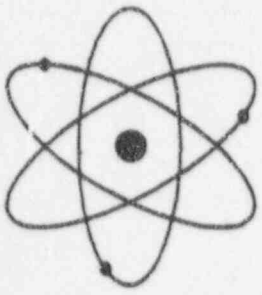

ERI/NRC 95-502

TECHNICAL EVALUATION REPORT ON THE SUBMITTAL-ONLY REVIEW OF THE MCGUIRE NUCLEAR STATION INDIVIDUAL PLANT EXAMINATION OF EXTERNAL EVENTS

DRAFT **REPORT**

February 1996

Energy Research, Inc.
P.O. Box 2034
Rockville, Maryland 20847-2034

Work Performed Under the Auspices of the
United States Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, D.C. 20555
Contract No. 92-04-050

The study defines vulnerabilities as "unduly significant sequences." It finds no vulnerabilities from external events. Although cut sets differ somewhat between the previous 1984 PRA and the IPEEE, the overall dominance of loss of offsite power has not changed.

The total calculated seismic core damage frequency is 1.1×10^{-5}/yr. The submittal states that the accident sequences that are the most important risk contributors involve loss of offsite power with subsequent loss of diesel generators. Recovery of offsite power and diesel generators is assumed to fail. Loss of nuclear service water is also an important contributor. The top thirteen cut sets involve 51% of the seismic core damage frequency. Of these, five are directly related to loss of offsite power and diesel generator failure; two involve loss of offsite power and failure of 125V DC which, in turn, prevents diesel generator startup; four are related to loss of both trains of nuclear service water; and two involve a combination of loss of diesel generator and nuclear service water. The study apparently assumes, even though it is not stated, that an earthquake will cause a reactor trip and a turbine trip.

LOCAs are screened out because (1) mechanical and structural equipment, which could fail in a way that causes a LOCA, are of high capacity, and (2) no bad-actor relays are associated with the potential for a LOCA. The governing failure mechanisms of the ice condenser function are collapse of the surrounding containment and crane supports which are of high capacity.

The relay review found that bad-actor relays, associated with the IPEEE equipment list, served an alarm function rather than a control function. No further fragility evaluation is performed on these relays, although relays are included in the systems analysis.

The submittal states that soil tests during construction indicate that soils under Seismic Category I structures are not susceptible to liquefaction. Findings relevant to specific issues are as follows:

USI A-45. Section 6.0 of the Individual Plant Examination (IPE) reports the calculated core damage frequency owing to failure of decay heat removal systems from external initiators is 10^{-5}/yr, with a seismic contribution of 7.8×10^{-6}/yr.

Generic Issue (GI)-131. Previous seismic analysis of the interaction of the movable in-core flux mapping system indicates that the restraints are adequate to prevent seismic interaction and breach of the pressure boundary.

Eastern U.S. Seismicity Issue. A sensitivity study was performed using the 1989 Lawrence Livermore National Laboratory (LLNL) hazard curves for McGuire. Cut sets of the top contributors and the total fractional contribution of each cut set to core damage frequency are not found to be significantly different.

USI A-17. The walkdowns identified a few minor seismic interaction issues which were corrected and identified as plant enhancements in Table 3-3 of the submittal. The licensee states that the walkdown did not identify significant interaction concerns.

1.1.2 Fire

The McGuire fire IPEEE is an update of the full scope, Level 3 PRA performed between 1981 and 1984. The update was started in 1988. Significant plant features relative to the fire analysis are the Standby Shutdown System, Appendix R separation between redundant trains, and ability to cross-connect nuclear

service water between units, with only one nuclear service water train required to supply the water needs of both units. Instrument air is also shared between units.

The following summarizes the fire IPEEE procedure used for McGuire.

The fire areas are reviewed during the walkdown to determine if an area could cause one or more initiating events. The areas that would not are screened out. The remaining areas are reviewed to determine the initiating event that gives the "worst case result" involving a fire in that room. The submittal states: "The risk from other possible scenarios is judged to be bounded by the risk from the scenarios examined."

Fire initiating event frequencies are developed using a database containing fire events through 1986 from Licensee Event Reports (LERs) and an EPRI study published in 1983. For most areas, fire initiating event frequencies are based on the selected components of an area. Where a component is selected to represent an area, the frequency of fire of that component is used rather than the frequency of all sources in that area. However, the fire initiation frequencies for the control and cable rooms are based on the ability of fires to occur in the entire area.

Each area is screened based on (1) whether the probability of damage for the worst case scenario is less than 10^{-6} per year, or (2) whether the fire damage probability is less than the internal events frequency of the same or similar scenario(s). The latter screening process is an important factor in understanding the low frequency of fire-induced core damage that is assessed for McGuire. The screening is performed using a Gallucci style fire event tree. The fire detection, suppression and propagation parameters of the event tree are based on NUREG/CR-0654, judgmentally adjusted to account for plant-specific features in each area. Analytical or tabular methods, such as COMPBRN and Fire Vulnerability Evaluation (FIVE), are not used to determine fire propagation potential.

Fire-induced failures are combined with random failures using the transient functional event tree/fault tree model to obtain an estimated core damage frequency. Fires in the control room and cable room are combined under the assumption that they had the same effect on the plant, namely, loss of nuclear service water.

The walkdown was performed to verify assumptions about plant configuration, locate cable runs, and address the Sandia Fire Scoping Study issues. The walkdown team was composed of two fire protection engineer, a PRA analyst, and a Program Manager, all from DPC. Peer review of the walkdown was performed by a fire protection engineer from Catawba.

The study identifies no vulnerabilities, which are defined as an "unduly significant sequence" (Page 1-3 of Reference [1]).

Five areas survive the screening. The assumed control room and cable room scenario is loss of nuclear service water; the assumed auxiliary shutdown panel scenario is loss of nuclear service water; the assumed vital instrumentation and control (I&C) battery area scenario is loss of nuclear service water; and the assumed main feedwater pump scenario is loss of offsite power.

Using the IPE model transient functional event tree and fault trees in Section 2 of Reference [4], cut set frequencies sum to a total fire core damage frequency of 2.3×10^{-7}/yr, which is less than 1% of the total core damage frequency of 7×10^{-5}/yr. The fire sequence for main feed pump fire falls into the TBU

functional sequence category. This type of sequence involves a transient with failure of secondary side heat removal (B) and failure of safety injection (U). Cable, control, and Vital I&C area fires, which are assumed to be equivalent to loss of nuclear service water, are identified as TQsU sequences. These sequences involve a transient with reactor coolant pump seal LOCA and failure of safety injection.

The most significant walkdown insight is the identification of the potential to lose nuclear service water from a fire in the Vital I&C area. A fire in this area could potentially affect both a Unit 1 train B cable and the 1EVDA panel board which houses control power for the train A 4160V breakers of nuclear service water.

It was also noted during the walkdown that water from suppression systems can migrate from the upper to lower switchgear room. A bounding core damage frequency of 3×10^{-6}/yr is estimated. This situation is neither included in the risk analysis nor identified as a vulnerability, because the actual core damage risk is judged to be much lower than the bounding estimate.

The report states that the walkdown verified that plant areas can adequately deal with smoke damage because of adequate ventilation or large spaces.

1.1.3 HFOs

The Licensee has conducted a detailed analysis of some High Winds, Floods and Other External Initiators (HFOs). This review has found some strengths and a number of weaknesses, which are summarized in Section 3.3 of this review.

The McGuire IPEEE submittal finds no unduly significant sequences (vulnerabilities) with respect to HFOs. The most significant contributor to the CDF due to external events was an HFO event (i.e., tornado). The report estimates that tornado events make up 63% of the CDF from external events. This is followed by seismic events that contribute about 36% of the external event CDF. Tornado-induced events are considered as non-recoverable losses of offsite power. The dominant sequences for tornado are those involving failure of the diesel generators to operate.

1.2 Overview of Review Process and Activities

1.2.1 Seismic

The seismic analysis of the IPEEE is reviewed for methodological completeness, accuracy and consistency with other studies. Rather than an independent set of calculations, the review uses experience based comparisons of other plants and other seismic assessments to judge the accuracy and completeness of the information provided by the licensee. The review covers the seismic aspects of References [1], [4] and [23]. In addition, References [5] and [6] are briefly reviewed for background.

This document provides observations by the review team regarding the IPEEE as defined in Generic Letter 88-20, Supplement 4 and NUREG-1407.

The review process is consistent with the review guidance documents of References [7] and [8]. The scope of the review covers elements of methodology, data, results, and insights. The review is conducted with an eye toward consistency with currently accepted methods, as well as the guidance in NUREG-1407. Data elements include equipment lists, hazard curves, fragilities, failure probabilities,

system model structure, and basic events. Results include minimal cut sets, core damage frequency and fractional contribution of cut sets, and effect of containment on risk.

The review team has not verified whether the data presented in the IPEEE matches the conditions of the plant, and whether the actions and procedures described are indeed implemented. Furthermore, independent calculations to verify results have, in general, not been performed.

1.2.2 Fire

The fire analysis of the IPEEE is reviewed for methodological completeness, accuracy and consistency with other studies. Rather than an independent set of calculations, the review uses experience based comparisons of other plants and other seismic assessments to judge the accuracy and completeness of the information provided by the licensee. The review covers the fire aspects of References [1], [5] and [23]. In addition, References [4] and [10] were briefly reviewed for background.

The review process is consistent with the review guidance documents of References [7] and [8]. The scope of the review covers elements of methodology, data, results, and insights. The review is conducted with an eye toward consistency with currently accepted methods, as well as the guidance in References [2] and [3]. Special attention is given (1) to the screening methodology, because a trend to prematurely screen out potentially significant areas or to inadequately justify screening out an area has emerged as a common problem among past fire PRAs and IPEEE analyses, and (2) to assumptions, because the results of many studies are unduly influenced by assumptions made to simplify or introduce conservatism. Other methodology elements include, for example, development of fire event trees, fire propagation, suppression and detection, and systems modeling. Data elements include such items as cable routing, fire area partitioning, fire initiation frequency, detection and suppression frequencies and recovery probabilities. Results include such items as minimal cut sets, core damage frequency and fractional contribution of cut sets, identification of important fire areas and scenarios, and effect of containment on risk.

The review team has not verified whether the data presented in the IPEEE matches the conditions of the plant, and whether the actions and procedures described are indeed implemented. Furthermore, independent calculations to verify results have, in general, not been performed.

1.2.3 HFOs

The HFO evaluation involved review of the High Winds, External Floods, Transportation and Nearby Hazardous events. The purpose of this review is to: (1) verify that the IPEEE submittal is in accordance with the information requested in Supplement 4 to Generic Letter 88-20, and associated guidance described in NUREG-1407; and (2) identify and summarize important IPEEE insights and findings.

The review process closely follows the guidance provided in the IPEEE Step 1 Review Guidance Document [8]. This process involves examination of the methodology, the data used, the results and the conclusions derived in the submittal. The methodology has been reviewed for consistency with current acceptable practices. Special attention has been placed on the adequacy of data bases used to estimate the frequency of HFO events. The consistency of the results with the conclusions derived in the submittal has been reviewed. The computations for frequency of occurrence of hazards and fragility estimations have been checked.

2.1.15 Treatment of GI-131

Previous seismic analysis (circa 1985) of the interaction of the movable in-core flux mapping system indicates that the restraints are adequate to prevent seismic interaction and breach of the pressure boundary.

2.1.16 Other Safety Issues

Regarding the Eastern U.S. Seismicity Issue, a sensitivity study was performed using the 1989 Lawrence Livermore National Laboratory (LLNL) hazard curves for McGuire. Cut sets of the top contributors and the total fractional contribution of each cut set to core damage frequency are not found to be significantly different.

Regarding USI A-17, the walkdowns identified a few minor seismic interaction issues which were corrected and identified as plant enhancements in Table 3-3 of the submittal. The licensee states that the walkdown did not identify significant interaction concerns.

2.1.17 Process to Identify, Eliminate or Reduce Vulnerabilities

The licensee used the PRA process, coupled with the walkdown, to identify vulnerabilities. No vulnerabilities were found. The walk down resulted in enhancements to reduce minor seismic spatial interactions as addressed in Table 3-3 of the submittal, under the title of Enhancements Resulting from the IPEEE Seismic Verification Walkdown.

2.1.18 Peer Review Process

A peer review was conducted in-house by a group of managers and senior engineers from the Catawba and Oconee stations. The focus points of the review are selection of areas and equipment, evaluation process, walkdown process and judgments, documentation, and results.

2.2 Fire

2.2.1 Documents Reviewed

The review covered the fire aspects of References [1] , [5] and [22]. In addition, References [4] and [10] were briefly reviewed for background. This document provides observations by the review team regarding the IPEEE as defined in Generic Letter 88-20, Supplement 4 and NUREG-1407. The review process is consistent with the review guidance documents of References [7], [8], and [9].

2.2.2 Methodology Selection

a. Method Selected For Fire IPEEE

The McGuire Fire IPEEE updates an existing PRA to account for the as-built plant. A walkdown was performed to verify assumptions about plant configuration, locate cable runs and address the Sandia Fire Scoping Study Issues.

b. Key Assumptions Used in Performing Fire IPEEE

The study's assumptions essentially govern the results:

- The study assumes that use of worst case fire scenarios in each area, instead of a variety of scenarios, is a conservative approach for calculation of core damage frequency and identification of vulnerabilities. This approach is used even if the selected scenario did not encompass the total fire frequency of the area.

- The study assumes that the effect of all control room fires, cable room fires, and fires in the Vital I&C area are identical, and have the same effect on the plant as loss of nuclear service water.

- The study assumes that locations in the plant may be dismissed on the basis that the fire equipment damage scenario frequency is less than the internal event frequency for the selected equipment in the area. Areas (equipment) dismissed on this basis are Auxiliary Building 733 (Switchgear); Auxiliary Building 716, Space 649 (Nuclear Service Water Pump); Auxiliary Building 767, Rooms 926 and 933 (Reactor Trip Switchgear and Control Room HVAC); Auxiliary Building 733, Room 723 (Component Cooling Water); Diesel Generator 1A; Turbine Building, except for the main feed pump area; Service Building 739 (Instrument Air); and Containment (Reactor Coolant Pumps [RCPs] and Power-Operated Relief Valves [PORVs]).

- The study assumes that if fires cause control fuses to blow before control equipment is tripped, then there is no fire damage that would cause core damage.

- The study assumes that the parameters of NUREG/CR-0645 are applicable to the simplified event tree it uses.

- The study assumes multiple opportunities for suppression without calculating either timing of suppression or fire growth.

- The study assumes that damage from fire suppression systems and smoke are insignificant when compared to damage owing to heat from fires, and are not included in the analysis. This assumption may be an artifact of the procedure in which transient combustible fires are not treated, and cabinet fires are treated in only a few locations. Typically, smoke and soot deposition on relays, contacts, and breakers can cause them to fail to actuate, and is an important concern in cabinet and pool fires.

c. Status of Appendix R Modifications

The submittal indicates that McGuire is in compliance with Appendix R.

2.2.3 Review of Plant Information and Walkdown

a. Walkdown Team Composition

The walkdown team was composed of two fire protection engineers, a PRA analyst, and the Program Manager, all from DPC, with peer review of the walkdown performed by a fire protection engineer from Catawba.

b. Significant Walkdown Findings

The walkdown was performed to verify assumptions about plant configuration used in the PRA, and to address the Sandia Fire Scoping Study Issues. The walkdown findings were an incentive to update the McGuire fire PRA, as documented in Revision 2 of Section 3.5 of Reference [1]. The most significant change to the PRA is the identification of the potential to lose nuclear service water from a fire in the vital I&C area. A fire in this area could potentially affect both a Unit 1 train B cable and the 1EVDA panel board, which houses control power for the train A 4160V breakers of nuclear service water. Thus, both trains of nuclear service water could be affected by the same fire. It was also noted during the walkdown that water from suppression systems can migrate from the upper to lower switchgear room. A bounding core damage frequency of 3×10^{-6}/yr is estimated. This situation is neither included in the risk analysis nor identified as a vulnerability, because the actual core damage risk is judged to be much lower than the bounding estimate. The report states that the walkdown verified that plant areas can adequately deal with smoke damage because of adequate ventilation or large spaces.

c. Significant Plant Features

Significant plant features relative to the fire analysis are the Standby Shutdown System, Appendix R separation between redundant trains, and ability to cross-connect nuclear service water between units, with only one nuclear service water train required to supply the water needs of both units. Instrument air is also shared between units.

2.2.4 Fire-Induced Initiating Events

a. Initiating Events Considered

The following initiating events are considered: plant trip, loss of offsite power, loss of main feedwater, loss of nuclear service water, loss of component cooling, loss of control area ventilation, loss of 4160 V essential power, loss of auxiliary shutdown panel, loss of vital instrumentation and control power (125V DC and 120V AC), loss of instrument air, and loss of coolant accident.

b. Analysis of Initiating Events

The fire areas were walked down to determine if an area could cause one or more initiating events. Questionnaires were filled out for each area. Areas that are deemed to not cause an initiating event are screened out.

The initiating event criterion used for the initial screening of rooms is not always reasonable. While there are areas in the plant that would not cause an initiating event, some of these areas (for example, #1 Auxiliary Building loss of Residual Heat Removal [RHR] pumps or Dog House loss of auxiliary feedwater valves) could initiate a manual shutdown owing to technical specification Limiting Conditions of Operation (LCOs). Manual shutdown also puts a demand on systems (e.g., auxiliary feedwater and RHR) that may be disabled by the fire. One of the principle reasons for performing a fire analysis is to investigate situations that cause a plant shutdown and also disable needed equipment. Other licensee's have performed a detailed investigation into how operators would react to fires in each fire area. This includes interviews with senior operators. This was not done in this study.

2.2.5 Screening of Fire Zones

DRAFT

a. Screening Methodology

The screening analysis is performed at two levels. First, fire areas are reviewed to determine if an area can cause one or more initiating events. The areas that can not are screened out. The surviving areas are assigned a "worst case result" scenario as described in Section 1.1.2.1. Second, each area is screened based on (1) whether the probability of damage for the worst case scenario is less than 10^{-6}/yr, or (2) whether the fire damage probability is less than the internal events failure probability for the same equipment. The screening uses a Gallucci style fire event tree. The parameters of the event tree are based on NUREG/CR-0654, adjusted for each area.

NUREG/CR-0654 was published in 1979 to provide a reasonably simple yet technically comprehensive approach to aid designers and regulators of fire protection systems. It recommended three approaches: a deterministic approach, a probabilistic approach, and a qualitative approach. The recommended probabilistic approach is called a critical-path technique, and was developed in 1976. A critical path diagram shows alternative paths of fire ignition, growth, discovery or detection, suppression or self-extinguishment. Multiple opportunities for suppression and detection are allowed in a path. The events in the diagram are associated with judgmentally (and statistically, when data existed) determined numbers between zero and one, provided in Table 4 of Reference [10], which are called probabilities. The table also provides qualitative criteria to guide the selection of the probabilities. The authors of NUREG/CR-0654 point out that the conservatism of the method depends on the conservatism of the probabilities selected. The probabilities used by the licensee, as discussed in Section 2.2.9 below, tend to overestimate the probability of suppression, in comparison with accepted data, thereby underestimating the fire risk. Furthermore, the event tree provided in the submittal is only an approximation of the more detailed and explicit critical path diagram in Reference [10]. Reference [10] states "it was necessary to visualize events at particular stages of fire development so that a valid estimate of the probability of success or failure could be made." The critical path diagram included parameters such as area of potential air-intake openings, fuel continuity, fuel availability, and penetration of barriers, all of which do not appear on the licensee's fire event tree. Therefore, the use of these probabilities in the simplified event tree used by the licensee may not be valid.

Selecting a "worst case result" scenario for a room is valid if the probability of all potential core damage scenarios for the room is accounted for. Except for the control and cable rooms, this is not the case in the McGuire study. During both screening and cut-set quantification, this study quantifies the frequency of the selected scenarios only. If an argument could be made to probabilistically screen out the selected scenario, the entire area was screened out. Cut-set quantification is performed only for the remaining areas, and not for all the scenarios that can occur from fires in the area. This procedure results in prematurely screening out rooms, the potential to miss vulnerabilities, erroneous perception of risk contributors, and underestimation of core damage frequency.

Using a screening criterion that eliminates rooms because fire damage to selected equipment within a room is less than the internal events value is not a method that can identify fire vulnerabilities and provide a useful measure of fire-induced core damage frequency. If a fire-induced equipment damage scenario has a lower frequency than a similar IPE equipment damage scenario, then the entire area is screened out. For example, the Diesel Generator 1A space contains cables of two MSIVs, and thus could cause a unit trip owing to a large fire. The estimated frequency of a large fire in that room is 6.6×10^{-4}/yr, which is lower than that in the internal event analysis, and is screened out. However, this value is more than three

orders of magnitude higher than the total calculated fire core damage frequency. Another similar example is the argument for screening out loss of control room HVAC. This argument ignores the issue that a large fire in that room might also fail equipment assumed to have a chance of operating in the internal events analysis. This criterion might be reasonable for areas in which there is no potential of a fire to spread from one piece of equipment (e.g., a pump) to cables or cabinets of other equipment. For example, screening out specific components such as the reactor coolant pumps and the nuclear service water pumps may be reasonable in this study, if cables or cabinets from other systems are unaffected by fires from these pumps.

Using a 10^{-6}/yr screening criterion is reasonable, as is using a fire event tree as a quantitative method for screening. Interestingly, the estimated frequencies for loss of one switchgear, the control room, the cable room, or one train of component cooling are identical to those estimated frequencies for Catawba.

Except for 4160 V switchgear, reactor trip switchgear, and the auxiliary shutdown panel in the auxiliary feedwater area, cabinet initiated fires are not included in the analysis The licensee's rationale for this is that cabinet fires are to less likely to damage the component of interest in a room (e.g., diesel generator or component cooling water pump), than a fire initiated at the component itself. This is invalid, of course, because a cabinet fire can damage the component's MCC or control cables.

All of the selected sequences for fire areas involved transients. The submittal briefly addresses a fire-induced LOCA in the control room, cable room, and containment. In all three cases, it is argued that because power can be removed from the pressurizer PORVs from outside of the control room, if they fail open by a fire, such an occurrence is not a concern and not further examined. The potential ability to remove power during a fire does not equate to a certainty that the event will occur. This is particularly the case for a control room fire that leads to having to abandon the control room. In such a case, an important consideration is the ability to identify a failed open PORV before the control room is abandoned.

b. Status of Cable Spreading and Control Rooms

These rooms are not screened out.

c. Improperly Screened Out Zones/Areas

Because of the concerns expressed in this review document, all areas and zones should be reevaluated using screening criteria and methods such as in the FIVE methodology.

An example of an improper use of a fire event tree to screen out an area has to do with the scenario/area loss of auxiliary shutdown panel in the auxiliary feedwater area. The panel contains a one-inch thick partition between redundant trains. The study states that the frequency of loss of any two redundant components (through the partition) is a Stage 2 fire, at a frequency of 1.7×10^{-6}/yr. It then states that the frequency of loss of all components is a Stage 3 fire, at a frequency of 7.5×10^{-8}/yr. This is hard to understand. If a fire is severe enough to heat up the cabinet to cause failure of a single set of redundant components through a one-inch partition, then how can any other set of redundant components be shown to survive? This is a misapplication of the fire event tree approach.

2.2.6 Fire Hazard Analysis

a. Fire Initiating Event Database

The development of initiating event fire frequencies by analysis of industry-wide data is laudable for a site that had little or no operational experience in 1984. However, this database was not updated for the 1988 through 1991 study, and plant-specific data is not used. A comparison of the initiating events used in this study with the Reference [12] database shows that the cable area, control room, and switchgear room frequencies used in the McGuire study are a factor of 2 to 3 lower than those recommended in the FIVE document. The Reference [12] frequencies are based on about 5 times as many fires and more than double the number of reactor years than the data used for the McGuire study. It is not surprising, therefore, that the fire initiation frequencies differ.

Frequencies of fire initiation in pumps may be of the correct order of magnitude in the McGuire study, as compared to the FIVE document. However, the frequency of fires over the entire area, not just a selected component, should have been developed to allow the assessment of alternative fires in the area. This procedure may lead to a misperception of risk contributors, missed vulnerabilities, and an underestimate of CDF.

The equation used to estimate component fire frequencies not specifically included in the database multiplies a surrogate component frequency by the ratio of the operating times of the component to the surrogate component. This has the obvious potential to underestimate frequency because it ignores the potential for the development of latent leaks which reveal themselves upon component startup.

b. Plant-specific Database

Plant-specific data is not used.

2.2.7 Fire Growth and Propagation

a. Treatment of Cross-Zone Fire Spread and Assumptions

The study includes a barrier penetration probability of 0.01 for three hour barriers with doors, and a barrier penetration probability of 0.2 for 1.5 hour barriers. These are meant to account for doors left open, and appear to be reasonable as overall average values. However, barrier penetration is allowed in the analysis only if the fire is at Stage 3 (fully engulfing the area). The potential for a fire to partially engulf an area (say Stage 2), and spread through an open door (or breach a barrier), is not considered. This does not account for a fire that starts in a combustible near an open barrier.

d. Computer Codes Used

Computer codes, such as COMPBRN, are not used for fire propagation, detection, and suppression.

2.2.8 Evaluation of Component Fragilities and Failure Modes

a. Definition of Fire-Induced Failures

Although not explicitly stated, the definition of failure appears to be loss of equipment functionality or, in the case of hot shorts, spurious actuation to an undesired position.

b. Method Used to Determine Component Capacities

Analytical or tabular methods, such as COMPBRN and FIVE, are not used to determine fire propagation potential. Temperature criteria for cable damage or electrical/electronic equipment damage are not used. Fire detection, suppression and propagation probabilities are based solely on the generic information in NUREG/CR-0654, judgmentally adjusted to account for plant-specific features.

c. Treatment of Operator Recovery Actions

The control room, auxiliary shutdown panel, and cable room fires are modeled in the systems analysis as if they are loss of nuclear service water. The vital I&C area fire is also modeled as a loss of nuclear service water. The recovery actions included in the analysis are cross-connection with the other unit, use of the containment ventilation cooling water system, and standby shutdown system. These recovery actions are "ANDed" together to reduce the core damage frequency from 1.3×10^{-4}/yr to 1.3×10^{-7}/yr. Justification for a logical "and" with respect to recovery actions depends on sufficient time available before core damage, and adequate procedures. The study does not provide this justification.

The main feedwater pump fire is modeled as a loss of offsite power, with loss of both diesel generators and the turbine-driven auxiliary feedwater pump. Recovery actions are not used in the analysis of this sequence.

2.2.9 Fire Detection and Suppression

a. Detection and Suppression Assumptions

Detection and suppression are addressed within the framework of the fire event tree. The detection and suppression probabilities are based on NUREG/CR-0654.

The response time of a fire brigade is assumed to be 3 minutes for initial response to an incipient fire and 10 minutes for a response to a large, automatically detected fire. Ten minutes to fire brigade response is used for all scenarios/areas. The submittal states that ten minutes was verified during the fire walkdown. However, no fire brigade test data is offered to support these response times. The three minute response for an incipient fire is low. How can an incipient fire be detected more readily than a large fire? It would be quite a sprint to reach some areas of the plant in 3 minutes. The relevant time, however, is not brigade initial response time. It is time to suppression, which must be longer than these times. No basis is provided for the assumptions.

b. Treatment of Fire Detection and Suppression

The fire event tree includes three opportunities for suppression. In order for a fire to be considered a Stage 3 fire it must have failed suppression three times in series (if detected). This inherently makes

assumptions that may not be realistic. For example, it implicitly assumes that failure of automatic suppression will always be accompanied by a second and third attempt in time to prevent a Stage 3 fire (by either auto-systems or manual). The suppression failure probabilities provided in Table 3.5-5 of the submittal are typically 0.1, 0.8, and 0.1, for a product of 8×10^{-3}. For the control room, the product is 4×10^{-3}. For the auxiliary feedwater room the product is 2.4×10^{-4}, and for the service water and component cooling water rooms the product is 1.2×10^{-3}. These combined failure probabilities are significantly lower than is typical of automatic detection/suppression systems, which are above 10^{-2} per reactor-year. The possibility of misaligned heads or nonconforming locations is not considered.

In addition, detection failure probabilities are treated separately. There are two opportunities in series to detect the fire. These are typically 0.1 and 0.05 to 0.01 for a product of 5×10^{-3} to 10^{-3}. For automatic fire suppression systems, the industry accepted number of 10^{-2} includes detection. Thus, the study has estimated detection/suppression failure frequencies that are at least three orders of magnitude lower in the absence of manual suppression. In effect, the study takes credit for a manual suppression failure frequency of less than 10^{-3}. This method has the potential to prematurely screen out areas, miss vulnerabilities, and underestimate core damage frequency.

c. Treatment of Suppression-Induced Damage

No cost-effective modifications to fire suppression systems have been identified to mitigate the effect of fire suppression water discharge and migration. However, only water is looked at, not CO_2 suppression.

An example of the treatment of the issue of suppression-induced damage is presented in Appendix B, Page 3.5-7, Rev. 2 of the McGuire IPEEE submittal [1]. Water from suppressing a fire in ETA (upper switchgear area) could penetrate the ETB (lower switchgear area) on the level below, because water from the ETA switchgear room could drain into the ETB switchgear room. The estimated frequency of this scenario is above 10^{-6}/yr, which is far higher than the other fire related ETA/ETB scenarios. The study claims that the risk is really far lower because the estimate is bounding. However, the study does not include a better estimate within the set of cut sets, does not identify this as a potential vulnerability, and does not identify fixing the floor drainage problem as a plant improvement that arose from the study.

2.2.10 Analysis of Plant Systems and Sequences

a. Key Assumptions Including Success Criteria and Bases

The assumptions discussed in previous sections, particularly (1) the use of a single worst case scenario to represent an area, (2) the underestimation of fire initiation frequency, and (3) the screening out of areas based on comparison to IPE results, caused the study to underestimate the significance of fires. An example follows.

The analysis of cut sets involving the control room assumes a Stage 3 fire that fully involves the control room. While this may be the worst case with respect to the ability of the plant to deal with the situation, it may not capture the majority of the risk with respect to total core damage frequency. For example, typical fire scenarios in control rooms involve smoke that is sufficient to force operators to abandon the control room, either because of the adverse environment or because control is lost from smoke damage. This category of scenarios is not included in the McGuire study.

b. Event Trees (Functional or Systemic)

Functional event trees supported by fault trees are used.

c. Dependency Matrix

A dependency matrix is not provided.

d. Plant Unique System Dependencies

There are no plant unique system dependencies.

e. Shared Systems for Multi-Unit Plant

The McGuire units share the ability to cross-connect nuclear service water, with only one nuclear service water train required to supply the water needs of both units. Instrument air is also shared between units.

f. Most Significant Human Actions

The most significant human actions are (1) failure to cross-connect with the other unit or use the remote shutdown panel, and (2) failure to initiate the Standby Shutdown System.

2.2.11 Core Damage Frequency Evaluation

a. Overall Treatment and Scrutability

The five areas that survive the screening are: vital I&C area; control room; cable room; auxiliary shutdown panel; and main feed pump area. The selected scenario for the first four is loss of nuclear service water. The selected scenario for main feed pump fire is loss of offsite power. The control and cable rooms are evaluated as if they are one area. Using the IPE model transient functional event tree and fault trees in Section 2 of Reference [4], cut set frequencies summed to a total fire core damage frequency of 2.3×10^{-7}/yr, which is less than 1% of the total core damage frequency of 7×10^{-5}/yr. The fire sequence for main feed pump fire falls into the TBU functional sequence category. This type of sequence involves a transient with failure of secondary side heat removal (B) and failure of safety injection (U). Cable, control, and vital I&C area fires, which are assumed to be equivalent to loss of nuclear service water, are identified as TQsU sequences. These sequences involve a transient with reactor coolant pump seal LOCA, and failure of safety injection. CAFTA is used to solve the trees, and cut sets are presented.

An important assumption in the quantification is as follows: loss of nuclear service water can be prevented if the fire causes a hot short to ground, followed by control fuse actuation, before a hot short causes equipment trip. The study estimated that such an event would occur 80% of the time. Thus, the probability of losing nuclear service water owing to a fire in the cable or control rooms is reduced by a factor of 5 (previous frequency multiplied by 1/5). This approach is applied only to the cable and control rooms. The basic problem with this approach is that it assumes that hot shorts are the only way that a fire in the area can cause damage or cause equipment to change state. For example, fires in cabinets can adversely affect the operation of equipment without producing hot shorts in cables.

Unfortunately, another limitation of the study, as pointed out in Section 2.2.5 above, is that cabinet fires are not adequately considered in this study.

2.2.12 Analysis of Containment Performance

a. Significant Containment Performance Insights

Typical of other fire PRAs, containment performance is assumed to be the same as for the internal event study, because all fire scenarios are seen as alternative initiating events for the internal event trees. There is no discussion on additional fire unique initiating events or containment failure modes.

b. Plant Unique Phenomenology Considered

Plant unique accident phenomenology associated with fires is not considered.

2.2.13 Treatment of Fire Scoping Study Issues

a. Assumptions Used to Address Fire Scoping Study Issues

An implicit assumption of the walkdown used to address these issues is that all ventilation equipment would be fully operational.

b. Significant Findings

1. The licensee states that where smoke can be generated by fire, existing smoke control capability (i.e., ventilation, automatic suppression, fire brigade action, and large areas) is sufficient to prevent unacceptable damage. The above discussion regarding the lack of consideration of cabinet fires and the assumption of ventilation availability is also relevant here.

2. The licensee found that no cost-effective modifications to fire suppression systems are needed (i.e., are identified) to mitigate the effect of fire suppression water discharge and migration. However, only water has been looked at, not CO_2 suppression.

3. The licensee states that seismic-induced failure of fire protection control panels is not a problem. Automatic heat activated sprinkler heads may be actuated during an earthquake. The licensee found seismic-induced failure of RCP motors not to be a problem, because fires in the motors would not affect the ability to achieve safe shutdown. However, seismic-induce fire effects on other equipment is not discussed in the submittal.

4. The licensee found control system interactions not to be a problem because of the Standby Shutdown System.

5. Intercompartment fire barrier breaching is considered in the fire PRA by use of an average screening value. It is not clear from the study if maintenance records were reviewed to verify the state of repair of barriers, doors, and dampers. However, the Standby Shutdown System further mitigates the adverse affects of failure of redundant trains caused by breach of fire barriers.

6. Discussion of manual fire fighting effectiveness is not included in the reviewed documents.

7. Discussion of fire barrier qualification is not included in the reviewed documents.

2.2.14 USI A-45 Issue

a. Methods of Removing Decay Heat

The McGuire plants can remove decay heat using:

1. Main feedwater or auxiliary feedwater, through power-operated relief valves (PORVs) or condenser dump valves,

2. Charging or SI, and PORVs, for feed and bleed,

3. RHR and long term recirculation, or

4. Standby Shutdown System.

Credit is taken for bleed and feed and the Standby Shutdown System. Fire is not a significant contributor to the risk associated with shutdown decay heat removal sequences.

2.3 HFOs

The IPEEE finds no unduly significant sequences (vulnerabilities) with respect to HFOs. The most significant contributor to the CDF due to external events is, however, an HFO event (i.e., tornado). The report estimates that tornado events make up 63% of the CDF from external events. This is followed by seismic events that contribute about 36% of the external event CDF. Tornado-induced events are considered as non-recoverable losses of offsite power. A PRA of tornado events reveals that the dominant sequences are those involving failure of the diesel generators to operate (start, run, or maintenance outage).

The general methodology utilized in the McGuire IPEEE follows that presented in NUREG-1407 for the analysis of other external events. The general methodology includes the following steps:

1. All natural and man-made external events are identified according to other PRAs, NSAC/60 [11], ANSI/ANS-2.12 [12], and NUREG/CR-2300 [13].

2. The resulting events are screened so as to select significant events.

3. A scoping analysis is performed on significant events. Only external floods and tornadoes were selected for detailed analysis. Although floods and tornadoes were further analyzed, transportation and nearby facility accidents were also closely evaluated and reported in the submittal.

4. The analysis is documented.

In performing steps 2 and 3 above, the following efforts were performed:

Weaknesses:

1. The method used for including nonseismic failures leaves room to doubt the completeness of the resulting cut sets.

2. A non-site specific spectral shape (NUREG/CR-0098 median, 5% damped spectral shape) is used without an accompanying sensitivity study to understand the effect of not using the suggested NUREG/CR-5250 shape.

3. The hazard analysis is truncated at 1.02g without performing a sensitivity study to investigate the effect of a truncation of less than 1.5g.

4. A soil failure analysis, including liquefaction at the site and of dams/embankments impacting the site, is not documented, although it is stated that construction records are reviewed to make the determination that liquefaction is not a problem.

5. The impact of unit differences on seismic risk results is not explained, and seismic events that could affect similar equipment in both units are not considered.

6. Human failure rates used in the analysis do not account for the earthquake level. The model and results used for the IPE are used for the seismic assessment. The licensee judged that earthquake-induced equipment failures would not have an effect on the operators because the same operating procedures would apply.

3.2 Fire

The McGuire fire IPEEE is an update of the full scope, Level 3 PRA performed between 1984 and 1987. Consistent with the guidance of NUREG-1407, the analysis identified critical fire areas, identified possible initiating events, calculated the fire initiation frequency, analyzed for the impairment of critical safety functions, and developed core damage cut sets with frequencies using a functional transient event tree and associated fault trees. A special fire event tree is used to help screen out areas, and assess fire damage and the frequency of fire damage. Typical of other fire PRAs, containment performance is assumed to be the same as for the internal event study, because all fire scenarios are seen as alternative initiating events for the internal event trees. There is no discussion of additional fire unique initiating events or containment failure modes. The walkdown was performed to verify assumptions about plant configuration, locate cable runs, and address the Sandia Fire Scoping Study Issues.

While the licensee's procedure for performing its fire IPEEE appears reasonable on the surface, its application and assumptions tend to prematurely screen-out fire areas, obscure or potentially miss vulnerabilities, provide an erroneous perception of risk contributors, and underestimate core damage frequency. The fire methodology employed is outdated and leads to a general underestimation of the significance of fires in the plant. The calculated core damage frequency is significantly lower than is typical of other Westinghouse PWRs. Even considering the mitigating effects of the Standby Shutdown System, a much higher fire-induced core damage frequency would be expected. Because of the concerns expressed in this review document, all areas and zones should be reevaluated using screening criteria and methods such as in the FIVE methodology.

Although this review found many methodological aspects of the study below the state-of-art, five aspects are of particular concern.

The first is the method used for screening of fire areas. This is based on comparison with the IPE results of the same or similar equipment damage scenarios. If a fire-induced equipment failure scenario causes equipment damage at a frequency lower than the frequency of a similar IPE equipment failure scenario, then the entire area is screened out. The submittal, therefore, does not present a total fire CDF. It presents only the sum of the scenario CDFs that happen to be larger than the corresponding IPE scenarios. This is not consistent with the spirit of GL 88-20, Supplement 4, which is concerned with identification of vulnerabilities for each external event on its own, rather than in comparison to another event. If the licensee's approach is taken to its logical extreme, then each external event, in total, could be screened out if its total CDF is less than the IPE CDF.

The second is the outdated data base which has led to use of fire initiation frequencies for key areas (control room, cable room, and switchgear rooms) that are one-half to one-third of the Reference [22] database. The five rooms which survived screening, and upon which the total CDF estimate is based, are analyzed using these low fire initiation frequencies. The same fire initiation frequencies are used for both Catawba and McGuire.

The third is the use of a single component and a single initiating event as representative of the area. For example, nuclear service water pumps are used as a source, but cabinets in that area are not. Vulnerabilities associated with other sources of fire (e.g., cabinets) in an area can not be identified by this method. The licensee states that this approach is used because the component causing the selected initiating event has the greatest chance of causing the initiating event. This neglects the possibility of other initiating events in the area caused by other sources.

The fourth is that four of the unscreened rooms are analyzed with a loss of nuclear service water transient initiating event. The assumption that all control, cable, vital I&C, and auxiliary shutdown panel room fires are equivalent to nuclear service water fires, therefore, manifests itself in cut sets that are comprised solely of nuclear service water related events. The licensee claims that the analysis is conservative because loss of component cooling water is the most severe transient which gives the worst case result. However, because this assumption, in effect, screens out all non-nuclear service water related equipment, this clearly can lead to missed vulnerabilities.

The fifth is the use of a multiplicative factor on the control and cable room scenarios that reduces the calculated core damage frequency for these rooms by a factor of five because, as the submittal argues, only hot shorts can cause failures that jeopardize the ability to control the plant. This argument fails to acknowledge an entire class of scenarios that involves loss of the ability to control the plant simply because of accumulated fire damage that opens circuits. Fires in either the control or cable spreading rooms can damage control and instrumentation equipment, without hot shorts, to the point that the ability to control the plant from the control room is lost. Fires in the control room, furthermore, may force operators to abandon the control room because of smoke. Smoke induced abandonment may be the result of limited visibility as well as non-breathable environment. In either case, abandonment of the control room means that plant control depends on successful use of the auxiliary or remote shutdown panels (or perhaps the SSF). Typically, control room abandonment scenario of this class would have been the most important core damage scenarios. In this study, a scenario of this class would have been the most important contributor. This class of scenarios does not appear to have been included in the submittal.

Strengths:

1. Consistent with the guidance of NUREG-1407, the analysis identified critical fire areas, identified possible initiating events, calculated the fire initiation frequency, analyzed for the impairment of critical safety functions, and developed core damage cut sets with frequencies using a functional transient event tree and associated fault trees.

2. A fire walkdown was conducted.

3. The licensee had control over the study, and apparently performed the entire study.

4. Internal peer review was performed.

5. Relay chatter is probabilistically treated in the logic model.

Weaknesses

1. The fire methodology employed is outdated and leads to a general underestimation of the significance of fires in the plant. The use of NUREG/CR-0654 values in the fire event tree may not be valid.

2. The screening method, which is based on comparison of fire induced equipment damage frequency with internal event induced equipment damage frequency, may have prematurely screened out significant areas.

3. An outdated fire database leading to low estimates of fire initiation frequencies is used.

4. A single "worst case result" scenario is used in each fire area, instead of a more comprehensive approach of evaluating fires at each potential source location.

5. Fire-induced failure cut sets are limited, by assumption, to loss of nuclear service water related events, except for the main feedwater fire scenario.

6. The treatment of the conditional probability of hot shorts as a multiplier on core damage frequency for the control and cable rooms is not valid.

7. A dubious assessment of area-by-area initiating event selection is used to screen out fire areas.

8. Inadequate attention is given to cabinet fires.

9. The fire event tree method and assumptions, with respect to propagation and suppression, underestimate fire risk.

10. The Fire Risk Scoping Study issues are either inadequately documented or addressed. Specifically, there is inadequate documentation with respect to seismic fire interactions, fire brigade effectiveness, and barrier effectiveness.