14.4 APPROACH TO SAFETY ANALYSIS

14.4.1 General

The below probabilistic analysis discussion reflects capabilities at the time of the initial BFN design. The most informative approach to safety analysis is generally one based on probabilistic analysis. Such an approach allows precise statements of unacceptable safety results and permits categorization and evaluation of failures by relative probabilities. To satisfactorily effect such an approach, adequate data on component failure rates, failure modes, failure distributions, repair times, and repair time distributions are required. With the necessary data, models can be constructed and analyzed to reveal the realistic probabilities of events pertinent to nuclear safety. General Electric is currently compiling sources of data and developing the techniques of probabilistic analysis. Although probabilistic analysis currently provides much insight into the problems of safety, the technique has not matured sufficiently or gained the general acceptance necessary to permit it to be the major analysis tool.

Until the probability approach matures, two basic groups of events pertinent to safety (abnormal operational transients and accidents) will be investigated separately. The preclusion of unacceptable safety results requires that no damage to the fuel occurs and that no nuclear system process barrier damage results from any abnormal operational transient. Thus, analysis of this group of events evaluates the plant features that protect the first two radioactive material barriers. Analysis of the events in the second group (accidents) evaluates situations that require functioning of the engineered safeguards including containment. Tables 14.4-1 and 14.4-2 display the overall results of these analyses.

In considering the various abnormal operational transients and accidents, the full spectrum of conditions in which the core may exist is considered. This is accomplished by investigating the differing safety aspects of the six BWR operating states, as described in Appendix G. In general, only the most severe event of a given type is described in detail.

Since the preclusion of unacceptable safety results for abnormal operational transients requires that no fuel damage occur, the limiting abnormal operational transients are examined for each fuel cycle to ensure this requirement is met. Different transient methodologies have been employed for the Browns Ferry abnormal operational transient analyses. The analyses for the following events are not dependent on fuel type or reactor power level: Control Rod Removal Error during Refueling (Section 14.5.4.3), Fuel Assembly Insertion Error during Refueling (Section 14.5.4.4), and Loss of Habitability of the Control Room (Section 14.5.9). Therefore, the GE analysis methodology is valid for these events and provides conservatism by accounting for uncertainties in computed results and utilizing NRC-approved methods. All other accident analyses employ AREVA

NRC-approved codes and methodologies. The results and methodology for the currently applicable limiting transient and accident analyses are contained in UFSAR Appendix N.

14.4.2 Abnormal Operational Transients

Figure 14.4-1 shows (in block form) the general method of identifying and evaluating abnormal operational transients. Eight nuclear system parameter variations are listed as potential initiating causes of threats to the fuel and the nuclear system process barrier; the parameter variations are as follows:

a. Nuclear system pressure increase,

b. Reactor vessel water (moderator) temperature decrease,

c. Positive reactivity insertion,

d. Reactor vessel coolant inventory decrease,

e. Reactor core coolant flow decrease,

f. Reactor core coolant flow increase,

g. Core coolant temperature increase, and

h. Excess of coolant inventory.

These parameter variations, if uncontrolled, could result in excessive damage to the reactor fuel or damage to the nuclear system process barrier, or both. A nuclear system pressure increase threatens to rupture the nuclear system process barrier from internal pressure. A pressure increase also collapses the voids in the moderator, causing an insertion of positive reactivity that threatens fuel damage from overheating. A reactor vessel water (moderator) temperature decrease results in an insertion of positive reactivity as density increases. This could lead to fuel overheating. Positive reactivity insertions are possible from causes other than nuclear system pressure or moderator temperature changes; such reactivity insertions threaten fuel damage caused by overheating. Both a reactor vessel coolant inventory decrease and a reduction in the flow of coolant through the core threaten to overheat the fuel as the coolant becomes unable to adequately remove the heat generated in the core. An increase in coolant flow through the core reduces the void content of the moderator, resulting in an increased fission rate. If uncontrolled, excess of coolant inventory could result in excessive carryover.

These eight parameter variations include all of the effects within the nuclear system caused by abnormal operational transients that threaten the integrities of the reactor fuel or nuclear system process barrier. The variation of any one parameter may cause a change in another listed parameter; however, for analysis purposes, threats to barrier integrity are evaluated by groups according to the parameter variation originating the threat. For example, positive reactivity insertions resulting from sudden pressure increases are evaluated in the group of threats stemming from nuclear system pressure increases.

Abnormal operational transients are the results of single equipment failures or single operator errors that can be reasonably expected during any mode of plant operations. The following types of operational single failures and operator errors are identified:

a. The opening or closing of any single valve (a check valve is not assumed to close against normal flow),

b. The starting or stopping of any single component,

c. The malfunction or maloperation of any single control device,

d. Any single electrical failure, and

e. Any single operator error.

Operator error is defined as an active deviation from written operating procedures or nuclear plant standard operating practices. A single operator error is the set of actions which is a direct consequence of a single erroneous decision. The set of actions is limited as follows:

a. Those actions that could be performed by not more than one person,

b. Those actions that would have constituted a correct procedure had the initial decision been correct, and

c. Those actions that are subsequent to the initial operator error and have an effect on the designed operation of the plant, but are not necessarily directly related to the operator error.

Examples of single operator errors are as follows:

a. An increase in power above the established flow control power limits by control rod withdrawal in the specified sequences,

b. The selection and complete withdrawal of a single control rod out of sequence,

c. An incorrect calibration of an average power range monitor, and

d. Manual isolation of the main steam lines due to operator misinterpretation of an alarm or indication.

The five types of single errors or single malfunctions are applied to the various plant systems with a consideration for a variety of plant conditions to discover events that directly result in any of the listed undesired parameter variations. Once discovered, each event is evaluated for the threat it poses to the integrities of the radioactive material barriers. Generally, the most severe event of a group of similar events is described.

Two additional events are analyzed as special cases: (1) loss of habitability of the control room. This abnormal condition is postulated to demonstrate the capability to perform the operations required to maintain the plant in a safe condition from outside the control room, and (2) Inability to shut down the reactor with the control rods. This event is presented to justify the requirement for the Standby Liquid Control System and results in a normal shutdown using this system. Therefore, no further analysis or evaluation is required other than that presented in Subsection 3.8 ("Standby Liquid Control System").

14.4.3 Accidents

Figure 14.4-2 shows (in block form) the method of identifying and evaluating accidents. For analysis purposes, accidents are categorized as follows:

a. Accidents that result in radioactive material release from the fuel with the nuclear system process barrier, primary containment, and secondary containment initially intact,

b. Accidents that result in radioactive material release directly to the primary containment,

c. Accidents that result in radioactive material release directly to the secondary containment with the primary containment initially intact,

d. Accidents that result in radioactive material release directly to the secondary containment with the primary containment not intact, and

e. Accidents that result in radioactive material release outside the secondary containment.

Accidents are defined as hypothesized events that affect one or more of the radioactive material barriers and which are not expected during the course of plant operations. The accident types considered are as follows:

a. Mechanical failure of various components leading to the release of radioactive material from one or more barriers. The components referred to here are not components that act as radioactive material barriers. Examples of mechanical failures are breakage of the coupling between a control rod drive and the control rod, failure of a crane cable, and failure of a spring used to close an isolation valve.

b. Overheating of the fuel barrier. This includes overheating as a result of reactivity insertion or loss of cooling. Other radioactive material barriers are not considered susceptible to failure due to any potential overheating situation.

c. Arbitrary rupture of any single pipe up to and including complete severance of the largest pipe in the nuclear system process barrier. Such rupture is assumed only if the component to rupture is subjected to significant pressure.

The effects of the various accident types are investigated, with a consideration for a variety of plant conditions, to examine events that result in the release of radioactive material. The accidents resulting in potential radiation exposures greater than any other accident considered under the same general accident assumptions are designated design basis accidents and are described in detail.

To incorporate additional conservatism into the accident analyses, consideration is given to the effects of an additional, unrelated, unspecified fault. The fault is assumed to occur in a safety-related component or piece of equipment that is needed to respond to the initiating event in order to achieve the intended safety-related function. Such a fault is assumed to result in the maloperation of a device which is intended to mitigate the consequences of the accident. The assumed result of such an unspecified fault is restricted to such relatively common events as an electrical failure, instrument error, motor stall, breaker freeze-in, or valve maloperation. Highly improbable failures, such as pipe breaks, are not assumed to occur coincident with the assumed accident in the short term. The additional failures to be considered are in addition to failures caused by the accident itself.

In the analyses of the design basis accidents consideration for a variety of single additional failures is made by making analysis assumptions that are sufficiently conservative to include the range of effects from any single additional failure. Thus, there exists no single additional failure of the type to be considered that could worsen the computed radiological effects of the design basis accidents.

14.4.4 Barrier Damage Evaluations

14.4.4.1 Fuel Damage

Subsection 3.7 ("Thermal and Hydraulic Design") describes the various fuel failure mechanisms and establishes fuel damage limits for various plant conditions. Preclusion of unacceptable safety result 1 and 2, for Abnormal Operational Transients is determined by demonstrating that abnormal operational transients do not result in a minimum critical power ratio (MCPR) of less than 1.0. If MCPR does remain above 1.0, no fuel failures result from the transients, and thus the radioactivity released from the plant cannot be increased over the operating conditions existing prior to the transient. It should be noted that maintaining MCPR greater than 1.0 is a sufficient but not necessary condition to assure that no fuel damage occurs. (This is discussed in Subsection 3.7.)

For situations in which fuel damage is sustained, the extent of damage is determined by correlating fuel energy content, cladding temperature, fuel rod internal pressure, and cladding mechanical characteristics. These correlations are substantiated by fuel rod failure tests and are discussed in Subsection 3.7 and Section 6.

Preclusion of unacceptable safety result 2 for accidents is shown by demonstrating that fuel clad temperature remains below 2200°F. The selection of this temperature limitation is discussed in Section 6.

14.4.4.2 Nuclear System Process Barrier Damage

Preclusion of unacceptable safety result 3 for abnormal operational transients and unacceptable safety result 3 for accidents is assessed by comparing peak internal pressure with the overpressure transient allowed by the applicable industry code. The only significant areas of interest for internal pressure damage are the high-pressure portions of the nuclear system primary barrier: the reactor vessel and the high-pressure pipelines attached to the reactor vessel. The overpressure below which no damage can occur is taken as the lowest of pressure increases over design pressure allowed by either the ASME Code Section III for the reactor vessel or USAS B 31.1 Code for the high pressure nuclear system piping. The ASME Code Section III permits pressure transients up to 10 percent over design pressure (110 percent x 1250 psig = 1375 psig); USAS B 31.1 permits pressure transients up to 20 percent over the design pressure.

Thus, it can be concluded that the high-pressure portion of the nuclear system process barrier meets the design requirement if peak nuclear system pressure remains below 1375 psig.

An analysis performance measurement, which is discussed in Subsection 3.6 ("Nuclear Design"), is used to evaluate whether nuclear system process barrier damage occurs as a result of reactivity accidents. If peak fuel enthalpy remains below 280 calories per gram no nuclear system process barrier damage results from nuclear excursion accidents.

14.4.4.3 Containment Damage

Preclusion of unacceptable safety result 1 (for abnormal transients) and 4 (for accidents) requires that the primary and secondary containment retain their integrities for certain accident situations. Containment integrity is maintained as long as internal pressures remain below the maximum allowable values. The maximum allowable internal pressures are as follows:

Drywell (primary containment)	62 psig
Pressure Suppression Chamber (primary containment)	62 psig
Secondary Containment	2 inches H_2O

Damage to any of the radioactive material barriers as a result of accident-initiated fluid impingement and jet forces is considered in the other portions of the Safety Analysis Report where the mechanical design features of systems and components are described. Design basis accidents are used in determining the sizing and strength requirements of much of the essential nuclear system components. A comparison of the accidents considered in this section with those used in the mechanical design of equipment reveals that either the applicable accidents are the same or that the accident in this section results in less severe stresses than those assumed for mechanical design.