuits of concern to post-fire safe shutdown is then reduced to two specific classifications:

1. *Required Cables*: Cables/circuits of equipment needed to ensure the proper operation or functioning of shutdown systems defined/designated in the SSA, and

2. *Spurious Non-safety Cables*: Cables/circuits of systems and equipment that are not needed to assure the operation of shutdown systems credited in the SSA, but whose inadvertent (spurious) actuation or mal-operation could impact the shutdown capability.

In its clarification of Generic Letter 81-12, the staff defined the scope of the spurious operation associated circuit concern as those circuits/cables whose damage due to fire could impact the safe shutdown *capability*. A fundamental presumption of the GL was that cables/circuits of equipment that could prevent operation or cause the mal-operation of *redundant shutdown systems* were provided with suitable fire protection features (i.e., satisfy Section III.G.2 of Appendix R), and would, therefore, remain free of fire damage. As shown in Figure A-1, however, even when redundant trains of "required" cables are provided with suitable protection features, fire damage to circuits/cables related to the operation of "non-essential" systems and equipment (i.e., not needed to ensure operation of the defined/credited shutdown systems) may significantly impact the shutdown capability.

In general, a circuit (cable) is considered to be *required* for safe shutdown if: (a) it is related to the operation of shutdown equipment (e.g., power, control, interlock circuits) and (b) fire-induced faults in the circuit (cable) can prevent the operation or cause a mal-operation of the shutdown system in which the component(s) is located. Power and control cables of pump P-1 in Figure A-2 and control cables of valve V6 are typical examples of "required cables." In contrast, "spurious non-safety 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-2 are examples. Although not needed to assure operation of the credited shutdown systems, fire damage to circuits such as these could significantly impact the shutdown capability.

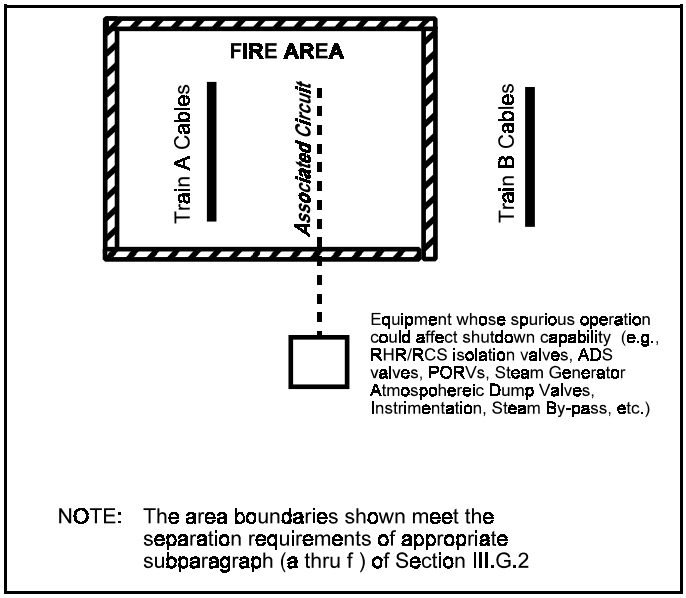


Figure 39Figure A-1 Spurious Operation Associated Circuits of Concern (Ref: GL 81-12 Clarification, Enclosure 2)

The achievement of safe shutdown is dependent on assuring the active control of some components and preventing the maloperation of other components. A post-fire safe shutdown analysis (SSA) should be a bounding analysis that identifies the range of possible fire impacts within each fire area (vulnerabilities) and assures 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 assure operation of credited shutdown *systems*. The scope of successful shutdown strategies also includes consideration of the effects of fire damage to non-essential equipment and systems whose inadvertent or spurious actuation could impact the shutdown *capability*.

As described in this document, a common approach for assuring 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, decay heat removal). With the shutdown paths and systems defined, equipment needed to ensure the proper operation of the credited shutdown systems (required components) and non-essential/non-safety equipment or systems whose spurious actuation could impact the shutdown capability are then be identified and documented on a *Safe Shutdown Equipment List* (SSEL). As a result of this process, the SSEL will include all components (essential and non-essential) whose damage due to fire could impact the shutdown capability and will not be limited to only those components needed to assure the operation of the defined shutdown systems. From this comprehensive listing of equipment, the SSEL can then serve as a starting point for identifying cables and circuits of concern to post-fire safe shutdown in each fire area.

Resolving Potential Vulnerabilities

When cables /circuits 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 assuring that an appropriate level of fire safety is achieved. Typical examples include:

1. Assuming that fire damage to affected cables/circuits 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), or

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

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 Section 6) to all exposed cables/circuits of concern will not impact the shutdown capability, or

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.

Defining The Scope of Circuits Requiring Detailed Review (Screening)

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 non-compliance 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 Appendix R Section III.G.2), 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 cables/circuits whose damage due to fire would not impact safe shutdown), it is desirable to limit its scope to only those cables/circuits whose damage due to fire could actually impact the shutdown capability. 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 Section 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"motor-operated valves V-3, V-7, V-8, V-9 and V-10 shown in Figure A-2, 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 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, V-7, V-8. 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.

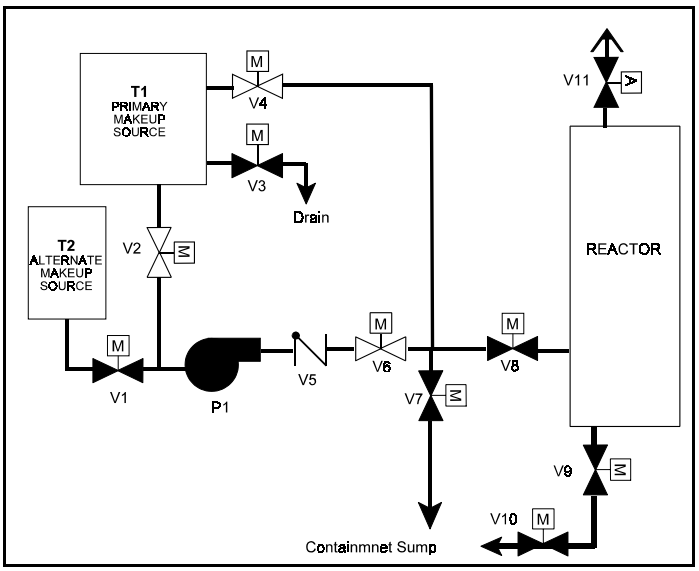


Figure 40Figure A-2 Simplified Shutdown System Flowpath

Resolving Specific Circuit Breaker Coordination Issues

In certain instances, it may not be practical (or possible) to achieve full coordination between electrical protective devices of a power supply required for post-fire safe shutdown (see Section 6.2.5.2). For cases such as this, evaluations that consider the specific impact of fire-induced failures at the fire location have been found to limit the extent of modifications that may otherwise be needed to achieve compliance with the regulation. For example, certain plants have demonstrated that certain coordination deficiencies may be successfully resolved by providing fire protection features (electrical raceway fire barrier system) to only a limited portion (length) of the potentially affected cables. An application of this approach is illustrated in Figure A-3. In this case, the plant's circuit coordination study has determined that required power source PS-1 lacks an acceptable level of coordination. Specifically, the the trip characteristics of load breaker CB-3 do not coordinate with the trip characteristics of feed breaker CB-1. As a result, fire-induced shorts to ground at any location along the entire length of the load cable connected to CB-3 could cause CB-1 to trip before CB-3 actuates. For post-fire safe shutdown this lack of coordination is unacceptable because a trip of CB-1 would result in a loss of electrical power to a required shutdown component (P-1). While replacing circuit breakers CB-1 and/or CB-3 with devices that fully coordinate is the preferred resolution, in this case such a modification is not deemed practical. Through the performance of additional evaluations, however, it is determined that power source PS-1 is only required to remain operational in the event of fire in FA-2, FA-4 and FA-6. Additionally, a review of cable routing data indicates that PS-1 is only vulnerable to failure in the event of fire in FA-4 or FA-6. Finally, by considering the specific effects of fire damage in FA-6, it is learned that the increased impedance provided by the length of cable between PS-1 and the actual fault location (the distance between CB-3 and the point where the cable enters FA 6) is sufficient to limit the available level of fault current

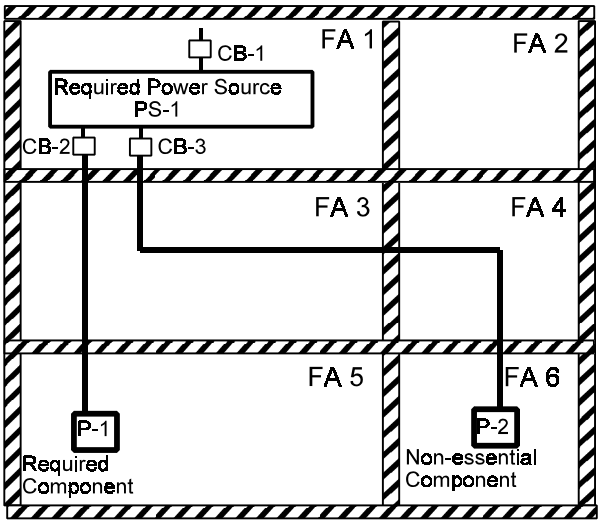


Figure 41Figure A-3 Resolving Coordination Deficiencies

to a value that will allow full coordination between CB-3 and CB-1. As a result of this process, the only portion of the load cable that is of concern to post-fire safe shutdown is a relatively small section that is routed within FA-4. As a result of this evaluation process the licensee now has several options available for achieving compliance with Appendix R. For example, the section of cable that is located within FA-4 may be wrapped with an electrical raceway fire barrier system, or it can be re-routed outside of the area (e.g. through FA-5).

Use of Alternate Equipment

Nuclear power plants typically contain a diversity of systems that may be configured to perform required safety functions. Consequently, the simplest and most viable option for resolving fire vulnerabilities in a given fire area or zone is to use other systems or equipment that are capable of performing the desired shutdown function but located outside the area of concern. This approach may be very broad, involving a complete revision of the method and systems selected to accomplish safe shutdown, or limited to verifying the availability a single piece of equipment. Since this approach can be readily accommodated by procedural changes and operator training, its implementation is highly cost effective.

Use of Manual Operator Actions

The use of manual operator actions to mitigate the possible effects of fire damage may provide a cost-effective approach to resolving identified vulnerabilities. As discussed in Section 5, however, this approach requires careful consideration of several important technical and operational concerns. Shutdown methodologies that have been found to successfully incorporate the use of manual operator actions address each of the following factors:

- ***Time:***

  There must be sufficient time for manual safe shutdown equipment manipulations to take place before the safe shutdown capability is jeopardized. The time available to perform manual realignment of equipment will vary significantly according to the specific system or component affected, and the location complexity of the manual alignments to be performed. For example, the time available to close a manual valve to mitigate flow diversion from a required system flow path depends largely on the size of the flow diversion path, the time for operators to reach the valve location, and the time to manually close the valve. Therefore a thermo-hydraulic timeline must be performed to ensure that all manual actions can accomplished before unrecoverable conditions occur. The evaluation should assume the failure takes place at the onset of fire unless it can be shown that adequate means (e.g., instrumentation, procedures, and training) are available for operators to "detect and defeat" the fire-induced failures before they cause the plant to enter an unrecoverable transient condition. In addition, there must be sufficient margin between analytical results derived from the thermo-hydraulic analysis and the actual time needed for operators to perform required actions (as determined from procedure walk-down validation/verification efforts). At least five (5) minutes of margin is appropriate. For example, if the thermo-hydraulic analysis indicates that 30 minutes are available to establish AFW flow in a PWR, it would be

expected that all manual actions necessary to establish AFW would be completed in 25 minutes or less.

•***Environment:***

The ability of operators to access the fire area where the manual actions are to be performed must be demonstrated. This evaluation should examine the environmental conditions in the fire area, as well as the routes to be traveled by the operator before and after the action is performed. Factors to be considered include radiation exposure rates, temperature, humidity, smoke and/or hot gases resulting from fire, fire suppression activities, and flooding. Radiation levels should not exceed normal 10 CFR Part 20 limits. Temperature and humidity limits should be acceptable based on OSHA guidance. Fire effects should be reviewed to ensure that smoke and toxic gases from the fire do not affect the capability to perform the manual action.

Typically, operator actions inside a fire-affected area or zone should not be credited unless it can be demonstrated that the action will not be required before the fire is fully extinguished and suitable environmental conditions are restored. It is the staff's judgement that where manual actions, including valve alignment and pump control, are required less than one-hour (sixty-minutes) after initial fire damage, an insufficient margin of safety exists to provide reasonable assurance that safe shutdown can be achieved and maintained. For those actions which must be taken beyond 60 minutes, the staff concludes that a sufficient time margin exists which provides reasonable assurance that these actions can be achieved in the time required. In addition, it must also be assured that fire damage within the fire area does not prevent completion of the action.

• ***Lighting:***

The availability and adequacy of plant lighting necessary to accomplish all required shutdown tasks should be demonstrated. This evaluation should examine plant lighting illumination requirements in the compartment where manual operations are performed, as well as in any access and egress routes traveled by the operator. Emergency lighting should be provided as required in Appendix R, Section III.J or by the licensee's approved fire protection program.

• ***Communications:***

A reliable communication system is essential to coordinate reactor shutdown activities between operators located in remote locations of the plant and operators stationed in the control room or remote shutdown panel(s). There are several types of "normal" plant communications systems (telephones, sound-powered phones, paging systems, and portable radios) already installed that may be used where possible. However, due to the location of equipment or connected cabling, these systems may be lost or unreliable during certain fire events. In such cases, or, where the performance (operation and effectiveness) of existing communication systems during fire has not been evaluated, a new, independent, communication system may be necessary. In certain cases portable radios may be used by

several organizations (e.g., fire brigade, security, and plant operations personnel). In such cases at least one channel should be reserved and designated for use by plant operators performing post-fire safe shutdown activities. The specific type of communication system selected should consider the effects of fire on its operation and its availability, reliability, and adequacy of operation in all areas of the plant where manual actions are performed.

- ***Equipment:***

  Manual safe shutdown actions should be reviewed to determine the need for supplemental repair equipment and tools. If required, these items should be readily available to the operator at all times, preferably stored at the location of the manual action and dedicated for use during post-fire shutdown procedures. For example, if the operator action involves the removal of fuses, a fuse puller should either be stored at the fuse panel or made available to the operators prior to performing the activity. Additionally, administrative procedures should be in effect to provide periodic verification of the availability and condition of any required tools and equipment.

- ***Manpower:***

  It must be demonstrated that a sufficient number of operating personnel will be available to support all manual reactor safe shutdown actions that may be needed in the event of fire in conjunction with all other activities necessary to shutdown the reactor and mitigate/suppress the fire.

- ***Procedures and Training:***

  All manual operator actions should be governed by established plant abnormal or emergency operating procedures, and operators should be trained in their implementation. All actions must be verified and validated by plant walkdowns using the current procedure. Procedure walkdowns must be timed to assure accomplishment within required timeframes specified in the plant's thermo-hydraulic timeline and safe shutdown analysis (with margin). The training program should include drills (practice sessions) demonstrating the feasibility of performing the required actions. Operators should not rely on having time to study plant procedures to find a method of operating plant equipment that is seldom used.

Specific Examples

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

I. Coordination of Electrical Protection Devices

Case 1: Potential for Secondary Fire Initiation

Problem: During a re-evaluation 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 switchgear. If the associated switchgear 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 switchgear and (2) the fire must occur in a fire zone other than where the switchgear 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 switchgear 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 switchgear. 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 switchgear 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 switchgear. 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 switchgear 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 licensee of a PWR discovered that a 125VDC 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 125VDC 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. 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 through the implementation of a plant modification to enclose the power cable in a one-hour rated fire wrap.

II. Circuit Faults

Case 1: Incompatible "Hot Short" Between Conductors (120VAC to 24VDC) Could Result in a Loss of the Service Water System.

Problem: In 2000 the licensee of a BWR discovered that a fire-induced circuit fault resulting from fire in the cable spreading room 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 24VDC 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 24VDC start control circuits to be energized by 120VAC power. This condition could disable the automatic starting and running of the pump relied on to provide cooling water to the the service water pump gland seals. The service water pumps are required to operate during an 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 2 : 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 due to fire would result in 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 a motor-operated valve located in the VCT supply line could cause the valve to shut. Although an alternate source of water is available from the 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 3: Potential Loss of All Vital Buses Due to Multiple Faults In Ungrounded DC Control Circuits

Problem: The alternative shutdown (ASD) strategy developed by a licensee of a PWR relied on manual operator actions to isolate 125VDC control power to breakers of 4kV switchgear. 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) re-assessment of its safe shutdown analysis, however, the licensee discovered that in the event of fire in certain ASD 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 4kV circuit breaker 125VDC 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 busses.

Since the 125VDC 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, local actions to remove 125VDC control power from the breakers was considered adequate to isolate the 4kV breakers from the alternate 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 Generic Letter 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 4: Spurious Opening of Multiple Safety Relief Valves

During a reevaluation for compliance with Appendix R to 10CFR50 the licensee of a BWR determined that a control room or relay room fire could cause multiple Safety Relief Valves 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. Due to the potential for fire induced failures high-volume make-up systems capable of mitigating this event (Core Spray, RHR-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 eleven DC operated Safety Relief Valves (SRV), of which seven Automatic Depressurization System (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 assure 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.

PRELIMINARY DRAFT
December 2002

APPENDIX B

SPECIFIC CIRCUIT ANALYSIS ISSUES

This appendix describes NRC expectations regarding certain circuit analysis issues. The specific issues discussed in this section have been the subject of much confusion and debate and include: Multiple Spurious Actuations, Fire Damage to Non-essential Systems, and Multiple Circuit Faults. Staff expectations are described in terms of "real world"examples of technical issues that were identified during the review of safe shutdown analyses developed by various licensees.

I. Multiple Spurious Actuations

In Section 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 the design of the alternate 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 by licensee's 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 cables and circuits. 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 assuring 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 in the following examples:

- At one PWR cooling water flow to the emergency diesel generator (EDG) is provided by either one of two parallel flowpaths. Since a "normally open" motor-operated valve 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 Q 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 cables/circuits within each fire area, the licensee had dispositioned this potential vulnerability on the assumption (per its interpretation of GL 86-10 Q 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 Section 6, the Safe Shutdown Equipment List (SSEL) identifies equipment that is needed to assure 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 prior to fire damage, 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 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 cables and circuits whose damage due to fire could impact the shutdown capability, 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 Safe Shutdown Analysis (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 Generic Letter 86-10 does not require the assumption of multiple hot shorts for non-hi/lo 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 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, non-concurrent). 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 of equipment whose spurious operation could affect safe shutdown were identified, they were included as required cables into the licensee's Appendix R separation analysis.

- The licensee of a BWR attempted to use 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 (<15 feet), the licensee did not consider the separation requirements of Section III.G.2 to be applicable on the basis that both (two) 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 10CFR50 requires, in part, that circuits and cables that could prevent operation or cause maloperation of structures, systems and components important to safe shutdown be provided with a level of fire protection necessary to ensure that they such circuits will remain free of fire damage. Consistent with the deterministic approach described in Section 6, cables and circuits 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, due to 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 Nuclear Energy Institute (NEI) dated March 11, 1997, the staff reiterated its position that 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 can not be predicted.

As described in Section 6 and Appendix A of this document, licensees are expected to identify equipment (safety-related and non-safety related) whose spurious operation could impact the safe shutdown capability described in the plant-specific Safe Shutdown Analysis (SSA). Following their identification, the routing of cables and circuits connected to this equipment should be identified and an evaluation performed to determine the potential for fire-induced faults to cause the connected equipment to spuriously actuate. If it can be demonstrated through the performance of a detailed circuit analysis 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 mal-function in a manner that would adversely impact the post-fire safe shutdown capability, fire protection features would not be necessary, and the component may be screened from further evaluation. In the absence of such an analyses, however, it must be assumed that the component will mal-operate as a result of fire damage to its potentially affected cables.

As discussed in Section 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 occur as a result of a postulated fire should be identified. While it is not assumed that all potential spurious actuations will occur instantaneously at the onset of fire, the analyst must consider the possibility for each spurious actuation to occur sequentially, as the fire progresses, on a one-at-a-time basis. For example, if control cables of two normally-closed MOVs are subject to damage, the potential for both valves to spuriously open as a result of fire damage can not be ignored. Since the control cable of neither valve is assured 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. Manual operator actions to mitigate this event may provide an acceptable resolution; provided: (a) they are developed and implemented in accordance with criteria described in Appendix A; (b) sufficient diagnostic instrumentation is known to be available (free of fire damage) to enable operators to promptly detect the spurious actuations; and (b) it is demonstrated that all required actions can be accomplished in a sufficiently timely manner before an unrecoverable condition is achieved. 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 actions which require one of the valves to be ensured closed by local manual operator actions.

II Fire Damage to Non-essential Systems

Fire damage to systems that are not needed to perform an essential shutdown functions (i.e., non-essential or non-safety systems) can have a significant impact on shutdown capability. For example:

- 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 54" 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 Main Steam Isolation Valves (MSIVs), closing of the feedwater discharge valves, and tripping the feedwater turbine from outside the main Control Room.

- The normal charging line to the Reactor Coolant System (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, 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 Safe Shutdown Equipment List. 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 Pressurizer Auxiliary Spray valve due to 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 on-site 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 Section 6 and Appendix A, the achievement of safe shutdown is dependent on assuring the active control of some components and preventing the maloperation of other components. A post-fire safe shutdown analysis (SSA) should be a bounding analysis that identifies the range of possible fire impacts within each fire area (vulnerabilities) and assures 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 assure operation of credited shutdown *systems*. The scope of successful shutdown strategies also includes consideration of the effects of fire damage to non-essential equipment and systems whose inadvertent or spurious actuation could impact the shutdown *capability*.

III. Multiple Circuit Faults

In Generic Letter 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 that 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 Safety Relief Valves (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.