SAFETY EVALUATION
WNP-2; LICENSE CONDITION 22
CONTROL SYSTEMS FAILURES

INTRODUCTION AND SUMMARY

The licensee was requested to review the adequacy of emergency operating procedures to be used to obtain safe shutdown of the reactor upon the loss of any Class 1E or non-Class 1E bus supplying power to safety related or non-safety related instrumentation and controls. This issue was addressed for operating reactors through IE Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power System Bus During Operation." The purpose of this review is to verify that the loss of power to any Class 1E or non-Class 1E ac or dc bus supplying power to plant instrumentation and controls will not result in an event requiring reactor shutdown, concurrent with the failure of instrumentation upon which operator actions to achieve reactor shutdown are based.

The licensee was also requested to determine whether multiple non-safety related (control) systems failures, resulting from the adverse environment created by a high energy line break (HELB), could result in consequences more severe than previously considered in the FSAR Chapter 15 accident analyses. This concern is addressed in IE Information Notice 79-22. Additionally, the licensee was requested to perform a review of all power sources, sensors, and sensor impulse lines that provide power or process information to two or more non-safety related (control) systems. The purpose of this review was to verify that the failure of a power source or sensor, or the rupture/plugging of an instrument header or impulse line will not cause multiple control systems failures resulting in consequences more severe than previously analyzed in the FSAR Chapter 15 analyses.

The WNP-2 operating license was conditioned to require that the above reviews be completed prior to startup following the first refueling outage. The specific license condition is listed below:

22. Control Systems Failures (Sections 7.7.2.1, 7.7.2.2, 7.5.2.3, SER, SSER #4)

Prior to startup following the first refueling outage, the licensee shall provide to NRC staff for review and approval any analysis or modifications needed to resolve the following items.

(a) capability to attain a safe shutdown condition following the loss of any Class 1E instrument bus

(b) the impact of control systems failures resulting from high energy line breaks on the transient and accident analyses

(c) the impact of control systems failures due to the failure of common power sources, sensors, or instrument sensing lines on the transient analyses.

The licensee provided the results of their reviews by letter G02-83-574 dated June 24, 1983. Additional information was provided in response to a staff request for additional information by letter G02-83-1040 dated November 10, 1983. Based on the review of the information provided by the licensee, the staff concludes that the issues identified in License Condition 22 have been resolved by the licensee as discussed in the following evaluation.

EVALUATION

Capability for Safe Shutdown Following Loss of a Bus Supplying Power to Instruments and Controls

The licensee was requested to:

1. Review the class 1E and non-class 1E buses supplying power to safety and non-safety related instrumentation and control systems which could affect the ability to achieve a cold shutdown condition using existing procedures or procedures developed under item 2 below.

2. Prepare emergency procedures or review existing ones that will be used by control room operators, including procedures required to achieve a cold shutdown condition, upon loss of power to each class 1E and non-class 1E bus supplying power to safety and non-safety related instrument and control systems, and

3. Rereview IE Circular No. 79-02, Failure of 120 Volt Vital AC Power Supplies, dated January 11, 1979, to include both class 1E and non-class 1E safety related power supply inverters. Based on a review of operating experience and the rereview of IE Circular No. 79-02, describe any proposed design modifications or administrative controls to be implemented as a result of the rereview.

The licensee submitted a report "Cold Shutdown Power Bus Failure Analysis Report," prepared by the General Electric Company, documenting the results of the above reviews. An electrical bus tree was constructed that showed the various ac and dc buses that could be used to achieve cold shutdown by normal and emergency means. The applicant then identified the various paths available to the operator to achieve cold shutdown, the instrumentation and control systems (including indications) in each path, and the respective loads in each of these systems. The report describes three shutdown paths and their relationship to one another. Either one of the three paths may be used to initiate cold shutdown and, depending upon availability, the paths may be mixed, i.e., start cold shutdown using the normal shutdown path, go into high pressure cooldown using the first alternate shutdown path and finish the cooldown using the normal shutdown path, staying with the first alternate shutdown path, or transferring to the second alternate shutdown path.

An evaluation was performed to determine the effects of the loss of power to each bus and its associated loads, including the cumulative effect of the loss of power condition on the ability to achieve a cold shutdown through each of the available paths. The applicant's evaluation concluded that cold shutdown can be achieved following any single bus failure, and that clear and unambiguous indication of an undervoltage condition (alarms and/or annunciations) is provided in the main control room to alert the operator to the loss of power. These bus failure indications will allow the operator to switch to an alternate shutdown path if necessary as governed by the procedures.

The applicant also stated that IE Bulletin 79-27 was re-reviewed concurrent with a review of the plant design, to determine if possible Class 1E and non-Class 1E power supply inverter failure modes exist as discussed in IE Circular 79-02. The applicant's review concluded that the design of the inverters is acceptable.

High Energy Line Breaks and Consequential Control Systems Failures

The licensee identified all non-safety grade control systems which may impact reactor critical parameters, (e.g., reactor vessel pressure, reactor vessel water level, critical power ratio, feedwater temperature, etc.) or the performance of safety-related equipment. Next, the licensee identified and located all high energy lines. For the reactor building, pipe break studies previously completed were referenced for line and break locations as well as targets.

In the identification of high energy lines, the licensee used the criteria for high energy lines established in Section 3.6.1 of the Standard Review Plan and Section 3.6.2 of the WNP-2 FSAR. High energy lines are defined as those which are in operation or maintained pressurized during normal plant conditions where the maximum temperature of the fluid in the line exceeds 200 F or the maximum pressure of the line exceeds 275 psig. High energy lines that operate above these limits for less than 2% of the time are classified as moderate energy lines and were excluded from the analysis. High energy lines which are less

than 1-inch in diameter were also excluded. The exclusion of these lines is acceptable because: 1) breaks of moderate energy fluid system piping are not postulated to occur in accordance with Branch Technical Position MEB 3-1 (see Section 3.6.1 of the Standard Review Plan), and 2) the environmental effects of breaks of lines 1-inch in diameter or smaller are less severe than for larger lines considered in the analysis (typically, these are instrument sensing lines whose failure can be detected from the abnormal behavior of instruments associated with the broken line).

The plant was then subdivided into HELB zones. Each zone is a separate area of the plant which is bounded by walls, ceiling, floors, etc. such that the environmental effects of a HELB in a given zone are confined to that zone and in some cases also to adjacent zones.

Next, the licensee determined those zones where components that can affect reactor critical parameters were located. The high energy lines identified were then assumed to break at all locations (zones) where the non-safety related/control components are located. The applicant used a "sacrificial approach" when analyzing the effects of a pipe break in a given zone (i.e., all non-safety related/control components in that zone were assumed to fail). All possible component failure modes were considered in an effort to determine the worst case failure mode for the components. Where a HELB could affect non-safety related/control components in more than one zone (e.g., a break within a small cubicle can conceivably blow out the door and the environmental effects of the break could affect components in the adjoining larger volume

zone), all components in the affected zones are considered to fail in their worst states. The sacrificial approach covers all potential component failure mechanisms (i.e., pipe whip, jet impingement, humidity, temperature, pressure, and radiation) since this approach assumes that the break will adversely impact all components in the respective zone(s).

The licensee analyzed the consequences resulting from each postulated break. Single control systems that were affected were reviewed to verify that the event incurred was bounded by the WNP-2 FSAR Chapter 15 analyses. If more than one control system was affected it was also reviewed to verify that the combined event incurred was bounded by Chapter 15 analyses. Those events that were not bounded were analyzed and the consequences of the event determined.

The licensee next analyzed multiple events. Multiple events were considered to be the result of pipe whip and jet impingement from a high energy line break with reactor scram culminating the events. Multiple events were not necessarily considered to occur simultaneously but were instead considered to occur at worst case timing until reactor scram.

Finally, worst case event combinations were looked at. The WNP-2 worst case event is a HELB on the 471' level of the turbine building. One set of Division A cable trays (power, control, and signal) and one set of Division B cable trays (power, control, and signal) run the length of the floor at this elevation gathering cables in route to the control room. A strategically located HELB could hit both sets of trays. Assuming worst case cable failures in all

trays, either open circuit or short, the following events, or any combination thereof, are possible:

1) Loss of Feedwater Heating
2) Feedwater Controller Failure-Maximum Demand
3) Pressure Regulator Fail-Closed
4) Loss of Feedwater Flow
5) MSIV Closure
6) Turbine Trip, Bypass On

Using the above events, the licensee performed an analysis which established a bounding event combination which resulted in the worst impact on critical reactor parameters. The initial conditions and input parameters used in the analysis are consistent with those used in Chapter 15. In establishing the bounding combination, events 1 through 4 were taken in a worst combination to bring the reactor to a power level just beneath thermal power monitor analytical scram limit (122% NBR). At this power level, events 5 and 6 above were assumed to occur.

The worst case sequence of the above potential combined events would be a loss of feedwater heating, then a pressure regulator failure culminated by an inadvertent MSIV closure. Loss of feedwater flow could only reduce the severity of the transient. The worst case combination would require the loss of feedwater heating and pressure regulator failure events to raise reactor power

and pressure levels just beneath RPS scram followed by MSIV closure. Occurrence of this event requires cable shorts and open circuits on the 471' elevation. The analysis showed that the reactor could be brought to cold shutdown with no increase in the risk to the health and safety of the public.

Based on the detailed review of the licensee's submittals, the staff has concluded that the methodology used and the results of the analysis performed by the licensee are acceptable.

Multiple Control Systems Failures

The licensee was requested to determine whether multiple control systems could fail simultaneously as a result of a common power source failing, a sensor that is supplying signals to several control circuits failing, or a failure of an impulse line that is supplying the physical data to several sensors. The licensee was then requested to verify that the consequences of the multiple control systems failures were bounded by the FSAR Chapter 15 analyses.

The licensee submitted a report "Common Sensor Failures Evaluation Report for Washington Public Power Supply System Nuclear Project No. 2," which discusses control systems, sensors and their impulse lines, and a report "Control System Failures Evaluation Report for WNP-2 Nuclear Power Station," which discusses control systems and their power sources. These reports identified those non-safety related/control systems that can effect reactor critical parameters

(e.g., reactor vessel water level, reactor vessel pressure, or reactor power level). The common sensors and power supplies were then identified, followed by sensor/impulse line failure mode analysis and an analysis of the loss of the critical loads. The results of these analyses were compared to Chapter 15 of the WNP-2 FSAR.

In the case of the common sensors, the comparison to Chapter 15 revealed that no new transient category events have been postulated as a result of the analysis. The licensee stated that there were no sensors that interfaced with multiple control systems. All sensor failure consequences which could effect or cause a reactor scram, a turbine trip, or a change in feedwater flow are bounded by FSAR Chapter 15 analysis.

In all cases, a plugged impulse line had no effect on the failure consequences. The licensee stated that although a plugged impulse line is usually not immediately detected, that the control/instrumentation channel performance can be verified by cross-checking the readouts of redundant channels. This process of comparison is performed on a shift basis which implies that a plugged impulse line would go undetected for not longer than one shift.

With respect to the loss-of-power sources and critical loads, the comparison to Chapter 15 revealed that the loss of power bus PP-3A-A was an event not previously analyzed in Chapter 15. The loss of this bus causes a partial loss of feedwater heating, a loss of the main turbine oil temperature control valve, and a potential main turbine trip due to vibration. The event, however, is

still bounded by existing analyses and it was not necessary to modify or augment the Chapter 15 analyses.

CONCLUSION

Based on its review of the licensee's responses to IE Bulletin 79-27, the staff concludes that there is reasonable assurance that any single instrumentation and control power bus failure will not result in a plant condition requiring reactor shutdown, and simultaneously cause the failure of instrumentation relied upon to achieve reactor shutdown.

Based on a detailed review of the licensee's analysis of HELBs and consequential non-safety related/control system component failures for several different zones (including the worst case event zone), the staff has concluded that the methodology used and the results of the analysis performed by the applicant are acceptable.

Based on the review of the licensee's analysis, the staff concludes that the effects of control systems failures resulting from power source, sensor, or instrument sensing lines are bounded by the WNP-2 FSAR Chapter 15 analyses (i.e., the previously reported limits of minimum critical power ratio, peak reactor vessel and main steam line pressures, and peak fuel cladding temperature for expected operational occurrence events would not be exceeded).

Based on the above, the staff concludes that the licensee has satisfied the requirements of License Condition 22, and therefore, that these issues are resolved.

It should be noted that the staff is currently reviewing the effects of control systems failures at nuclear power plants under Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems." The staff's preliminary conclusions regarding resolution of USI A-47 have not identified any significant concerns for BWRs resulting from power source, sensor, or instrument sensing line failures.