NORTHEAST UTILITIES

THE CONNECTICUT LIGHT AND POWER COMPANY
WESTERN MASSACHUSETTS ELECTRIC COMPANY
HOLYOKE WATER POWER COMPANY
NORTHEAST UTILITIES SERVICE COMPANY
NORTHEAST NUCLEAR ENERGY COMPANY

General Offices • Selden Street, Berlin, Connecticut

P.O. BOX 270
HARTFORD, CONNECTICUT 06141-0270
(203) 666-6911

June 25, 1984

Docket No. 50-336
A02399

Director of Nuclear Reactor Regulation
Attn: Mr. James R. Miller
Operating Reactors Branch #3
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Gentlemen:

Millstone Nuclear Power Station, Unit No. 2
Reactor Protection and Engineered Safeguards System
Actuation Logic

The review of the Reactor Protection System (RPS) inoperable bypass channel condition at Millstone Unit No. 2 was first initiated by the Staff's letter dated August 3, 1977(1) in which Northeast Nuclear Energy Company (NNECO) was requested to either modify our technical specifications such that inoperable RPS channels be placed in the tripped condition within one hour after being declared inoperable or determine the suitability of operating the RPS in a two-out-of-three logic. In response to this request, NNECO reviewed the first proposal and determined that such specifications were unwarranted. As such, NNECO provided the Staff with information to support operation of the RPS in a two-out-of-three logic configuration, with an installed spare channel in our letter dated September 21, 1977(2). Several months after the docketing of this letter, we presumed that the matter was resolved. Some three and one-half years later, by letter dated April 16, 1981(3), the Staff reopened this issue expanding the review to include the Engineered Safety Features Actuation System (ESFAS). Reference (3) further requested NNECO to provide information regarding the adequacy of both physical and electrical separation as long-term operation of a four channel RPS and ESFAS in a two-out-of-three logic configuration would be acceptable provided all four channels are sufficiently independent.

As NNECO had previously addressed these concerns for the RPS in Reference (2), we supplemented this information by letter dated October 23, 1981(4) for

(1)G. Lear letter to D. C. Switzer, dated August 3, 1977.

(2)D. C. Switzer letter to G. Lear, dated September 21, 1977.

(3)R. A. Clark letter to W. G. Counsil, dated April 16, 1981.

(4)W. G. Counsil letter to R. A. Clark, dated October 23, 1981.

A001

both the RPS and ESFAS. The information provided in Reference (4) reaffirmed NNECO's position that the RPS as well as the ESFAS is designed for two-out-of-three logic configuration with an installed spare; thus concluding to the Staff that the Technical Specifications which permit extended bypass of one channel of either the RPS or ESFAS are appropriate.

On March 31, 1982[5], the NRC Staff presented, by letter, their modified position for operation of the RPS and ESFAS with one out of four channels in bypass. This letter provided two options for Licensees to follow. The first option allows bypass operation for a period not to exceed 48 hours at which time the inoperable channel must be placed in a tripped condition. The second option allows bypass of an inoperable channel for a lengthy period of time with no degradation to safety provided the criteria delineated in Reference (5) are satisfied. NNECO notes that the second option is in concert with the Technical Specifications as they currently exist at Millstone Unit No. 2.

NNECO has completed its review of the RPS and ESFAS in light of the Reference (5) criteria. Our position remains that operation of both the RPS and ESFAS in a two-out-of-three logic configuration with one channel in bypass is justified. This document verifies that plant design complies with the criteria delineated in Reference (5) as discussed below.

1. High Energy Line Break

   The protection system should be reviewed for the effects of high energy line breaks. Each licensee must analyze the protection system to verify that high energy line hazards in coincidence with the bypass of a channel will not negate the minimum acceptable redundancy required by IEEE Std. 279-1971. It should be noted that credit is not to be taken for the "fail-safe" mode of the channels affected by high energy line breaks.

   Response:

   In Reference (5), NNECO provided detailed information on the physical and electrical separation of the RPS and ESFAS channels. Regarding the design criteria, the RPS and ESFAS are designed and constructed to the general requirements of IEEE standard:

IEEE 279-1971	Criteria for Protection Systems for Nuclear Power Generating Stations

   In addition, the requirements of IEEE Standards 308-1971, 323-1971, 336-1971, 338-1971, 344-1971 were adhered to for both systems.

   NNECO has reviewed the design bases for separation of redundant channels of the RPS and ESFAS systems and concludes that the design adequately assures that a high energy line break will not impact more than one of four independent measurement channels. Therefore, the redundancy required by IEEE 279-1971 is met even with one channel in bypass. Spatial separation

---

[5]R. A. Clark letter to W. G. Counsil, dated March 31, 1982.

between cable trays carrying redundant cables is normally not less than four feet vertically and eighteen inches horizontally. Where these spacings between trays and redundant systems cannot be maintained, barriers are provided to preserve the physical and electrical integrity of the cables.

Each channel of the RPS is routed through a separate containment electrical penetration assembly. In the control room, each channel is located in a separate compartment. Mechanical and thermal barriers exist between compartments to preclude common failures.

Physical separation of the redundant channels of the ESFAS is equivalent to that of the RPS. Physical and electrical separation of the RPS is described in Millstone Unit No. 2 FSAR Sections 7.2.5 and 7.2.6.4, while this subject is discussed in FSAR Section 8.7 for the ESFAS.

The NRC Staff has previously reviewed and evaluated the protection and control system in accordance with the Commission's General Design Criteria (GDC) as published July, 1971, and IEEE 279, dated June 3, 1971. Based on a review of the FSAR and various electrical drawings, the Staff determined in the Safety Evaluation Report (SER) for Millstone Unit No. 2 that the final design of the protection and control systems, including operation with one channel in bypass, do indeed conform to the design criteria. Based on the review of the design bases, NNECO further concludes that the design satisfies the physical independence provisions of Regulatory Guide 1.75. Specifically, Regulatory Guide (RG) 1.75 describes a method acceptable to the NRC of complying with IEEE Standard 279-1971 and Criteria 3, 17, and 21 of Appendix A to 10CFR50 in this respect. Inasmuch as the SER has concluded that the protection systems do indeed conform to the applicable GDC and IEEE 279-1971, it may be concluded that the Staff has previously concurred with our determination of compliance with RG 1.75.

2. Single Failure in Combination with Prolonged Bypass

There may be cases where the prolonged bypass of a specific protection channel in combination with a single failure might jeopardize plant protection (i.e., channels remaining will not sufficiently detect associated transients and accidents without causing unacceptable consequences such as core damage, etc.). The licensee should review the accident analyses (i.e., rod drop accident, rod ejection, etc.) to verify that the bypass of a specific protection channel in coincidence with a single failure of a redundant channel will not prevent required protection for any transient or accident.

Response:

NNECO has had its fuel vendor review the Item 2 concerns and has concluded that bypass of a specific protection channel in combination with a single failure will not prevent required protection for any transient.

Three asymmetric accidents were identified to be of interest. They are:

a) single rod withdrawal accident,

b) dropped Control Element Assembly (CEA) events and

c) CEA ejection at hot zero power and hot full power.

a. Single Rod Withdrawal Accident--This accident is not a design basis event for Millstone Unit No. 2. However, should a single rod withdrawal occur, the transient would be terminated on a thermal margin/low pressure trip since a single rod withdrawal would not result in a flux transient of sufficient magnitude to actuate the high power level trip generated by the excore detectors. The Millstone Unit No. 2 Technical Specifications also require a power reduction to no less than or equal to 70% in the case of a rod misaligned by more than 20 steps from its respective bank.

b. Dropped CEA Accident--This accident at Millstone is not a limiting event and does not require a trip signal from the excore detectors to ensure the specified acceptable fuel design limits (SAFDLs) are maintained. Adequate margin for this event is ensured by operating the plant within the requirements of the Technical Specifications.

c. CEA Ejection Transient--The CEA ejection transient relies upon termination by a reactor trip actuated by neutron flux signals. The reactor trip prevents core conditions which may lead to damage to the reactor coolant pressure boundary, or sufficiently disturb the core, its support structures or other reactor pressure vessel internals such that the capability to cool the core is significantly impaired. The consequence of a CEA ejection is a rapid reactivity insertion together with an adverse core power distribution, possibly leading to localized fuel rod damage. The core power rise is limited by the Doppler feedback effect, and the transient is terminated by a reactor shutdown following a high power level trip.

For the safety evaluation of the CEA ejection transient, power distributions were generated for a number of ejected rods to determine if the resulting signals could actuate the neutron flux trip with one channel in bypass and a single failure of a redundant channel. For the worst case ejected rod, the two detectors are assumed to be radially adjacent and are on the far side of the core opposite the ejected CEA. This situation does not present a problem since there is sufficient flux propagation across the core that excore detector perception would not be impaired.

Therefore, it is concluded that bypass of a specific protection channel in coincidence with a single failure of a redundant channel will not prevent required protection for any transient or accident.

3. Channel Independence

The four protection channels must be reviewed for physical independence. Each licensee should confirm that the four protection channels as installed meet the physical independence criteria of Regulatory Guide 1.75.

Response:

The four protection channels for both the RPS and ESFAS as installed meet the physical independence criteria of Regulatory Guide 1.75. NNECO refers the reader to our response to Criterion 1 for additional details.

4. Independence of the Vital Buses

Each plant must be reviewed for independence of the vital buses. The Combustion Engineering (CE) reactor protection system (RPS) is made up of four (4) protection channels for each trip parameter. Each parameter channel consists of bistable relays and associated contacts which are arranged into six logic ANDS (AB, AC, AD, BC, BD, CD matricies) which represent all possible coincidences of two combinations (e.g., combinations of two-cut-of-four logic).

Each logic matrix is powered by two of four Class 1E independent 120 Vac vital buses as shown in Figure 1. This arrangement may challenge the isolation and hence independence of the redundant ac vital power buses. It is typical of licensees using the CE design to assure that the independence of these buses is maintained through the use of qualified isolators.

Licensees desiring to use the Technical Specifications of Enclosure 1 should confirm that tests and analyses have been performed to demonstrate independence of the redundant vital buses. The tests and supporting information should include:

a) The use of a plant-specific mock-up representing one protection logic matrix system (i.e., two matrix power supplies, each with its own simulated 120 Vac vital bus supply, matrix relays, bistable power supplies, bistable trip units, and isolation circuitry),

b) The application of surges (internal and external transient voltages) and faults (including continuous phase-to-phase short-circuits, phase-to-ground short-circuits and the application of continuous external high voltages) to the simulated 120 Vac vital bus supplying power to an associated matrix power supply,

c) Application of the surges and faults between each matrix power supply input conductor and ground (common mode) and across (line-to-line) the matrix power supply input conductors (transverse mode),

d) Monitoring the redundant simulated 120 Vac vital bus supplying power to its matrix power supply to measure any effect as a result of application of the faults or surges on the other bus

e) Acceptance criteria for perturbations which would be allowed within the redundant vital bus without interfering with any protection system actions,

f) Justification that the faults and surges used during the testing exceed the maximum worst-case failures which could occur within the protection systems circuits.

Response:

At Millstone Unit No. 2 four DC/AC inverters power four vital instrument buses which provide independent 120 volt AC power for each measurement channel in the RPS and ESFAS. Two inverters are supplied by the Facility 1 safeguards battery and two inverters are supplied by the Facility 2 battery.

To provide increased reliability, each of the four vital AC buses which supply each respective RPS channel has an alternate power supply via a "zero break" status transferswitch. Vital channels 1 and 2 are fed from the separate DC/AC inverters whose source of DC power is the turbine battery. Vital channels 3 and 4 are fed from one of the two regulated AC instrument power panels. In the event of a loss of a vital bus, the protective channel associated with the bus goes into a trip condition.

NNECO has performed an evaluation of the RPS circuitry including the 28 VDC Matrix Logic Power Supplies to demonstrate the independence of the vital buses. Using the criteria set forth in item 4 of Reference (1), the following observations are made:

- o Single phase to ground faults and surges applied to a vital AC source will have no effect whatsoever. Since the circuits are ungrounded, no current will flow.

- o A continuous phase-to-phase short-circuit of the vital AC input to one Matrix Power Supply will have no effect upon the output of the other Matrix Power Supply or its vital AC input. A half trip condition will result from the loss of output of the Matrix Power Supply whose input is short circuited.

- o Even if transverse mode surges or continuous high voltage were applied to a Matrix Power Supply and effects were assumed to propagate through the regulated power supply to the Matrix circuits and relays, the redundant vital AC supply would be effectively isolated from the assumed effects by the inherent DC to AC blocking of the associated power supply as well as a reverse biased diode and the impedance of the Matrix relays plus the shunting effect of the normally closed Matrix contacts.

Based on the above observations, it is concluded that no single failure of a vital AC supply will unacceptably degrade another.

5. Logic Matrix Circuitry Failure Due to a Vital Bus Single Failure

Each plant must be reviewed to assure that, with a channel in bypass, a single failure of a vital bus will not prevent the protection system from performing its protective function.

As stated in item 4 above, the CE reactor protection system forms six logic matricies (AB, AC, AD, BC, BD and CD) from all possible coincidences of two combinations of the four protection channel bistables and associated contacts. Due to the vital bus arrangement a single failure of a vital bus coincident with the bypass of a channel could prevent the required protective function of the RPS.

Looking at figure 1, assume that a channel A trip parameter is bypassed. This results in negating the AB, AC and AD logic matricies protective functions. This now leaves the BC, BD, and CD logic matricies for protection. However, as shown in figure 1, these remaining matricies are being supplied by a common vital bus. It can now be postulated that a single failure (fault, surge, etc.) within the common vital bus system might propagate through the logic matrix power supplies into the matrix circuitry. This could thereby cause a failure (welding of contacts) of the remaining logic matricies such that the required protective function cannot be performed.

Licensees desiring to use the Technical Specifications of Enclosure 1 should confirm that sufficient tests and analyses have been performed to assure that with a channel bypassed, a vital bus single failure will not negate the required protective function. The tests and supporting information should include:

a) The use of a plant-specific mock-up representing one protection logic matrix system (i.e., two matrix power supplies, each with its own simulated 120 Vac vital bus supply, matrix relays, bistable power supplies, bistable trip units, and isolation circuitry),

b) The application of surges (internal and external transient voltages) and faults (including continuous phase-to-phase short-circuits, phase-to-ground short-circuits and the application of continuous external high voltages) to the simulated 120 Vac vital bus supplying power to an associated matrix power supply,

c) The application of surges and faults between each matrix power supply input conductor and ground (common mode) and across (line-to-line) the matrix power supply input conductors (transverse mode),

d) Monitoring the auctioneered matrix power supply output to measure any effect on the logic matrix circuitry as a result of application of the faults or surges,

e) Verification that during and after the application of the surges and faults, the protection circuits will perform their protective actions,

f) Justification that the faults and surges used during the testing exceed the maximum worst-case failures which could occur within the protection systems circuits.

Response:

In analyzing a potential logic Matrix circuitry failure due to a vital bus single failure, the same model and faults used in the previous analysis with respect to item 4 are used again. Therefore, the previous observations are applicable. This means that only transverse mode surges or continuous high voltage applied to a Matrix regulated power supply have any potential for causing logic Matrix circuitry failures. If it were assumed that a higher than normal voltage were to result at the output terminals of the regulated power supply, a higher than normal current would flow through Matrix logic

contacts and the two Matrix relays associated with the power supply. Since the contacts are normally closed (low resistance), little heating (I^2R) of the contacts could occur. However, heating in the relay coils would rise, possibly causing one or both relay coils to fail. Such relay coil failures, however, are not of concern since failure of one or both of these coils will de-energize its respective trip circuit breaker control relay resulting in a half-trip condition. Contact welding would not occur due to either self heating or contact opening, since welding requires both molten contact material and contact pressure.

While Criterion 5 postulates a high-voltage condition at the output terminals of a power supply, no failure is recognized which would cause such a condition. As discussed in item 4, the vital buses are normally powered from inverters. As such, the maximum output voltage of an inverter is limited by the input battery voltage. Additionally, the inverters regulate the output voltage of 120 volts AC to within $\pm$ 2 percent with an input voltage of up to 140 volts DC. The distribution circuits from the vital buses are provided with fuses and circuit breaker protection to assure individual circuit faults are isolated close to the fault. Additional detail on the battery system and 120 volt instrument power for the RPS and ESFAS are provided in section 8.5 and 8.6 of the Millstone Unit No. 2 FSAR.

Based on the above information, it is concluded that only a failure which would result in welding Matrix Relay Contacts would prevent tripping. No such single failure is credible. This determination is supported by Regulatory Guidance published in SECY-77-439, regarding the application of Single Failure Criterion of Appendix A of 10CFR50, which states in pertinent part:

> "...only those systems or components which are judged to have a credible chance of failure are assumed to fail when the Single Failure Criterion is applied."

Summary

Based on the review of the original design bases, including physical and electrical separation of the RPS and ESFAS channels, NNECO has addressed the criteria outlined in enclosure 2 of Reference (5) and determined that Millstone Unit No. 2 complies with those criteria as discussed above.

Thus, in accordance with present Millstone Unit No. 2 Technical Specifications, NNECO concludes that one channel of the four channel protection system may be bypassed for an indefinite period of time without compromising safety. There is no need to propose more restrictive Technical Specifications at this time.

This determination is further supported by NUREG 1024 "Technical Specifications Enhancing the Safety Impact." Under the direction of Mr. Victor Stello, Jr., NUREG 1024 documents the work of an NRC Task Group established to identify the scope and nature of problems existing in current Technical Specifications. One finding of Task Group relevant to this subject recommends that action statements should:

> "...assure that they are designed to direct the plants to a safe operational mode such that public risk is minimized and that unnecessary transients and shutdowns are precluded."

As evidenced by our discussion above and in Reference (4), operation at Millstone Unit No. 2 allowing one channel in bypass does, in fact, reduce the probability of inadvertent protection system trips or unnecessary shutdowns while maintaining the integrity of the system and thus assuring public risk is minimized.

By letter dated April 4, 1984(6), the NRC Staff requested that Northeast Nuclear Energy Company inform the Staff in writing of our final decision regarding the withdrawal or modification of our application to amend the Technical Specifications as requested September 21, 1977. The application proposed specifications reflecting operation with the RPS in a two-out-of-three logic configuration. On the basis of our discussion above, NNECO has met the criteria delineated in Reference (5) to apply option 2 allowing plant operation with one RPS channel in bypass. As such, NNECO withdraws its application of Reference (2), and proposes to retain existing Technical Specification provisions.

We trust you will find this information satisfactory to resolve this issue.

Very truly yours,

NORTHEAST NUCLEAR ENERGY COMPANY

W. G. Counsil
Senior Vice President

---

(6) J. R. Miller letter to W. G. Counsil, dated April 4, 1984.