~~OFFICIAL USE ONLY~~

Distribution:
Suppl.
RPB-5 Reading
Orig: DFKnuth
P. S. Boyd

Docket No. 50-275

NOV 30 1967

Mr. Munzio J. Palladino
Chairman, Advisory Committee
on Reactor Safeguards
U. S. Atomic Energy Commission
Washington, D. C. 20545

Dear Mr. Palladino:

Twenty-four copies of a report prepared by the Division of Reactor Licensing are transmitted for the review by the Committee. The report is the section on Instrumentation for the Diablo Canyon report transmitted on November 28, 1967.

Sincerely yours,

Peter A. Morris, Director
Division of Reactor Licensing

Enclosure:
ACRS Report (24 cys)

When separated from enclosures, handle this document
at UNCLASSIFIED
(Insert proper classification)

~~OFFICIAL USE ONLY~~ C-22

OFFICE ▶	RPB-5/DRL	DRL:PT	DRL:RP	DRL:D		
SURNAME ▶	~~DFKnuth~~/ds	SLevine	RSBoyd	PAMorris		
DATE ▶	11/29/67	11/ /67	11/ /67	11/30/67		

Form AEC-318 (Rev. 9-53)

U.S. GOVERNMENT PRINTING OFFICE : 1966—O-214-629

NOV 30 1967

5.0 Instrumentation and Control

5.1 Reactor Protection System

The reactor protection system monitors signals from nuclear and process instrumentation which are indicative of reactor plant operation. When an unsafe condition is sensed, the reactor protection system trips the reactor. The Diablo Canyon reactor protection system will differ from that provided for the San Onofre and Connecticut Yankee reactors. It will also differ from that described in recent PSAR's for Westinghouse designed plants. The changes were made to comply better with the provisions of the Proposed IEEE Standard, Nuclear Power Plant Protection Systems and as the result of the high power density core and the use of partial length rods. Because of the known design changes, we specifically asked for additional information for our review of the Diablo Canyon facility. This additional information was presented in Amendment No. 7. Our review is based on the information as submitted and from subsequent discussions with the applicant. The results of these discussions will be documented at a later date.

The reactor protection system will be designed on a channelized basis to provide for isolation between redundant protection channels. Isolation of redundant analog channels will originate at the sensors and continue back through the field wiring and containment penetrations to the analog protection racks. Isolation of field wiring will be achieved using separate wire ways, cable trays, conduit runs, and containment penetrations for each redundant channel. Redundant analog equipment will be isolated by locating the equipment in four separate protection racks. The four racks of equipment will be energized from separate a.c. power sources.

Each reactor protection system instrument channel will terminate in a

reactor trip bistable mounted in one of the four protection racks. The trip bistable is the final operational component in the analog channel. The transition from reactor protection instrument channel identity to logic channel identity will be made at the logic relay coil/relay contact interface. Each bistable will drive two logic relays (C&D). The contacts from the "C" relays are interconnected to form the required actuation logic for Trip Breaker No. 1 through d.c. power source No. 1. This logic network is duplicated for Trip Breaker No. 2 using d.c. power source No. 2 and the contacts from the "D" relays. The tripping of either breaker will trip the reactor. The two logic channels will be mounted in separate racks thus providing good physical and electrical separation. The only electrical connections between the logic channels are at the bistable to relay inter connections. The minimum physical separation will probably be in the manual trip switch circuit. The final design of this portion of the circuit will be evaluated in detail at the operating license review for adequacy of channel separation.

We believe that the channelized approach and the proposed electrical isolation and physical separation is adequate and meets the intent of the Proposed IEEE Standard, Nuclear Power Plant Protection Systems (Sec. 4.6).

The two, three pole reactor trip circuit breakers are connected in series between two paralleled three phase, 260 volt, rod drive MG sets and the rectifier d.c. power supplies. The trip breakers control a.c. power to four rectifier d.c. power supplies. The rod magnets are divided between four d.c. buses each of which is supplied by one of the d.c. power supplies. The opening of either trip breaker de-energizes all four d.c. buses and causes all of the rods (except the part length rods) to fall into the core. The applicant believes that the large amount of power required by the rod magnets essentially

rules out the possibility of a failure to trip due to a fault which applies a voltage source to the rod magnet circuit. We agree that the power requirements reduce the probability. We believe, however, that the multiple d.c. buses are important in assuring that the first detectable failure does not fail the system. There is a single three phase a.c. bus between the trip breakers and the d.c. power supplies. The applicant has stated that this bus will consist of totally enclosed bus bars. We believe that the voltage and current requirement (about 400 KVA at 260 volts three-phase) and the enclosed bus arrangement provides adequate assurance of meeting the single failure criterion. We will review the final bus arrangement in detail at the operating license evaluation.

The individual reactor protection channels feeding reactor trip signals into the logic channels are as follows:

Trip Parameter	Coincidence logic
High Nuclear Flux (source range) - high level	One out of two
High Nuclear Flux (intermediate range) - high level	One out of two
High Nuclear Flux (power range) low power trip	Two out of four
High Nuclear Flux (power range) high power trip	Two out of four
Low pressurizer pressure	Two out of four
High pressurizer pressure	Two out of four
High pressurizer water level	Two out of three
Turbine trip	Two out of three
Low reactor coolant flow	Two out of three in any one loop above 75% power Two out of three in any two loops above 10% power

Reactor coolant pump breaker opening	One out of one in any one loop above 75% power One out of one in any two loops above 10% power
Loss of feed water flow	One out of two steam-feed flow mismatch with one out of two low level in any steam generator.
Low steam generator level	Two out of three low-low water level in any steam generator
Overpower Δ T	Two out of four
Over temperature ΔT	Two out of four
Manual scram	

The nuclear instrumentation used for reactor protection is an out-of-core system. It consists of two source range channels, two intermediate range channels, and four power range channels. The power range detectors are long ionization chambers in which the center electrode is divided in two equal sections. Each long detector is in effect two detectors each equal in length to about half the length of the core. The ion current from the halves of each power range detector is summed to indicate reactor power and to supply signals for the high flux trips. The ion current from each detector half is displayed to provide the operator with a gross indication of flux distribution. The functional adequacy of the out-of-core nuclear instrumentation is covered elsewhere in this report.

The difference between the ion current in the upper and lower half of each power range detector will also be measured. If the difference exceeds a given level, a signal will be transmitted to the over power ΔT and the over temperature ΔT protection channels. This feature is provided for Diablo Canyon to protect the high power density core by reducing the overpower ΔT and over temperature ΔT reactor trip settings if the power is unequally distributed.

The overpower ΔT protection is basically a fixed ΔT trip. A hot leg and a cold leg resistance thermometer in each loop supplies ΔT information to a channel of overpower ΔT protection. The trip point is lowered upon measured differences in upper and lower signals of a power range detector. Each of the four power range detectors supplies a signal to a different overpower ΔT channel.

The over temperature ΔT is provided to protect the reactor by responding to ΔT, average temperature, and pressurizer pressure in the following manner:

$$\Delta T \text{ Trip} = \Delta T \text{ constant} - K_1 T_{avg} + K_2 P$$

The trip point of the overtemperature ΔT protection is reduced upon unequal flux distribution in the same manner as in the overpower ΔT protection.

The functional adequacy of the overpower ΔT and over temperature ΔT protection will be evaluated after the final design and analysis is completed.

Each instrumentation channel, both nuclear and process, which supplies a signal for reactor portection is read out in the control room. The read-out allows the operator to detect failures in the analog portion of protection channels by cross comparing channels monitoring the same variable and those monitoring variables having a known relation to each other.

The applicant has stated that the reactor protection system will be designed, built and tested in accordance with the Proposed IEEE Standard for Nuclear Power Plant Protection Systems (Rev. 9). We have examined the applicant's preliminary design to evaluate the ability to comply with the following sections of the Proposed IEEE Standard:

Single failure criterion	(Section 4.2)
Channel independence and isolation	(Section 4.6)
Control and protection interaction	(Section 4.7)

Periodic on-line testing	(Section 4.10)
Channel bypass	(Section 4.11)
Operating bypasses	(Section 4.12)
Multiple trip settings	(Section 4.15)
Manual actuation	(Section 4.17)

Single Failure Criterion - Section 4.2 requires that no single component failure shall prevent the protection system from fulfilling its protective function when required. Our review of the applicant's proposed design indicates that he can meet the single failure criterion by redundancy of reactor protection channels. The previously tabulated list of reactor trips shows that each parameter listed is monitored by redundant instrumentation channels capable of meeting the single failure criterion. We believe the proposed logic can be designed to meet the single failure criterion. The proposed channel redundancy and the preliminary design of the logic provide adequate assurance that the single failure criterion can be met in the final design.

Channel Independence and Isolation - Section 4.6 requires that redundant protection system channels and their associated elements shall be electrically independent and packaged to provide physical separation. The evaluation of this section is contained above with the description of the channelized approach to the system design and equipment layout.

Control and Protection System Interaction - Section 4.7 of the Proposed IEEE Standard addresses the condition where a plant transient which requires protective action can be brought on by a failure or malfunction of a control system and the same event prevents proper action of a protection system channel or channels designed to protect against the resultant unsafe condition.

Section 4.7 requires that after such a malfunction the remaining portion of the protection system independently meet the single failure criterion. Plant designs in which the protection system and control systems are not interconnected comply with Section 4.7 without further design provisions. The Diablo Canyon design, like others in which control and protection systems are interconnected, requires specific evaluation. The applicant stated that only sensors will be shared by the protection system and control systems. Isolation has been provided to prevent the control systems from interacting with the protection system. Temperature, pressure, and nuclear flux sensors, for example, supply protection system signals and signals to the automatic rod control. The instrumentation channels used to trip the reactor on low steam generator level are also used to control steam generator level.

We believe that the requirements of Section 4.7 can be met where control and protection systems are interconnected by the proposed isolation and the use of greater than minimum redundancy in the protection system. This is the method used in the Diablo Canyon design where four instrumentation channels are used in a 2 of 4 reactor trip logic. An instrument channel failure which might initiate an accident would affect only one protection channel. After such an unsafe failure the protection logic would be 2 of 3, which provides adequate redundancy.

There are three instances where control and protection are interconnected and only minimum redundancy is provided. These are the high pressurizer water level, loss of feedwater flow, and low steam generator level reactor trips. These are evaluated in the two paragraphs below. The two steam generator reactor trips are evaluated together because of their similarity.

(a) Only three channels of pressurizer level instrumentation are proposed,

one of which is used to control level via the charging pumps. These same three channels are used in 2 of 3 logic to trip the reactor on high level. If the high level reactor trip were required for reactor safety, the design would not meet Section 4.7 and would not be acceptable. The applicant, however, stated that the high pressurizer level reactor trip is provided to reduce the probability of operating the safety valves. This reactor trip is not required to protect the reactor. The safety valves have adequate capacity to relieve full charging pump flow. The proposed pressurizer level control and protection is adequate, provided the final design analysis shows that a reactor trip on high pressurizer level is not required to protect the reactor.

(b) The logic of the loss of feedwater flow reactor trip is 1 of 2 steam-feed flow mismatch coincident with 1 of 2 low level for any steam generator. The instruments which supply the trip signals will also be used to control feed flow and steam generator level. The low-low steam generator level reactor trip uses a 2 of 3 logic from any steam generator. One of the three level channels used for the reactor trip can be selected to control the level of the steam generator. The applicant believes that each of these two reactor trips meets Section 4.7 of the IEEE Proposed Standard. His basis is that an instrument channel failure cannot cause the control system to initiate the accident the protection channels are designed to prevent. A comparator which blocks automatic control when the control channel deviates from another channel must be relied upon to prevent accident initiation. We believe that reliance upon a

component in a control system is not a satisfactory means of meeting Section 4.7. We believe that the proposed design of the loss of feedwater flow and the low-low steam generator level reactor trips are acceptable only if they are not required for reactor safety. The applicant stated that these reactor trips are provided to prevent steam generator damage. Low level in one steam generator does not constitute a loss of heat sink. Any malfunction which could cause the loss of level in all steam generators is independent of the flow and level signals used in the protection system. The proposed loss of feedwater flow and low-low steam generator level reactor trips are acceptable provided the final analysis shows that the loss of level in one steam generator does not require a reactor trip to protect the reactor.

Periodic On-Line Testing - A means has been provided to test the protection system while operating at power. Testing of the protection system, with the exception of the sensors, is accomplished in two steps. The first tests the analog channels to the trip bistable outputs and the second tests the logic channels down to and including the main trip breakers. The operational availability of sensors is determined by cross checking between readouts of redundant channels.

Each protection rack will include an analog test panel containing the necessary switches, test jacks and recorders required to test those channels contained within the rack. Each test panel will have a hinged cover which, when opened, will initiate an alarm indicating that that protection rack is under test. This test panel cover design will, (1) preclude closing the

cover unless the test plugs are removed, and (2) mechanically return all test switches, except the bistable trip switches, to operate. The bistable trip switches must be manually reset after test.

The testing of an analog channel consists of (1) placing the output relays in a tripped condition, (2) interrupting the sensor circuit, and (3) substituting a test input for the sensor. The test input will be varied until the bistable trips (as shown by an indicator light). The trip level can be determined from the readout on the control panel or from a plug-in test meter.

The logic channels are tested one at a time using the test panels provided for each logic channel. For illustration, the testing of logic channel no. 1 is described below. Bypass breaker no. 1 is racked in so as to parallel trip breaker no. 1 in order to prevent tripping the reactor during the logic test(Bypass breaker no. 1 is tripped by logic no. 2 if an actual trip signal is received during testing). Trip breaker no. 1 is tripped. Logic no. 1 is tested by simulating each combination of trip inputs by operating test switches which de-energize relays in the logic matrix. An event recorder confirms which combination de-energizes the trip breaker undervoltage coil. At the conclusion of the test the bypass breaker is racked out leaving the normal circuit configuration.

We believe the preliminary design of the test circuits for the protection system meets the IEEE Proposed Standard Section 4.10. We believe that the protection system can be tested adequately at power. The use of local coincidence necessitates a two step test scheme to insure proper operation from sensor to trip breaker. The circuits are necessarily more complex than would be required with general coincidence, but we believe they will permit

adequate testing. The use of the same channelized equipment arrangement for the test circuit as for the protection system should provide assurance that test circuit failures will not cause the loss of protection functions.

Channel Bypass - There are provisions to switch any protection channel to a tripped mode. The coincidence and redundancy to be designed into the system allows a channel to be switched into the trip mode without tripping the reactor or violating the single failure criterion. These features allow any channel to be maintained or tested during power operation without tripping the reactor or violating the single failure criterion. We believe these proposed features are adequate and meet the intent of Section 4.11. An indication of a bypassed channel is provided in the main control room.

Operating Bypasses - Below are listed those trip functions which are automatically or manually bypassed due to operational necessity:

Trip Function	Condition
High nuclear flux low power trip (power range)	Defeated at power
Low pressurizer pressure	Defeated below 10% power
High pressurizer water level	Defeated below 10% power
Turbine trip	Defeated below 10% power
Low reactor coolant flow (two out of three in any one loop)	Defeated below 75% power
Low reactor coolant flow (two out of three in any two loops)	Defeated below 10% power
Reactor coolant pump breaker opening (one out of one in any one loop)	Defeated below 75% power
Reactor coolant pump breaker opening (one out of one in any two loops)	Defeated below 10% power

The above mentioned trip functions which are bypassed are automatically reinstated whenever the permissive conditions are not met. The means

provided to achieve this will be designed to meet the provisions of the IEEE Proposed Standard. We believe the proposed design can meet Section 4.12 and will be adequate. In addition to the above listed operational bypasses, the source range level trip and the intermediate range level trip must be bypassed as the flux level is increased during startup. The operator is prevented from bypassing the source range trip until the flux is in the intermediate range. He is similarly prevented from bypassing the intermediate range trip until the flux is in the power range. We have not reviewed the logic of the circuits which perform this permissive function. There is, however, sufficient redundancy to meet Section 4.12 in these circuits. If the final analysis shows that either the source or intermediate range level trip is required for safety, its bypass circuit will be required to meet Section 4.12 of the IEEE Proposed Standard.

Multiple Trip Settings - The protection system contains fixed trip settings except for the overpower ΔT and overtemperature ΔT channels in which the set point is varied as a function of plant variables. The channelized arrangement of the proposed design should assure that a single failure could not prevent the more restrictive setting from being used if required. We believe that the proposed design will meet Section 4.15 and will be adequate.

Manual Actuation - Manually actuated switch(es) will be provided to initiate protection system action by simultaneously interrupting the d.c. power sources to the undervoltage coils of the trip breakers. The very minimum of equipment is required to initiate a manual trip (a pushbutton and a trip breaker). The applicant has not completed the design to the extent of determining whether one or two switches will be used, however, the final design should satisfy Section 4.17 of the IEEE Proposed Standard.

5.2 Engineered Safety Features

The applicant stated that the circuits which actuate engineered safety features will be designed to the IEEE Proposed Standard. He also stated that the same channelized approach will be used for these circuits as is proposed for the reactor protection system.

Safety injection is initiated when there is indication of low pressurizer level coincident with low pressurizer pressure or when high containment pressure is sensed. Three coincidence trip devices are each fed by a channel of pressurizer level and a channel of pressurizer pressure. A coincidence trip device trips when its level and pressure channels both supply trip signals. The tripping of any one of the three coincidence trip devices will actuate safety injection. An indication of high containment pressure from any two of three instrument channels will initiate safety injection independent of the pressurizer instrumentation. Actuation of safety injection from pressurizer instrumentation and from containment instrumentation will each be designed to meet the single failure criterion. The proposed design which actuates safety injection from either pressurizer or containment instrumentation provides desired diversity. We believe the safety injection actuation circuits are adequate because of the diversity provided and because of compliance with the Proposed IEEE Standard.

Containment isolation is actuated by a coincidence of two of three indications of containment high pressure. The channels of containment pressure instrumentation which actuate containment isolation are not the same channels used to actuate safety injection. Since the applicant is designing this circuit to the Proposed IEEE Standard, we believe it to be acceptable.

The containment spray actuation circuit utilizes the containment pressure

instruments used in both the safety injection circuit and the containment isolation circuit. Containment spray actuation requires tripping of two of three of the channels which actuate safety injection and two of the three channels which actuate containment isolation. The added coincidence makes this circuit somewhat more prone to failure than either the safety injection or containment isolation circuit. The circuit can, however, be designed to meet the single failure criterion. We believe that this circuit, which will be designed to the Proposed IEEE Standard, is satisfactory.

We have had discussions with the applicant concerning the ability of the engineered safety feature electrical equipment to perform its function in an accident environment. We believe that, before plant operation, data should be available to prove the capability of this equipment to function in the combined temperature, pressure, humidity environment associated with the design basis accident. This equipment includes cables, motors, detectors, and valve operators located inside the containment which are associated with the engineered safety features. The applicant has agreed to have data available to prove the operability of the engineered safety feature equipment. Where appropriate data exists, it will be made available. Where such data does not now exist, the required environment tests will be performed. Where the equipment tested is not identical to the installed equipment, the extrapolation will be justified.

.3 Instrumentation

.1 Nuclear Instrumentation

A major change in the proposed nuclear instrumentation design is the complete absence of period or startup rate information. This is the first power reactor we know of to be designed with no period or startup rate

should agree with the individual (actual) position indication unless a malfunction causes the rod drive not to respond to the pulses.

The display provided for the operator consists of a readout for each group position and a single indicator with a selector switch for reading out the actual position of any selected rod. Based upon discussion with the applicant a deviation alarm circuit is also included which compares each individual rod position indication with its group indication. An alarm is actuated at any time an individual indication deviates from its group's position by more than a preset amount. By using the selector switch and individual indicator, the operator can determine which rod is out of position. We believe that the rod position indication is adequate since two malfunctions are required for a rod to be in a position other than its indicated position without the operator's knowledge. The two failures are the incorrect movement of the rod and failure of the individual rod position indication. A failure in either an individual indication circuit or a group indicator would be detected by the deviation alarm circuit.