860923

SAFETY EVALUATION REPORT
PRESSURE TRANSMITTER FAILURE EVENT OF JULY 30, 1986 AND RESULTANT INOPERABILITY OF STEAMFLOW/FEEDFLOW MISMATCH TRIP CIRCUITS AT SAN ONOFRE, UNIT 1

INTRODUCTION

The steam pressure transmitter (PT459), which is used for density compensation of all steam flow channels, failed on July 30, 1986. The failure of the transmitter caused a loss of feedwater transient and loss of capability to trip the reactor on steam/feed flow mismatch. The steam/feedwater flow mismatch signal provides first line protection for loss of feedwater events as input to the Reactor Protection System and is one of the input signals to the feedwater control system. Reactor trip occurs when steam flow exceeds feedwater flow by a preset amount for any two of the three steam generators. The staff has reviewed the loss of feedwater event and the design of steam/feedwater flow mismatch protection against the licensee's design criteria as stated in Amendment 19 of the Final Operating License Application (Reference 1) and in a Systematic Evaluation Program submittal (Reference 2) as described in the following evaluation.

EVALUATION

The feedwater flow and the steam flow signals are used to anticipate changes in steam generator level and provide protection against feedwater loss by initiating a scram upon flow mismatch above a predetermined setpoint (25%). Signals from three independent steam flow monitors FT460, FT461 and FT462 and three independent feedwater flow monitors FT456, FT457 and FT458 are fed into three comparator bistables, FM456B, FM457B

and FM458B, respectively. However, only one steam pressure transmitter (PT459) is used for density compensation of all steam flow channels which in turn are used in all three steam/feed flow mismatch trip circuits. Southern California Edison (SCE), the licensee for San Onofre Unit 1, responded in Amendment No. 19 to the Final Operating License Application (Part 1, Volume 1, Section 3.1) submitted by Reference 1 with the following statements regarding Criteria No. 20 and 22;

Statement of Criterion 20 - Protection Systems Redundancy and Independence:

"Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure or removal from service of any component or channel of a system will result in loss of the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served. Different principles shall be used where necessary to achieve true independence of redundant instrumentation components."

Licensee Statement:

"The San Onofre protection systems are designed such that failure or removal from service of any component or channel will not result in loss of protection function. Each protection parameter is monitored by at least two channels. Loss of one channel leaves redundant channels capable of initiating safety action intact. Redundant channels are separate and independent, with separate detectors, power sources, signal conditioning equipment and logic devices.

Statement of Criterion 22 - Separation of Protection and Control Instrumentation Systems:

"Protection systems shall be separated from control instrumentation systems to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels."

Licensee Statement:

"In evaluating the control and protection system interaction with respect to conformance to IEEE 279, it has been shown that although actual separation is not in all cases accomplished, effective separation of control and protection systems has been achieved. The control system includes pressure, linear flux, and temperature channels which are also in the protection system. The channel redundancy provided and the control system design are such that failure of a channel common to both the protection and control systems would leave intact systems which satisfy the general functional requirements and the failure criteria."

With regard to the Systematic Evaluation Program, SCE made the following response in Reference 2 regarding steam/feedwater flow mismatch.

Steam/Feedwater Flow Mismatch:

"Isolation of the feedwater flow controller, action pak, and process recorder can be demonstrated for open circuit faults. This is due to the parallel wiring scheme used at San Onofre Unit 1 for the feedwater flow controller, action pak, and process recorder which allows the signal to perform its protection function despite an open circuit fault in either device."

"Although no isolation exists for the other postulated faults, RPS function is assured by the complete independence of the three redundant channels within the steam to feedwater flow mismatch circuitry. The 2 out of 3 voting logic is configured such that any fault on one channel will not preclude these circuits from performing their protection functions."

It is the staff's assessment that the design of the SONGS 1 steam/feedwater mismatch protection does not conform with the licensee's description of design capability in regard to the single failure criterion and control system

interaction as described above. The rationale for assessing the plant to be in nonconformance with its design basis is based on the single failure of the pressure transmitter (PT459) which caused a transient and a loss of first-line protection function. Contrary to SCE's description of the design capability in the Final Operating License Application, all three channels of steam/feedwater flow mismatch were lost due to a single failure of the pressure transmitter.

As stated above under criterion 20, separate signal conditioning equipment is provided for each channel. However, only one steam pressure transmitter (PT459) is provided for the three Steam Flow Computers (FM 460, FM 461 and FM 462). In order to comply with the SCE stated design description, separate independent pressure transmitters should have been provided for each steam generator to meet the single failure criterion.

CONCLUSION

The staff has concluded that the design of the steam flow/feed flow mismatch trip circuits does not conform to the applicable design criteria 20 and 22 contained in Amendment 19 of the Final Operating License Application (Reference 1). The staff considers these criteria and the statement in Reference 2 on steam to feedwater flow mismatch to be part of the licensing basis of SONGS #1. It is the staff's position that modifications should be made to bring the subject system into

conformance with its design bases or the design bases redefined with appropriate analyses and justification provided for the revised design bases. Furthermore, the licensee should perform a review of the Reactor Protection System and Engineered Safety Features Actuation System for conformance to the criteria in References 1 and 2 and submit the results of this review to the staff.

References:

1. Letter, J. B. Moore, SCE to Director, DOL, NRC, dated July 28, 1970.

2. Letter, M. O. Medford, SCE to D. M. Crutchfield, NRC, dated March 30, 1984.

ENCLOSURE #2

REQUEST FOR ADDITIONAL INFORMATION

1. Provide the results of the analyses/reanalyses for all events for which the steam/feedwater mismatch provides protection showing the timing of the RPS trips for primary and backup protection.

2. Describe the effect of a power supply failure to the pressure sensing instrumentation on the feedwater control system and steam/feedwater mismatch protection system. Describe and identify the power supplies to the pressure sensing channel and the steam and feedwater flow instrumentation as well as the other instrumentation providing protection against loss of feedwater events.

3. Describe all functions of the steam line pressure transmitter PT-459, i.e., identify all instrumentation channels and equipment or systems to which it provides signal input. Describe those operator actions, if any, which are based on use of this transmitter to measure steam pressure.

4. Discuss the consequences of failure of the steam-line pressure transmitter in such a manner that it measures an erroneous high pressure, low pressure or provides no signal. Describe the results of the worst case failure of the pressure sensing system and its impact on feedwater control and reactor protection without operator action.

5. Describe and provide the results of any reanalyses of accidents and transients for which earlier analyses relied on signals provided by the pressure transmitter. Include, but not necessarily limit discussion to the following:

   a. Loss of normal feedwater with the limiting single failure of an auxiliary feedwater pump. The revised analysis discussed in your submittal of August 21, 1986 was intended to address the impact of no steam flow/feed flow mismatch reactor trip on a loss of normal feedwater transient. However, your revised analysis does not consider the effect of a limiting failure in the auxiliary feedwater system. Since failure of the pressure transmitter may be the initiator for this transient it is necessary to address an accompanying independent single failure such as the turbine driven AFW pump.

   b. Feedwater line break outside containment with the limiting single failure.

   c. Feedwater line break inside containment with the limiting single failure.

   d. Steam line breaks inside and outside containment with the accompanying limiting single failure. For steam line breaks inside containment discuss both containment pressure and reactor coolant system cooldown effects.