TECHNICAL EVALUATION OF THE ELECTRICAL, INSTRUMENTATION, AND CONTROL ASPECTS OF THE OVERPRESSURE MITIGATING SYSTEM FOR SURRY, UNITS 1 AND 2

(Docket Nos. 50-280, -281)

EG&G Idaho, Inc.

8002130

CONTENTS

1.0 INTRODUCTION 1

2.0 EVALUATION 1

2.1 System Electrical and Control Description 2

2.1.1 Isolation Valve Alarm 3
2.1.2 PORV Channel Separability 4
2.1.3 PORV Operation 5

2.2 System Testability 5

2.3 Pressure Transient Reporting and Recording Requirements 6

2.4 Disabling of Components During Cold Shutdown 6

2.5 Technical Specifications 6

3.0 CONCLUSIONS 7

4.0 REFERENCES 8

TECHNICAL EVALUATION OF THE
ELECTRICAL, INSTRUMENTATION, AND CONTROL ASPECTS
OF THE OVERPRESSURE MITIGATING SYSTEM
FOR SURRY, UNITS 1 AND 2

(Docket Nos. 50-280, -281)

1.0 INTRODUCTION

By letter dated October 14, 1977 (Reference 1) Virginia Electric and Power Company (VEPCO) submitted to the NRC a plant specific analysis in support of the proposed reactor vessel overpressure mitigating system (OMS) for Surry Nuclear Power Station, Units 1 and 2. This information supplements other documantation submitted by VEPCO during 1976 and 1977 (References 2 through 8). The electrical, instrumentation, and control system aspects of the proposed design have been reviewed for this Technical Evaluation Report.

The proposed OMS includes sensors, actuating mechanisms, alarms, and valves to prevent a reactor coolant system transient from exceeding the pressure/temperature limits included in the Surry, Units 1 and 2 Technical Specifications as required by Appendix G to Chapter 10, Code of Federal Regulations, Part 50 (10 CFR 50).

2.0 EVALUATION

The proposed overall approach to eliminating overpressure events incorporates administrative, procedural, and hardware controls with reliance upon the plant operator for the principal line of defense. Preventive administrative/procedural measures include (a) procedural precautions, (b) deenergization of essential components not required during the cold shutdown mode of operation, and (c) maintaining a non-water solid reactor coolant system condition whenever possible.

The basic design criteria that were applied in determining the adequacy of the electrical, instrumentation, and control aspects of the low temperature overpressure protection system are:

POOR ORIGINAL

(1) Operator Action – no credit can be taken for operator action until ten minutes after the operator is aware, through an action alarm, that a pressure transient is in progress.

(2) Single Failure Criterion – the pressure protection system shall be designed to protect the reactor vessel given a single failure in addition to the failure that initiated the pressure transient.

(3) Testability – the system design shall include provisions for testing on a schedule consistent with the frequency that the system is relied upon for pressure protection.

(4) Seismic and IEEE 279 Criteria – ideally, the system should meet seismic Category I and IEEE 279 criteria. The basic objective is that the system should not be vulnerable to a common failure that would both initiate a pressure transient and disable the OMS. Such events as loss of instrument air and loss of offsite power must be considered.

In addition to complying with these criteria, the licensee has agreed to provide a variety of alarms to alert the operator to (a) manually enable the pressure protection system during cooldown, (b) indicate the occurrence of a pressure transient, and (c) indicate closure of either power operated relief valve (PORV) isolation valve which ensures a complete pathway from the pressurizer to the pressurizer relief tank.

2.1 System Electrical and Control Description

The control circuitry for the OMS has been designed to comply with IEEE-Std 279-1971, except for the two variations discussed in

POOR ORIGINAL

Section 2.1.2. The compliance of the design with IEEE 279-1971, including the exceptions described by VEPCO (Reference 5) is adequate.

The OMS has two channels that are completely independent except that the channels share an alarm to show that the OMS should be enabled and an alarm to indicate the approach to a possible overpressure event. The alarms are isolated from the channels they serve so that a failure in the alarm circuitry will not incapacitate either channel. Each channel of the OMS is enabled by transferring the key operated ENABLE/DISABLE switch for the channel from the DISABLE to the ENABLE position (two switches must be transferred to completely enable the OMS). Each channel has two pressure setpoints. Setpoint #1 has a value of 400 psig for both channels. When the OMS is enabled the NDT PRESSURE HIGH annunciator will be activated if the pressure exceeds Setpoint #1 for either channel, thus alerting the operator of the need for actions to remedy the cause of the increasing pressure. Setpoint #2 has a value of 410 psig for Channel #1 and a value of 425 psig for Channel #2. When the OMS is enabled and the pressure exceeds Setpoint #2 for a channel, the pressurizer (PORV) for that channel is opened to provide a pathway from the pressurizer to the pressurizer relief tank.

During power operation the ENABLE/DISABLE switches for both channels of the OMS are in the DISABLE position, and the pressure is above Setpoint #2 for both channels so that the NDT PRESSURE SYSTEM REQUIRED annunciator is off. As the reactor is cooled down the pressure decreases and, when it reaches 400 psig, the NDT PRESSURE SYSTEM REQUIRED annunciator comes on, thus alerting the operator of the need to manually enable the OMS by transferring both key-controlled ENABLE/DISABLE switches to the ENABLE position. If both isolation valves between the pressurizer and the pressurizer relief tank are open, the NDT PRESSURIZER SYSTEM REQUIRED annunciator will go off, indicating that the OMS is enabled. These design features are adequate.

2.1.1 Isolation Valve Alarm. The required isolation valve alarm is provided by the NDT PRESSURE SYSTEM REQUIRED annunciator. When the

POOR ORIGINAL

OMS is being enabled, the annunciator will not clear unless both isolation valves have been opened. This ensures that a path from the pressurizer to the pressurizer relief tank is maintained. With the OMS enabled, the annunciator will alarm upon the closing of either isolation valve. The two channels share a single alarm. These design features are adequate.

2.1.2 PORV Channel Separability. Each of the two PORVs has its own independent instrumentation and control channels, except that the two channels share a common annunciator. A Failure Mode and Effects Analysis (Reference 8) has shown that no single failure can disable both channels, and VEPCO has stated that the design meets all of the final criteria except the following two requirements from IEEE 279 for electrical components:

(1) The requirement of automatic removal of a bypass (Section 4.12)

The bypass function will be served by two key lock swiches, one for each power operated relief valve, under administrative control. The switch will be enabled at the proper point (temperature versus pressure) on the cooldown curve and disabled at the proper point on the heatup curve. The position of the switch versus system requirements will be annunciated to indicate improper system alignment.

(2) The requirement of identifying components as to protection grade (Section 4.22)

The existing components are mounted and wired in control cabinets and wireways. However, channel independence conditions are met, as the channels are totally separate and the new system will also be installed separately. To disrupt the existing

POOR ORIGINAL

system to move the components and wires into protection marked areas does not provide a sufficient advantage to be worth the risk involved to the rest of the station.

The exceptions to IEEE 279 are justifiable and the design is adequate.

2.1.3 PORV Operation. The pressurizer power operated relief valves (PORVs) are spring-loaded, normally-shut valves that are opened by motive air controlled by solenoid operated valves (SOVs), one for each PORV when the CMS is enabled. The motive air is normally supplied by the containment instrument air system. To ensure operability upon loss of the normal air supply, each PORV has an independent backup air supply. One PORV opens at 410 psig and resets at 400 psig, the other opens at 425 psig and resets at 415 psig. Each backup air supply will have four high pressure bottles with each bottle capable of opening a PORV 31 times so that the system capacity is 125 cycles. This sizing considers that the fastest system response time is six seconds per cycle and that operator response will not take place for ten minutes. On this basis, the required capacity for the backup air supplies is 100 cycles. Check valves isolate the normal and the two backup air supplies so that a failure in one supply will not disable the other supplies. This design is adequate.

2.2 System Testability

Testability will be provided prior to establishing a solid system by use of the remotely operated isolation valve, ENABLE/DISABLE switch, and normal electronics surveillance procedure methodology. The testing requirements will be incorporated in the Technical Specifications. The provisions for testability are adequate.

POOR ORIGINAL

2.3 Pressure Transient Reporting and Recording Requirements

The staff position on a pressure transient which causes the overpressure protection system to function, thereby indicating the occurrence of a serious pressure transient, is that it is a 30-day reportable event. In addition, pressure and temperature instrumentation are required to provide a permanent record of the pressure transient. The response times of the temperature/pressure recorders shall be compatible with a pressure transient increasing at a rate of approximately 100 psi per second. This instrumentation shall be operable whenever the OMS is enabled.

2.4 Disabling of Essential Components Not Required During Cold Shutdown

Except as required for brief intervals by operating procedures or Technical Specifications, the staff position requires that essential components not required during cold shutdown that could produce an overpressurization event, be disabled or isolated from the RCS during cold shutdown and that the controls to disable or isolate these components be incorporated in the Technical Specifications. In particular, the safety injection accumulators and the high pressure safety injection pumps are included in the components to be disabled or isolated. While the system is water solid, two of the three charging pumps will be disabled by removal of the power to them. Valves and breakers used to disable equipment during cold shutdown will be tagged or locked to prevent inadvertent changes of state.

2.5 Technical Specifications

To ensure operation of the OMS, the licensee is to submit for staff review Technical Specifications to be incorporated into the license for Surry, Units 1 and 2. These specifications are to be consistent with the intent of the statements below. The licensee should ensure that the Technical Specifications proposed are compatible with other licensee requirements.

POOR ORIGINAL

(1) Whenever the RCS temperature is less than the minimum pressurization temperature, the OMS shall be enabled with both PORVs operable, except one PORV may be inoperable for seven days. If these conditions are not met, the primary system must be depressurized and vented to the atmosphere or to the pressurizer relief tank within eight hours.

(2) Enablement of the overpressure mitigating system requires that the low pressure setpoint will be selected, the upstream isolation valves open, and the backup air supply charged.

(3) No more than one high head SI pump injection valve may be energized at RCS temperatures below 380°F unless the vessel head is removed.

(4) A reactor coolant pump may be started (jogged) only if there is a steam bubble in the pressurizer or the SG/RCS temperature difference is less than 50°F.

(5) The OMS must be tested on a periodic basis consistent with the need for its use.

(6) When the plant is in a cold shutdown condition, the safety injection accumulators shall be isolated from the RCS by verifying that the accumulator isolation valves are in the closed position and power to the valve operators is removed.

3.0 CONCLUSIONS

The electrical, instrumentation, and control aspects of the Surry, Units 1 and 2 OMS design are adequate on the basis that (a) the compliance with the IEEE 279 design criterion is acceptable, (b) the system

POOR ORIGINAL

is redundant and meets the single failure criterion, (c) the design requires no operator action for ten minutes after the operator receives an overpressure action alarm, (d) the system is testable on a periodic basis, and (e) the proposed changes to the Technical Specifications reduce the probability of overpressurization event to an acceptable level. However, it is recommended that final acceptance by the NRC be contingent upon the licensee incorporating Technical Specifications that comply with the list in Section 2.5.

4.0 REFERENCES

1. VEPCO letter (Stallings) to NRC (Rusche) dated October 14, 1978.

2. VEPCO letter (Stallings) to NRC (Rusche) dated September 7, 1976.

3. VEPCO letter (Stallings) to NRC (Rusche) dated November 3, 1976.

4. VEPCO letter (Stallings) to NRC (Rusche) dated December 17, 1976.

5. VEPCO letter (Stallings) to NRC (Rusche) dated February 25, 1977.

6. VEPCO letter (Stallings) to NRC (Rusche) dated February 25, 1977.

7. VEPCO letter (Stallings) to NRC (Rusche) dated April 22, 1977.

8. VEPCO letter (Stallings) to NRC (Rusche) dated April 1, 1977.

9. Memorandum, R. Baer to K. Goller, December 29, 1977, Review of Surry, Units 1 and 2 Overpressure Mitigating System.

POOR ORIGINAL