PDR

NOV 14 1969

Roger S. Boyd, Assistant Director for Reactor Projects, DRL
THRU: Saul Levine, Assistant Director for Reactor Technology, DRL

NORTHERN STATES POWER COMPANY, MONTICELLO NUCLEAR GENERATING PLANT, UNIT 1, DOCKET NO. 50-263; SAFETY ANALYSIS

The safety analysis relating to the Protection System and Emergency Power System is transmitted for inclusion in the report being prepared for consideration by the ACRS at the December meeting. The paragraphs of the report listed below identify unresolved problem areas or areas which require confirmatory information:

Paragraph	Subject
1.1.1	Flow-Biased Flux Reactor Trip
1.1.5.1	ARS - Pressure Interlock
1.1.8	Standby Gas Treatment System
1.1.10	Single Failure Criterion
1.4	Environmental Testing

Original signed by
Voss A. Moore

V. A. Moore, Chief
Instrumentation and Power
Technology Branch
Division of Reactor Licensing

RT-852A
DRL:I&PTB:TAI

Enclosure:
Safety Analysis

cc w/encl:
F. Schroeder
D. Muller
D. Vassallo

Distribution:
Suppl.
DRL Reading
AD/RT Reading
I&PTB Reading

bcc: S. Levine
R. DeYoung
V. Moore
T. Ippolito

OFFICE ▶	DRL:I&PTB	DRL:I&PTB	DAD/RT	AD/RT		
SURNAME ▶	TIppolito:ese	VMoore	RDeYoung	SLevine		
DATE ▶	11/14/69	11/14/69	11/14/69	11/14/69		

Form AEC-318 (Rev. 9-53) U.S. GOVERNMENT PRINTING OFFICE : 1966—O-214-629

NOV 14 1969

MONTICELLO NUCLEAR GENERATING STATION

UNIT 1, DOCKET NO. 50-263

EVALUATION OF THE INSTRUMENTATION, CONTROL AND AUXILIARY ELECTRIC POWER SYSTEMS

1. Introduction

The instrumentation, control and auxiliary electric power systems have been evaluated against the Commission's General Design Criteria (GDC) and /or the Proposed IEEE Criteria for Nuclear Power Plant Protection Systems (IEEE 279) dated August 28, 1968. A comparative review was made with the Dresden Nuclear Power Station, Units 2 & 3, the design of which was evaluated in our Report Number 2 to the ACRS, dated August 8, 1969. The reactor protection instrumentation and control systems as well as the instrumentation which initiates and controls the engineered safety features were found to be functionally the same. However, the auxiliary electric powersystems were found to be unique to each application.

During the course of our evaluation, we had several meetings with the applicant and his representatives. Two of these meetings were devoted to the review of elementary diagrams. In addition, a visit was made to the site on September 17 and 18, 1969, for the purpose of observing the physical arrangement and installation of the instrumentation, control, and auxiliary electric power systems.

Our report is limited to the BWR generic problem areas first identified in the Dresden, Units 2 & 3, evaluation, areas of design for which new information is available, and design features unique to Monticello. Specifically these areas are:

a. BWR Instrumentation Generic Problem Areas
b. Reactor Protection System and Engineered Safety Feature (ESF) Installation Criteria
c. Auxiliary Electric Power Systems
d. Environmental Testing of Electrical Components and Instruments

1.1 BWR Instrumentation Problem Areas

1.1.1 Flow-Biased Flux Reactor Trip

Six Average Power Range Monitor (APRM) instrument channels are provided for continuous monitoring and indication of reactor power and to supply trip signals to the reactor protection system. As a result of our expressed concern, the applicant has modified his design to provide reactor trip signals which are automatically biased by reactor coolant recirculation flow. The design modifications differ from our understanding of those proposed in Dresden, Units 2 & 3 and those shown in elementary diagrams for Oyster Creek, Unit 1, and Nine Mile Point. The difference is that in the Monticello design the fixed high flux reactor trip is being removed whereas in the other designs this trip remained in effect. Our concern with the Monticello design

is that the instrumentation which monitors recirculation flow and provides the flow bias input to the APRM channels is not immune to single failures.

The applicant has stated that his design is such that these failures will not negate the ability to trip the reactor at the fixed 120% high flux level. Further, he stated that except for the flow bias instrumentation, the design meets the requirements of IEEE 279. This exception is the same as that identified and accepted in Dresden, Nine Mile Point and Oyster Creek. The applicant will submit elementary diagrams of his design to assist us in confirming the suitability of these modifications. We anticipate no problems in this regard.

1.1.2 Rod Block Monitor (RBM)

The RBM is designed to initiate a rod block under the worst permitted bypass and detector failures to prevent local fuel damage during single rod withdrawal errors starting with any permitted power and flow condition. The RBM consists of two channels of instrumentation which are effective only during rod selection and movement above 30% power. The Dresden, Units 2 & 3, review identified single failures which would preclude rod block action when required. The consequence of failure of the RBM is evaluated and documented in the Dresden, Units 2 & 3, application and is applicable to Monticello. This evaluation shows that during reactor operation with certain limiting control rod patterns, the withdrawal of a designated single rod

could result in one or more fuel rods with MCHFR's less than 1.0. As in the case of Dresden, the judgment was made (1) that the limiting rod patterns are unique, (2) that during operation with such patterns, testing of the RBM system prior to withdrawal of such rods and on a daily basis thereafter will provide adequate assurance against improper rod withdrawals. The applicant has agreed to the same conditions and has included the requirement in the Technical Specifications.

1.1.3 Containment Spray Actuation

The containment spray system consists of the same components as the LPCI plus the additional valves and piping required to direct cooling water into the containment spray headers. These components are arranged in two loops and the controls for each loop are located in the same logic matrix associated with its corresponding LPCI loop. The admission valves for each loop are manually initiated by a switch in the control room. The remote manual controls for these valves are interlocked so that opening is not possible unless primary containment pressure is above 1 psig and reactor water level inside the core shroud is above 2/3 core height. Our review of these interlocks revealed that single failures could result in the loss of both containment spray loops as well as prevent termination of the flow in one loop when high containment pressure is reduced. Additionally, a single failure could result in the initiation of a single loop prior to the core being adequately covered (Failure of the 2/3 core shroud level interlock).

The applicant has revised the design of this instrumentation. Our review of the elementary diagrams of this revised design revealed that:

1. Initiation logic has changed from two-out-of-two per loop to a one-out-of-two taken twice logic per loop. This corrects the problem concerning initiation of the containment spray system.

2. Single failures remain which would prevent a single loop from being shut down either manually or automatically.

3. Single failures remain which would permit the initiation of a loop with the water level in the core below the 2/3 core shroud level.

4. This revised circuitry did not include the provision for testing the sensors.

Items 2 and 3 above are not required to be corrected since these failures do not constitute any danger to the public health and safety. The applicant has agreed to incorporate test jacks, test lights, and alarms in his design of containment spray initiation sensor circuitry. We conclude that the design is satisfactory for this application.

1.1.4 Diversity in Initiation of Core Spray and LPCI

The inputs for initiating the core spray system and its functionally

redundant and diverse counterpart, the LPCI system, are derived from signals which are a direct measure of the desired variables. The pumps for these systems are started by diverse (high containment pressure or low water level) signals. The admission valves of both systems, however, are operated by the same non-diverse but redundant reactor low pressure signals. These low pressure signals also compromise the independence of the core spray and LPCI systems. The applicant has agreed to provide equipment diversity in the form of two different types of pressure sensing devices. This design change is the same as that proposed and accepted during the review of Dresden, Units 2 & 3.

1.1.5 Auto-Relief System (ARS)

1.1.5.1 Pressure Interlock

The applicant has revised the design of the ARS to provide an interlock which will prevent automatic initiation unless the low pressure core cooling systems are available. This interlock function receives input signals from six pressure switches monitoring the discharge pressure of the six pumps (two core spray pumps and each of the four LPCI pumps) such that one switch monitors one pump. The circuitry is arranged such that the operation of any one switch (one pump operating) will permit the automatic initiation of the ARS. A review of the elementary diagrams revealed that single failures in

this interlock function will not prevent automatic initiation. However, single failures will result in automatic initiation with none of the low pressure core cooling systems available. Additionally, the design does not incorporate provisions for the testing of these added sensors.

The applicant states that the design of this pressure interlock satisfies his design criteria in that single active component failures will not negate the purpose of this function. He has been advised that we require that this pressure interlock be capable of performing its intended function in the presence of any single failure (single failure as defined in IEEE 279), and that the design incorporate provisions for sensor testing. This problem remains unresolved.

1.1.5.2 ARS Manual Initiation

The applicant has modified the design of the ARS to make manual initiation immune to single component failures. To provide this capability, provisions were made to automatically and independently provide each relief valve with an alternate soure of 125 vdc control power upon loss of the preferred source. This is accomplished by the provision of a preferred 125 vdc source monitor relay for each valve. Loss of the preferred power source will de-energize the relay, open the circuit from the preferred source and then complete the circuit to the alternate source. This same modification has been incorporated in each of the two automatic initiation logic matrices.

Our review of the elementary diagrams did not reveal any area which causes us concern except to ensure that the relay monitors are in fact the type which function to "break before make." The applicant has subsequently confirmed that the proper relay is being used in this design.

The justification and/or reasons for using single component failure criterion as a basis for this design is addressed in section 1.1.11 of this report.

1.1.6 Testability of Engineered Safety Feature Instrumentation

The design of the engineered safety feature circuitry did not include provisions for non-ambiguous periodic testing. The applicant has provided in the design of the emergency core cooling system (RHR, Core Spray, HPCI and ARS) instrumentation, permanently installed test jacks, test lights, and alarms. These added features will facilitate periodic testing, and reduce the need for using clip leads or to disconnect wiring. Even with these features, non-ambiguous periodic testing remains heavily dependent on written procedures. These procedures are scheduled to be completed just prior to core loading. However, preliminary procedures will be available in time for preoperational testing. We will request the Division of Compliance to review these procedures to assure that all credible random faults are detectable during periodic testing.

1.1.7 Reactor Building (RB) Ventilation Isolation

Isolation of the RB ventilation system and initiation of the Standby Gas Treatment System (SGTS) can be actuated by (1) the radiation monitors located in the ventilation exhaust plenum, or (2) the area monitors located above and to the side of the refueling pool. Two monitors are provided in each of these areas. Isolation of the RB ventilation system and initiation of the SGTS occurs on one of two upscale trips or two downscale trips from either set of monitors. Our review of the elementary diagrams revealed that the monitors located in the RB vent exhaust plenum as well as those located over the refueling pool are immune to single failures and are capable of being tested during operation. This design is similar to that proposed and accepted in our Dresden, Units 2 & 3, review.

1.1.8 Standby Gas Treatment System (SGTS)

The SGTS consists of two separate and redundant full capacity filter/absorber/fan units. The major components are shown in Figure 5.3.1 of the FSAR. This system is provided to maintain a small negative pressure (0.25 inches) in the reactor building under isolation conditions to minimize ground level release of airborne radioactivity. This system is initiated by either low water level, high containment pressure, or high radiation signals. The radiation monitors providing these signals are described in section 1.1.7 of this report.

Our review of elementary diagrams reveals that although each equipment train is physically and electrically separate from the other, the control instrumentation is not independent. In the proposed design, an equipment chain is dependent upon the failure of its redundant counterpart for initiation and operation. The applicant was advised that the lack of independence creates undue vulnerability to single failures. Further, he was advised that the design should be changed to satisfy the same basic principles of independence required in the reactor protection system.

The applicant stated that the design will be changed to assure that the control circuitry which detects the failure of the first equipment train and actuates its redundant counterpart will meet IEEE 279. We will advise the Committee orally of the schedule for submission of the design revisions for our evaluation.

1.1.9 Confirmation of HPCI Operation

The HPCI system is not individually designed to meet the single failure criterion. It is, however, functionally redundant to the Automatic Relief System (ARS) in conjunction with the core spray or LPCI systems. Although our review of the control and protection circuitry of the HPCI has indicated that the design is capable of meeting its functional requirements, we believe that a confirmatory field test of this system is necessary. The applicant has agreed to

perform preoperational tests with actual or simulated signals to verify its functional capability. We have concluded that this system is acceptable.

1.1.10 Single Failure Criterion

The applicant lists in the design basis for engineered safety feature initiation and control instrumentation the requirement that no single component failure shall prevent a protective action. The definition of single component failures, as we interpret it, does not agree with the single failure criterion defined in IEEE 279. The applicant has been requested to identify all reactor protection and engineered safety features instrument systems to which the single component failure applies and to provide justification for taking exception to IEEE 279. The applicant has agreed to submit this information in a forthcoming amendment. Further, we are led to believe that all protection systems, when one considers functional redundancy, meet the single failure criterion of IEEE 279. If this is confirmed in the forthcoming amendment, this matter will be resolved. Otherwise each system will have to be re-evaluated to determine its effect on public health and safety. We will report orally to the Committee in this regard.

1.2 Reactor Protection System (RPS) and Engineered Safety Features (ESF) Installation Criteria

The applicant has documented his criteria for the installation of the RPS and ESF. We conclude from our review of these criteria that if properly implemented, the probability of loss of redundant channels from a single cause such as fire will be acceptably low. These criteria include identification of safety related circuits and components from like items not related to safety.

Our site visit, however, revealed that the physical and electrical installation of the RPS instrument sensor located in the turbine building differed considerably from those sensors located in the reactor building. In some instances, the installation of these sensors does not satisfy our understanding of the applicant's design criteria. The RPS sensors located in the turbine building are those which monitor for condenser low vacuum, control valve fast closure, turbine first stage pressure, main steam line low pressure, and turbine stop valve closure.

Of the aforementioned sensors, only the installation of the control valve fast closure sensors is judged unacceptable since we cannot conclude that the installation is immune to a single common fault or event. Additionally, provisions are not included in the design to permit testing of these sensors during operation. The

sensors monitoring the action of the control valves are four pressure switches sensing the turbine acceleration relay oil pressure. Loss of oil pressure on this relay results in closure of the control valves. These sensors were observed to be mounted in an enclosure somewhat smaller than one cubic foot in size and located at the front end of the turbine. Within this enclosure, the four switches are mounted on a vertical steel plate of about 5/8 inches in thickness. Two switches are mounted on each side of the plate. The cables and sensing lines to these sensors were not installed; however, it is evident they would all have to be within inches of each other.

The applicant has agreed to modify the installation of these sensors to provide greater assurance against their failure from a single common event and to provide a means to permit testing of these sensors during power operation. We will request the Division of Compliance to assure that this installation as well as the installation of the other sensors located in the turbine building satisfy the stated criteria and are satisfactory.

1.3 Auxiliary Electric Power Systems

1.3.1 Offsite Power

Offsite power for the Monticello Unit will be supplied from the plant 345 kv and 115 kv switchyards. Power is supplied to the switchyards via multiple 115 kv and 345 kv lines over multiple rights-of-way.

Each of these lines independently has the capacity to supply sufficient power for safe shutdown or the engineered safety features loads. The incoming auxiliary power requirement is provided from the Northern States Power network and from the Upper Mississippi Valley Power Pool, the United Power Association and the Interconnected Systems Group.

Studies were conducted by NSP to determine the network characteristics and the system stability. From these studies the applicant concluded that loss of the Monticello Unit (460 MW) could be tolerated and that the spinning reserve ($\sim$ 618 MW in 1970) and the quantity of kinetic energy of the prime movers and generators would minimize the system disturbance. Thus, the loss of the Monticello Unit should not result in the inability of the grid to supply power to the station.

Initially the offsite transmission systems will be terminated at the substation switchyards in ring bus configurations; later, the switchyards will be converted into a breaker-and-one-half arrangement. We have concluded that either breaker arrangement is adequate in that a single failure cannot negate the ability of the grid to supply offsite power to the engineered safety feature loads.

The switchyard breaker controls are not specifically designed to meet the AEC General Design Criteria (GDC 39). A single battery system is used to supply the control and power requirements for the actuation of the switchyard circuit breakers. Our review of this

design reveals that loss of voltage in this battery system is alarmed in the control room and that operating personnel are trained to effect local (at the switchyard) circuit breaker operations in accordance with an approved procedure. We conclude from the aforementioned provisions and the applicant's stated maintenance procedures that there is adequate assurance against undetected failures and that repairs can be readily effected in this system. As a result, we judge that the addition (backfitting) of a redundant switchyard battery system would not add significantly to the public health and safety and is not required for this application.

From the substation switchyards, two overhead lines, one at 115 kv and one at 13.8 kv, are run to the station transformers at the reactor building approximately 1300 feet away. Two transformers connect the 115 kv and 13.8 kv lines into the station's two 4.16 kv essential buses.

Power is supplied by the reserve transformer during startup and shutdown and by the unit auxiliary transformer during normal operation. Upon unit trip, an automatic fast transfer to the reserve transformer will occur. Inability of this transformer to supply auxiliary power results in an automatic transfer to the second reserve transformer. This latter source is of smaller capacity but is capable of providing sufficient power to assure safe shutdown or supply all engineered safety feature loads.

We have concluded that, because of the capacity and redundancy provided and the relative independence of the redundant power sources, the offsite power system meets Criterion 39 and is acceptable.

1.3.2 Onsite Power

The design of the auxiliary power system utilizes the split bus concept. The 4160 auxiliary buses are in eight sections. Two of these buses, and their associated 480 volt load centers, supply power to the essential loads. The remaining buses supply power to all other plant services. No provisions are made to automatically connect redundant buses together upon a loss of power. This assures that a fault in one system will not be propagated to its redundant counterpart.

Two diesel generators provide power for the two essential buses, each bus having its own source of power. Each diesel generator is rated at 2500 kw (continuous), and 2750 kw (2000 hour). Both units start automatically, and are ready to accept load after ten seconds, upon initiation by either of the low reactor water level, high containment pressure, or loss or potential loss of offsite power signals. The diesel generators are independent with respect to physical location (separate Class I rooms), cooling water, air start systems, control and sequential loading circuits, and fuel supply. Makeup to each unit's day tank (8 hour supply) is from a single fuel oil storage tank which has sufficient fuel capacity for one week's operation of one unit at full

power. Redundant fuel pumps are provided to pump fuel from the storage tank to the day tanks of each diesel.

The required loads, after two hours in a DBA and loss of off-site power condition, total 2527 kw (design) and 2745 kw (maximum) for each diesel generator. The applicant has stated that, even though the continuous rating is exceeded, the 2000 hour and 30 minute ratings provide adequate margin for the intermittent and short time loads especially if load diversity factors are considered. While we do not agree that design loads should exceed the continuous rating, it is our judgment that, since the automatically energized loads are within the continuous rating and the other loads are under operator control, this is not sufficiently significant to require a backfit of larger capacity diesel generators. Additionally, it is our understanding that the applicant's operating procedure will require load sharing beyond the two hour accident period to further assure diesel loads remain within the continuous rating.

Three (250 v, 125 v, and 24 v) d-c power systems are provided. These systems are insulated from ground and each is provided with a ground detection system to annunciate the first ground. All batteries are mounted on racks designed to withstand the maximum earthquake. Each system, as well as the redundant components within each system, is physically and electrically separated from the others. We conclude that, since a loss of any d-c bus does not result in the loss of any protection function, the design of the d-c power system is adequate.

As originally designed, the redundant 125 v battery systems were interconnected by automatic transfer switches. This design compromised independence and was susceptible to failure from single common events. The applicant has agreed to provide manually controlled switches in lieu of the automatic switches. We conclude that this change provides further assurance that no single failure in the 125 v battery system will result in the complete loss of any protection function and is, therefore, considered adequate.

We conclude that, because of the capacity and redundancy provided and the relative independence of the redundant features, the onsite power system meets Criterion 39 and is acceptable.

1.4 Environmental Testing

A study was made by the applicant to determine whether the electrical equipment used in the reactor protection and engineered safety features could perform their design functions in an accident environment.

The electrical equipment located in containment that must function consists of a-c electric motor-operated valves with their associated operators and electrical cabling, and solenoid actuators for main steam isolation and ARS valves. The applicant has stated that qualification tests have been satisfactorily completed on prototype pieces of equipment and a summary report will be submitted. We conclude that

these equipment are satisfactory for use in this application provided the test report does not reveal areas of concern. We will report orally to the Committee in this regard.

The instruments inside containment that must function are limited to the sensors used for the reactor water level measurements. Test results included in the FSAR show that the sensors remain operable and maintain their required accuracy during and subsequent to rapid depressurization of the vessel. We conclude that this instrumentation is satisfactory for this application.

The applicant has proposed a program for assuring that Class I instrumentation meets seismic requirements. Our review of the original program plan submitted in the FSAR found it to be incomplete in scope since such vital Class I systems as Standby Gas Treatment, Containment Isolation, and Emergency Electric Power are not included. The applicant has re-examined the scope of the program to include all Class I systems.

The applicant has stated that this program will be completed for the General Electric supplied systems by December 31, 1969, and for the balance of plant systems by _____. The applicant will be required to correct any problem that is judged significant to the public health and safety prior to commencement of commercial operation.