SECTION 7

INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

Instrumentation and Control Systems provide the reactor operator with the required information and control capability to operate the station in a safe and efficient manner. Where safety functions are involved, logic circuitry and actuators are provided to execute equipment actions without operator action.

Instrumentation and Control Systems are broadly classified as being either Safety-Related Systems or Control Systems. The nuclear instrumentation (1) and engineered safety features' circuits are discussed in separate parts of this section. Other specific design features or topics also separately discussed are: in-core instrumentation, operating control stations and engineered safeguards sequence control. Controls and electrical drawings for safety-related equipment can be found in Reference 2.

Instrumentation and controls are provided to monitor and maintain all operationally important reactor operating parameters such as neutron flux, system pressures, flow rates, temperatures, levels, and control rod positions within prescribed operating ranges. The quantities and types of instrumentation provided are adequate for safe and orderly operation of all systems and processes over the full operating range of the plant.

Process variables which are required on a continuous basis for the startup, power operation, and shutdown of the station are indicated in, recorded in, and controlled as necessary from the Control Room. The operating staff is cognizant and in control of all test, maintenance, and calibration work and can fully assess all abnormal plant conditions knowing the extent to which specific and related operating tasks are in process.

Control System failure analyses have been conducted for Unit 2 and were reported to the Nuclear Regulatory Commission on June 2, 1982, in a report entitled, "Salem Generating Station, Unit 2, Control Systems Failure Analysis." The systems reviewed were 1) Steam Dump, 2) Ex-core Nuclear Instrumentation, 3) Pressurizer Pressure and Level Control, 4) Feedwater Control and 5) Rod Control. The systems were evaluated for: 1) break of common instrument lines, 2) loss of power to all components powered from a single source, and 3) break of any single instrument line. It was concluded that the consequences of single control system failures are adequately bounded by the accident analyses of Section 15.

7.1.1 Identification of Safety-Related Systems

7.1.1.1 Reactor Trip Systems

The Reactor Trip System consists of equipment which initiates reactor trip or activates engineered safety features. All equipment from sensors to actuating devices is considered a part of the protective system. The reactor trip breakers and the undervoltage attachment are safety related. Engineered safety features are discussed in Section 7.3.

Design criteria permit maximum effective use of process measurements both for control and protection functions, thus enhancing the capability to provide an adequate system to deal with the majority of common-mode failures as well as to provide redundancy for critical control functions. The design approach provides for monitoring of numerous system variables by different means, i.e., system diversity. This diversity has been evaluated for a wide variety of postulated accidents (3).

7.1.1.2 Fission Process Monitors and Controls

Criterion: Means shall be provided for monitoring or otherwise measuring and maintaining control over the fission

process throughout core life under all conditions that can reasonably be anticipated to cause variations in reactivity of the core.

The Nuclear Instrumentation System described in Section 7.2 safeguards the reactor by monitoring the neutron flux and generating appropriate trips and alarms for various phases of reactor operating and shutdown conditions. It also provides indication of reactor status during startup and power operation.

A comprehensive discussion of the Nuclear Instrumentation System, covering design bases and a detailed description of the system, can be found in Reference 1.

7.1.1.3 Plant Comparison

Salem Generating Station's Protection and Engineered Safety Features Actuation Systems are functionally identical to those in the D. C. Cook Plant.

Both stations have solid state logic protection systems and extended testability of engineered safety features actuation circuitry.

Both stations have incorporated the power range fast flux rate trip with the corresponding deletion of the automatic rod withdrawal block on indication of rod drop.

The design of both systems conforms to IEEE Standard 279-1971 and the General Design Criteria.

7.1.2 Identification of Safety Criteria

7.1.2.1 Design Bases

Criterion: Core protection systems, together with associated equipment, shall be designed to prevent or to suppress

conditions that could result in exceeding acceptable fuel damage limits.

If the Reactor Trip System receives signals which are indicative of an approach to unsafe operating conditions, the system actuates alarms, prevents control rod withdrawal, initiates load cutback, and/or opens the reactor trip breakers.

The basic reactor operating philosophy is to define an allowable region of power, pressure, and coolant temperature conditions. This allowable range is defined by the primary tripping functions: The overpower ΔT trip, the overtemperature ΔT trip and the nuclear overpower trip. The operating region below these trip settings is designed so that no combination of power, temperatures, and pressure could result in departure from nucleate boiling ratio less than 1.3 for any credible operational transient with all reactor coolant pumps in operation. Tripping functions, in addition to those stated above, are provided to back up the primary tripping functions for specific abnormal conditions.

Rod stops from nuclear overpower, overpower ΔT, and overtemperature ΔT deviation are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal initiated by a malfunction of the Reactor Control System or by operator violation of administrative procedures.

7.1.2.2 Independence of Safety-Related Systems

7.1.2.2.1 Redundancy and Independence of Safety-Related Systems

Criterion: Redundancy and independence designed into safety-related systems shall be sufficient to assure that no single failure or removal from service of any component or channel of such 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.

The Reactor Trip System is designed so that loss of voltage in a channel will result in a signal calling for a trip, except for reactor coolant pump bus undervoltage, underfrequency, and auto shunt trip which require dc voltage to actuate. The Reactor Trip System design combines redundant sensors and channel independence with coincident trip philosophy so that a safe and reliable system is provided in which a single failure will not violate reactor protection criteria.

The design philosophy for the Reactor Protection and Control Systems is to make maximum use, for both protection and control functions, of a wide range of measurements. The Reactor Protection and Control Systems are separate and identifiable. The design approach permits not only redundancy of control, providing its own desirable increment to overall plant safety, but also provides a protection system which continuously monitors numerous system variables by different means; i.e., protection system diversity.

The extent of protection system diversity has been evaluated for a wide variety of postulated accidents (3). Generally, two or more diverse protective functions would terminate an accident before intolerable consequences could occur.

The Reactor Protection System is independent of the Control System, although the Control System is dependent upon signals derived from the Reactor Protection System through isolation amplifiers. The design approach is to make maximum and thereby most efficient use, for both control and protection purposes, of all measurements of plant variables.

In the Reactor Protection System, two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the rod cluster control assembly drive mechanisms. The breakers are connected in series with the power supply so that opening either breaker interrupts power to all full length rod drive mechanisms permitting the rods to free fall into the core.

Further detail on redundancy is provided through the description of the respective systems covered by the various subsections within this Section. The power supply for the Protection Systems is discussed in Section 8.

7.1.2.2.2 Protection Against Multiple Disability for Safety-Related Systems

Criterion: The effects of adverse conditions to which redundant channels or Protection Systems might be exposed in common, either under normal conditions or those of an accident, do not result in loss of the protection function or shall be tolerable on some other basis.

Separation of redundant analog protection channels originates at the process sensors and continues through the wiring route and containment penetrations to the analog protection racks. Physical separation is used to achieve separation of redundant transmitters. Separation of wiring is achieved using separate wireways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment is separated by locating modules in different protection rack sets. Each redundant protection channel set is energized from a separate instrument bus, which can be energized by the standby ac power system.

7.1.2.2.3 Demonstration of Functional Operability of Safety-Related Systems

Criterion: Means shall be included for suitable testing of the active components of protection systems while the reactor is in operation to determine if failure or loss of redundancy has occurred.

The signal conditioning equipment of each protection channel in service at power is capable of being calibrated and tested independently by simulated analog input signals to verify its

operation without tripping the reactor. The testing scheme includes checking through the trip logic to the trip breakers. Thus, the operability of each trip channel can be determined conveniently and without ambiguity. Functional operation of the power sources for the Protection System is discussed in Section 8.

7.1.2.2.4 Protection System Failure Analysis Design

Criterion: The protection systems shall be designed to fail into a safe state or into a state established as tolerable on a defined basis if conditions such as disconnection of the system, loss of energy (e.g., electrical power, instrument air), or adverse environments (e.g., extreme heat or cold, fire, steam, or water) are experienced.

Reactor trip channels are generally designed on the "de-energize to operate" principle; a loss of power causes a channel to go into its trip mode. Exceptions to this case are the reactor coolant pump bus undervoltage and underfrequency trips, and the automatic reactor shunt trip feature which require dc voltage to actuate. All safety-related air operated valves are spring loaded to move to the preferred position on loss of instrument air.

Reactor trip is implemented by simultaneously interrupting power to the magnetic latch mechanisms on all drives allowing the rods to insert by free fall. The protection system is thus inherently safe in the event of a loss of power. This equipment is selected to withstand the most adverse environmental conditions to which it will be subjected; this would also include post-accident conditions within the containment, if the equipment is required to operate in the post-accident environment.

7.1.2.2.5 Reactivity Control Systems' Malfunctions

Criterion: The Reactor Trip Systems shall be capable of protecting against any single malfunction of the Reactivity Control Systems, such as unplanned continuous

withdrawal (not ejection or dropout) of a control rod, by limiting reactivity transients to avoid exceeding acceptable fuel damage limits.

Reactor shutdown with rods is completely independent of the normal control functions since the trip breakers interrupt the power to the rod mechanisms regardless of existing control signals. Effects of continuous withdrawal of a rod and of deboration are described in Section 15.

7.1.2.3 Missile Protection

Criterion: Adequate protection for those engineered safety features, the failure of which would result in undue risk to the health and safety of the public, shall be provided against dynamic effects and missiles that might result from plant equipment failures.

The applicable portions of the missile protection criteria as stated in Section 1.3 apply to Class I equipment in this Section.

Several criteria related to all Instrumentation and Control Systems but more specific to other plant features or systems are discussed in other sections, as listed:

Criterion	Discussion
Suppression of Power Oscillations	Section 3
Reactor Core Design	Section 3
Quality Standards	Section 1
Performance Standards	Section 1
Fire Protection	Section 9
Missile Protection	Section 5
Emergency Power	Section 8

7.1.2.4 Periodic Testing of the Protection Systems (IEEE Standard 338-1971)

IEEE Standard 338-1971, "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," was used as a guide in developing the periodic testing program details for Salem.

1. The response time specified in Paragraph 4.1 of IEEE Standard 338-1971 is not checked periodically as is the setpoint accuracy. The response time of Protection System instruments is checked during preoperational testing and after replacement of any component affecting the response time. Response times are checked during refueling outages.

2. The reliability goals specified in Paragraph 4.2 of IEEE Standard 338-1971 are not applicable since the test frequencies are dictated in the Technical Specifications.

3. The periodic test frequency discussed in Paragraph 5.2 of IEEE Standard 338-1971, and specified in the Technical Specifications, is conservatively selected to assure that equipment associated with protection functions has not drifted beyond its minimum performance requirements.

4. The test interval discussed in Paragraph 5.2 of IEEE Standard 338-1971, is developed on past operating experience and analytical methods, and will be modified if necessary to assure that system and subsystem protection is reliably provided.

7.1.2.5 Conformance to IEEE Standard 344-1971

The Reactor Protection System, engineered safety feature circuits, and the Emergency Power System have been designed to assure that these systems do not lose their capability to perform the required functions in the event of a design basis earthquake. Such equipment is designed Class I as defined in Section C.1. A listing for the general category of Class I items is given in Section C.2.

The Protection System has been designed and qualified to assure its capability to initiate a protective action during the design basis earthquake. The engineered safety feature circuits have been designed and qualified to assure their capability in performing the required functions during post-accident operation. There may be deformation of the equipment; however, functional capability must be maintained. Equipment suppliers have been given the seismic design requirements, and the ability of such equipment to perform its required functions has been verified either by analysis or by testing. Typical Protection System and Engineered Safety Features System equipment are subjected to type tests under simulated seismic motion and/or dynamic mathematical analysis to demonstrate ability to function.

Type testing has been done on this equipment by using conservatively large accelerations and applicable frequencies. This testing conformed to the guidelines set forth in IEEE Standard 344-1971, "IEEE Guide for Seismic Qualification of Class I Electrical Equipment for Nuclear Power Generating Stations."

References 4, 5, 6, and 7 provide the seismic evaluation of safety-related equipment. The results show that there were no electrical irregularities that would leave the plant in an unsafe condition even though some trips were initiated.

Table 3.10-1 contains all the safety-related electrical equipment that requires seismic qualification.

7.1.2.6 Conformance and Exceptions to IEEE Standard 323-1971

The safety-related equipment is type tested to substantiate the adequacy of design. This is the preferred method as indicated in IEEE Standard 323-1971, "IEEE Trial-Use Standard Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations." Type tests already performed (References 4, 8, 10) in accordance with criteria standards established at the time of the construction permit, may not conform to the format guidelines set forth in IEEE Standard 323-1971.

7.1.2.7 Conformance to IEEE Standard 336-1971

Installation, inspection, and testing activities for instrumentation and electric equipment are in accordance with IEEE Standard 336-1971, "IEEE Standard Installation, Inspection and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations." The overall quality assurance program is described in Section 17.

7.1.2.8 Conformance to 10CFR50.62

The AMSAC conforms to the requirements of 10CFR50.62 as discussed in Section 7.8.

7.1.2.9 Instrumentation Piping/Tubing Code Reconciliation Associated With Unit 2 SGR

Instrumentation piping/tubing fabrication, installation, and examination involved in installing the Unit 2 Steam Generators utilized ASME Section XI (1998 Edition with 2000 Agenda) and ASME Section III, Subsection NC and NCA (1995 Edition through 1996 Addenda). Both of these later codes are NRC-endorsed per 10CFR50.55a and were reconciled to the original construction codes.

7.1.3 Control Room Design Review

A preliminary design review assessment of the Salem Unit 2 Control Room was undertaken in the spring of 1980 by Public Service Electric & Gas in conjunction with human factors personnel from Essex Corporation. It was concluded in the preliminary review "the design of the Salem 2 Control Room, which was repeatedly developed through the use of mockups and operator walk-throughs, evidences a high level of concern for the capabilities and limitations of the human operator, with some notable exceptions." The authors cautioned that the human engineering discrepancies and conclusions were tentative pending further evaluation and analysis. A detailed control room design review (DCRDR) (11) was subsequently undertaken. The DCRDR was performed for Units 1 and 2 in accordance with the intent of NUREG-0700 (12). The DCRDR process was divided into the following major steps:

1. Operating Experience Review
2. Control Room Inventory
3. Control Room Survey
4. System Function Review and Task Analysis
5. Verification of Task Performance Capabilities
6. Validation of Control Room Functions and Integrated Performance Capabilities

Design review team members assessed the identified and prioritized human engineering discrepancies (HEDs) and recommended corrective actions, if applicable, for the resolution of each. Recommendations for HED resolution were developed for all significant HEDs using the resources of the DCRDR team and other specialists (e.g., Plant Engineering and Operating Departments). These recommendations took into account the impact of the correction on operating effectiveness, system safety, acceptability of design, and consistency with present Control Room characteristics.

A list of all HEDs requiring plant changes appears in Section 3.1.1 of the DCRDR report (11). All HEDs identified during the review are listed in Volume 2 of the same report.

A re-evaluation of human factors issues affected by the changes in the general arrangement of the Control Room(s) undertaken in 1996 has been conducted. The human factors issues affected by the changes include lighting, control room colors, sound propagation, task analyses, relocation of communications devices and information systems, adequacy of storage locations and traffic flow within the control room. The results of this review are contained in Reference 13.

7.1.4 References for Section 7.1

1. Lipchak, J. B. and Stokes, R. A., "Nuclear Instrumentation System," WCAP-7380-L (Proprietary) December 1970 and WCAP-7669 (Nonproprietary), April 1971.

2. "Controls and Electrical Drawings for Safety-Related Equipment," Volumes 1 through 4, Salem Nuclear Generating Station, Units 1 and 2, Public Service Electric and Gas Company, July 1973.

3. Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse PWRs," WCAP-7306, April 1969.

4. Vogeding, E. L., "Seismic Testing of Electrical and Control Equipment," WCAP-7397-L (Proprietary), January 1970 and WCAP-7817 (Nonproprietary), December 1971.

5. Vogeding, E. L., "Seismic Testing of Electrical and Control Equipment (WCID Process Control Equipment)," WCAP-7397-L, Supplement 1 (Proprietary), January 1971 and WCAP-7817, Supplement 1 (Nonproprietary), December 1971.

6. Potochnik, L. M., "Seismic Testing of Electrical and Control Equipment (Low Seismic Plants)," WCAP-7817, Supplement 2, December 1971.

7. Vogeding, E. L., "Seismic Testing and Electric and Control Equipment (Westinghouse Solid State Protection System) (Low Seismic Plants)," WCAP-7817, Supplement 3, December 1971.

8. "Test Report - Nuclear Instrumentation System Isolation Amplifier," WCAP-7819, Revision 1, January 1972.

9. Deleted

10. Locante, J., "Environmental Testing of Engineered Safety Features Related Equipment (NSSS - Standard Scope)," WCAP-7410-L, Volume 1 (Proprietary), December 1970 and WCAP-7744, Volume 1 (Nonproprietary), August 1971.

11. "Public Service Electric & Gas Co.," Salem Generating Station, Units 1 and 2, Detailed Control Room Design Review, Volumes 1 and 2, December 1983.

12. USNRC, NUREG-0700, "Guidelines for Control Room Design Reviews."

13. "Public Service Electric & Gas Co.," Salem Generating Station, Units 1 and 2, Supplemental Control Room Human Factors Design Review in Support of DCP 1EC-3360.