TVA

Tennessee Valley Authority, Post Office Box 2000, Spring City, Tennessee 37381

NOV 05 1992

William J. Museler
Site Vice President
Watts Bar Nuclear Plant

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

Gentlemen:

In the Matter of the Application of	)	Docket Nos. 50-390
Tennessee Valley Authority	)	50-391

WATTS BAR NUCLEAR PLANT (WBN) UNIT 1 - PROPOSED CHANGES TO FINAL SAFETY ANALYSIS REPORT (FSAR) FOR INSTALLATION OF WESTINGHOUSE EAGLE-21 PROCESS PROTECTION SYSTEM (TAC 81063)

In a letter dated July 10, 1991, TVA provided notification of its plan to install Westinghouse Electric Corporation's new Eagle-21 process protection system at WBN Unit 1 in place of the older Foxboro process control system. This design modification represents a fundamental advance in electronics technology since the Eagle-21 system incorporates digital electronics and microprocessors to accomplish the same reactor protection and control functions as the Foxboro system, which used analog electronics. Also, as part of the Eagle-21 modification, several reactor protection features are being revised to simplify operational control of the plant and to reduce the potential for initiation of unnecessary protective actions.

Enclosed with this letter for NRC staff review are proposed FSAR changes associated with installing the Eagle-21 system. The changes are indicated as markups of the effected pages of Chapters 1, 3, 4, 5, 6, 7, 8, 10, and 15. TVA plans to incorporate these changes formally in a future FSAR amendment.

In addition to the enclosed licensing information, TVA has already provided a technical description of WBN's Eagle-21 system in a letter dated February 26, 1992. This letter enclosed Westinghouse Topical Report WCAP-12374 ("Eagle-21 Microprocessor-Based Process Protection System"), Revision 1, and stated that WCAP-12417 ("Median Signal Selector for Foxboro Series Process Instrumentation - Application to Deletion of Low Feedwater Flow Reactor Trip") also applied to WBN.

A001

NOV 05 1992

Note that some of the accident analysis markups in Chapter 15 reflect changes that are related to both the installation of the Eagle-21 system and also the recent recaging modification to WBN's reactor fuel assemblies. For expediency, both of these design changes were addressed in revised accident analyses at the same time. Detailed information on fuel assembly recaging, which modified the structural skeletons of WBN's existing fuel assemblies to incorporate the improved mechanical features of Westinghouse's VANTAGE 5H fuel design, has already been submitted in separate correspondence. The proposed FSAR changes for the VANTAGE 5H fuel assembly recaging modification were enclosed with a letter dated August 24, 1992. In some places, the proposed FSAR changes in the August 24 letter duplicate the proposed FSAR changes in the enclosure attached to this letter.

Also note that the description of WBN's anticipated-transient-without-scram mitigation system actuation circuitry (AMSAC) in Section 7.7.1.12 may need to be further revised in a future FSAR amendment. TVA is currently evaluating the operational effects on AMSAC of the new steam generator low-low level reactor trip setpoint and trip time delay that are part of the Eagle-21 upgrade. Corresponding changes to AMSAC setpoints may be required. However, the AMSAC system is not connected to, nor functionally associated with the Eagle-21 system. AMSAC is only a diverse backup to the reactor trip system per 10 CFR 50.62, and no credit is taken for AMSAC in WBN's safety analyses. Therefore, TVA considers that NRC staff review of the Eagle-21 system can proceed without waiting for the details of any AMSAC changes that may result.

If you have any questions, please telephone John Vorees at (615) 365-8819.

Very truly yours,

W. J. Museler

William J. Museler

Enclosure
cc: See page 3

NOV 05 1992

cc (Enclosure):

NRC Resident Inspector
Watts Bar Nuclear Plant
P.O. Box 700
Spring City, Tennessee 37381

Mr. P. S. Tam, Senior Project Manager
U.S. Nuclear Regulatory Commission
One White Flint, North
11555 Rockville Pike
Rockville, Maryland 20852

Mr. B. A. Wilson, Project Chief
U.S. Nuclear Regulatory Commission
Region II
101 Marietta Street, NW, Suite 2900
Atlanta, Georgia 30323

cc (Enclosure):
NRC Resident Inspector
Watts Bar Nuclear Plant
P.O. Box 700
Spring City, Tennessee 37381

Mr. P. S. Tam, Senior Project Manager
U.S. Nuclear Regulatory Commission
One White Flint, North
11555 Rockville Pike
Rockville, Maryland 20852

Mr. B. A. Wilson, Project Chief
U.S. Nuclear Regulatory Commission
Region II
101 Marietta Street, NW, Suite 2900
Atlanta, Georgia 30323

GLP:JV:NCH:CR
cc (w/o Enclosure, except as noted):
M. J. Burzynski, LP 5B-C
S. O. Casteel, FSB 2K-WBN
E. S. Christenbury, ET 11H-K
J. D. Christensen, TSB 1E-WBN
W. R. Cobean, Jr., LP 3B-C
L. M. Cuoco, LP 5B-C
W. L. Elliott, IOB 1A-WBN
M. J. Fecht, LP 5B-C
R. W. Huston, Rockville Licensing Office
R. W. Johnson, FSB 2J-WBN
N. C. Kazanas, FSB 1B-WBN
D. L. Koehl, MOB 2N-WBN
T. J. McGrath, LP 3B-C
R. M. McSwain, MR 2C-C
K. A. Meyer, Trailer E23-WBN
D. E. Moody, MOB 2R-WBN
G. R. Mullee, BR 5D-C
D. E. Nunn, LP 3B-C
H. H. Weber, FSB 1B-WBN
RIMS, QAC 1G-WBN (Enclosure)

S:\SFS\SUBMIT\E21FSAR.NCH

50-390 WATTS BAR 1 TVA

PROPOSED CHANGES TO FSAR CHAPTERS 1, 3, 4, 5, 6, 7, 8, 10, and 15

REC'D W/LTR DTD 11/5/92...9211160059

ENCLOSURE

(Proposed Changes to FSAR Chapters 1, 3, 4, 5, 6, 7, 8, 10, and 15)

1.2.2.3 Control and Instrumentation

0794 PKG

The reactor is controlled by temperature coefficients of reactivity, control rod clusters, and a soluble neutron absorber, boron, in the form of boric acid.

Instrumentation and controls are provided to monitor and maintain essential reactor facility operating variables such as neutron flux, primary coolant pressure, temperature, and control rod positions within prescribed ranges.

The non-neutronic process and containment instrumentation measures temperatures, pressure, flows, and levels in the Reactor Coolant System, steam systems, containment, and auxiliary systems. Process variables which are required on a continuous basis for the startup, power operation, and shutdown of the plant are monitored in a controlled access area. The quantity and types of process instrumentation provided are adequate for safe and orderly operation of all systems and processes over the full operating range of the plant.

Reactor protection is achieved by defining a region of power and coolant temperature conditions allowed by the principal tripping functions: the overpower ΔT trip, the overtemperature ΔT trip, and the nuclear overpower trip. The allowable operating region within these trip settings is designed to prevent any combination of power, temperatures, and pressure which would result in a Departure from Nucleate Boiling Ratio (DNBR) < 1.3. Additional tripping functions such as a high-pressurizer pressure trip, low-pressurizer pressure trip, high-pressurizer water-level trip, low reactor ~~loss of~~ coolant flow trip, ~~steam and feedwater flow mismatch trip~~, steam generator low-low water-level trip, turbine trip, safety injection trip, nuclear source and intermediate range trips, neutron flux rate trips, and manual trip are provided to support the principal tripping functions for specific accident conditions and mechanical failures. Independent and redundant channels are combined in logic circuits which improve tripping reliability and minimize trips from spurious causes. Protection interlocks, initiation signals to the Safety Injection System, containment isolation signals, and turbine runback signals further assist in plant protection during operation.

The Control System enables the nuclear plant to accept a step-load increase of 10% and a ramp increase of 5% per minute within the load range of 15% to 100% of nominal power. The Control System will also take a 50% load reduction with steam bypass without tripping the reactor.

reactor coolant pump undervoltage and underfrequency trips

TABLE 1.3-1
DESIGN COMPARISON (EXCLUDING SECONDARY CYCLE)
Nuclear Plant Units 1 and 2 - Comparison with Donald C. Cook, Trojan, and Sequoyah

CHAPTER NUMBER	CHAPTER TITLE SYSTEM/COMPONENT	REFERENCES (FSAR)	SIGNIFICANT SIMILARITIES	SIGNIFICANT DIFFERENCES
5.0 (Cont'd)				
	Residual Heat Removal System	Section 5.5.7	D. C. Cook, Sequoyah, Trojan	None.
	Pressurizer*	Section 5.5.10	D. C. Cook Sequoyah, Trojan	None.
6.0	Engineered Safety Features			
	Emergency Core Cooling System	Section 6.3	D. C. Cook, Sequoyah Trojan	None.
	Ice Condenser	Section 6.7	D. C. Cook, Sequoyah	Trojan does not use an ice condenser.
7.0	Instrumentation and Controls			
	Reactor Trip System	Section 7.2	System functions are similar to D. C. Cook Sequoyah, Trojan	~~None.~~ Insert A
	Engineered Safety Features Systems	Section 7.3	System functions are similar to D. C. Cook, Sequoyah, Trojan	None.
	Systems Required For Safe Shutdown	Section 7.4	System functions are similar to that of of D. C. Cook, Trojan Sequoyah	None.
	Safety Related Display Instrumentation	Section 7.5	Parametric display is similar to that of D. C. Cook, Trojan, Sequoyah	Actual physical configuration may differ due to customer design philosophy.
	Other Safety Systems	Section 7.6	Operational Functions are similar to D. C. Cook, Trojan, Sequoyah	None.
	Control Systems	Section 7.7	Operational functions are similar to D. C. Cook, Trojan, Sequoyah	The Sequoyah Nuclear Plant has a 50 percent load rejection capability while that of the D. C Cook Plant is 100 percent. The rod position indication for the Sequoyah Nuclear Plant and the D. C. Cook Plant is an analog system; Trojan's RPI is a digital system.

163

0794 PKG

Insert A to Table 1.3-1, Sheet 2

Sequoyah and Watts Bar have a Westinghouse EAGLE 21 digital Process Protection System; Trojan and D. C. Cook use an analog system. Sequoyah's low-low steam generator level trip function is processed through an environmental allowance modifier/trip time delay (EAM/TTD) functional algorithm in the EAGLE 21 system. This allows a lower low-low level setpoint when an adverse containment environment does not exist as determined by monitoring containment pressure. Watts Bar uses the TTD without EAM.

TABLE 1.3-3 (Continued)

System	Reference Section	Changes
Post Accident Monitoring	7.0	A Post Accident Monitoring System has been added.
Source Range Monitor	7.0	An additional source range monitoring system was added for backup control.
Process Protection System	7.0	The Foxboro analog instrumentation in the Process Protection System racks has been replaced with Westinghouse EAGLE 21 digital system. Concurrently, some functional changes were made which improve plant availability and reliability.

0794 PKG

initiates a reactor trip when any appropriate monitored variable or combination of variables exceed the normal operating range. Setpoints are chosen to provide an envelope of safe operating conditions with adequate margin for uncertainties to ensure that fuel design limits are not exceeded.

Reactor trip is initiated by removing power to the rod drive mechanisms of all the full length rod cluster control assemblies. This will allow the assemblies to free fall into the core, rapidly reducing the reactor power output.

The Engineered Safety Features Actuation System automatically initiates emergency core cooling, and other safeguards functions, by sensing accident conditions using redundant ~~analog~~ channels measuring diverse parameters. Manual actuation of safeguards is relied upon where ample time is available for operator action. The ESF Actuation System also provides a reactor trip on manual or automatic safety injection (S) signal generation.

process protection system

The response and adequacy of the protection systems is analyzed for all conditions specified by the ANS N18.2 standard, through Condition IV.

Criterion 21 - Protection System Reliability and Testability.

The Protection System shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the Protection System shall be sufficient to assure that (1) no single failure results in loss of protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the Protection System can be otherwise demonstrated. The Protection System shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Compliance

The Protection System is designed for high functional reliability and inservice testability. The design employs redundant logic trains, and measurement and equipment diversity.

The Protection System is designed in accordance with IEEE Standard 279-1971. All safety actuation circuitry is provided with process protection system, nuclear instrumentation system and the

a capability for testing with the reactor at power. The Protection Systems, including the engineered safety features test cabinet comply with Regulatory Guide 1.22 on periodic testing of Protection System actuation functions. Under the present design, there are protective functions which are not tested at power. The functions can be tested under shutdown plant conditions, so that they do not interrupt power operation, as allowed by Regulatory Guide 1.22. Insert 38

In those cases where equipment cannot be tested at power, it is only the actuation device function which is not tested. The logic associated with the actuation devices has the capability for testing at power. Such testing will disclose failures or reduction in redundancy which may have occurred. Removal from service of any single channel or component does not result in loss of minimum required redundancy. For example, a two-of-three function becomes a one-of-two function when one channel is removed. (Note that this is not true for the logic trains which are effectively a one-out-of-two logic).

Semiautomatic testers are built into each of the two logic trains in a protection system. These testers have the capability of testing the major part of the protection system very rapidly while the reactor is at power. Between tests, a number of internal protection system points including the associated power supplies and fuses are continuously monitored. Outputs of the monitors are logically processed to provide alarms for failures in one train and automatic reactor trip for failures in both trains. Self-testing provision is designed into each tester. Additional details can be found in Sections 7.2 and 7.3.

<u>Criterion 22</u> - Protection System Independence

The Protection System shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

<u>Compliance</u>

Design of Protection Systems includes consideration of natural phenomena, normal maintenance, testing and accident conditions such that the protection functions are always available.

Insert 38 to Page 3.1-16

For those process protection functions that may be tested in bypass, alarms are provided in the control room and at the process rack to indicate the bypassed condition. Additional information on the capability of the process protection system to be tested in the bypassed mode is provided in Section 7.2.2.1.3, Subsections 10, 11, 12, 13 and 14.

System in that control signals are derived from Protection System measurements where applicable. These signals are transferred to the Control System by isolation ~~amplifiers~~ devices which are classified as protection components. The adequacy of system isolation has been verified by testing under conditions of postulated credible faults. The failure or removal of any single control system component or channel, or failure or removal from service of any single Protection System component or channel which is common to the Control and Protection System leaves intact a system which satisfies the requirements of the Protection System. Distinction between channel and train is made in this discussion. The removal of a train from service is allowed only during testing of the train.

Criterion 25 - Protection System Requirements for Reactivity Control Malfunctions.

The protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal (not ejection or dropout) of control rods.

Discussion:

The Protection System is designed to limit reactivity transients so that fuel design limits are not exceeded. Reactor shutdown by full length rod insertion is completely independent of the normal control function since the trip breakers interrupt power to the rod mechanisms regardless of existing control signals. Thus in the postulated accidental withdrawal, (assumed to be initiated by a control malfunction) flux, temperature, pressure, level and flow signals would independently be generated. Any of these signals (trip demands) would operate the breakers to trip the reactor.

Analyses of the effects of possible malfunctions are discussed in Chapter 15. These analyses show that for postulated dilution during refueling, startup, or manual or automatic operation at power, the operator has ample time to determine the cause of dilution, terminate the source of dilution and initiate reboration before the shutdown margin is lost. The analyses show that acceptable fuel damage limits are not exceeded even in the event of a single malfunction of either system.

TABLE 3.2-2

SUMMARY OF CRITERIA - MECHANICAL SYSTEM COMPONENTS

Compartment	Scope (1)	Safety Class (2)	Code (3)	QA Required (4)	Location (5)	Rad Source (6)	Seismic (7)
Reactor Vessel	W	A	13	X	C	X	I
Full Length CRDM Housing	W	A	III-1	X	C	X	I
CRDM Head Adapter Plugs	W	A	III-1	X	C	X	I
Steam Generators (Tube Side)	W	A	III-1	X	C	X	I
(Shell Side)	W	A(17)	III-1	X	C	X	I
Pressurizer	W	A	III-1	X	C	X	I
Reactor Coolant Pipe	W	A	III-1	X	C	X	I
Reactor Coolant Fittings	W	A	III-1	X	C	X	I
Reactor Coolant Fabricated Piping	W	A	III-1	X	C	X	I
Reactor Coolant Crossover Legs	W	A	III-1	X	C	X	I
~~RTD Bypass manifold~~	~~W~~	~~A~~	~~III-1~~	~~X~~	~~C~~	~~X~~	~~I~~
Reactor Coolant Thermowell	W	A	III-1	X	C	X	I
Thimble Guide Tubing	W	A	III-1	X	C	X	I
Thimble Guide Couplings	W	A	III-1	X	C	X	I
Flux Thimble Assembly	W	B	III-2	X	C	X	I
Loop Bypass Line	W	A	III-1	X	C	X	I
Pressurizer Safety Valves	W	A	III-1	X	C	X	I
Power Operated Relief Valves	W	A	III-1	X	C	X	I
Pressurizer Relief Tank	W	G	VIII	X	C	P	I(L)

164

DELETE

0794 PKG

0794 PKG 2

Instrumentation

The seismic type testing performed by the NSSS supplier (Westinghouse) is described in References [1] through [10], and [21]. For References [1] through [10], the ~~The~~ test method used was the sine beat procedure described in IEEE Standard 344-1971 and Reference [11]. In addition, as noted in Section 3.10.1, Westinghouse conducted a "Demonstration Test Program" which, when considered in conjunction with the tests presented in References [11] through [13], results in meeting the requirements of IEEE-344-1975.

Supporting Structures (Panels, Racks, Cabinets, and Boards)

The qualification of the supporting structures for Seismic Category I instruments has been accomplished by either analysis or testing. The method commonly used is testing under simulated conditions. All tests by TVA before September 1, 1974 on these supporting structures were similar. The support structure was mounted on a vibration generator in a manner that simulated the intended service mounting. The vibratory forces were applied to each of the three major perpendicular axes independently. Maximum service dead loads were simulated. Selected points were monitored to establish amplification of loads. Testing was done at the structure's resonant frequencies. The resonant frequencies were determined by an exploratory test using a sinusoidal steady-state input of low amplitude, (two continuous sweeps from 1 to 33 Hz at a rate of 1 octave per minute). The qualification test was conducted using the sine beat method at the resonant frequencies using the appropriate acceleration input as determined from the building response acceleration spectra. 64

Later qualification tests typically used multifrequency time history input motion for which the test response spectra enveloped the required response spectra in accordance with IEEE 344-1975 guidelines. 64

3.10.3 Methods of Qualifying TVA-Designed Supports for Electrical Equipment Instrumentation and Cables

The methods and procedures of design and analysis or testing of electrical equipment and instrumentation supports, cable trays, cable tray supports, conduit, conduit supports, and conduit banks are provided in the following sections.

3.10.3.1 Electrical Equipment and Instrumentation Assemblies 64

TVA-designed supports and anchorage for Category I electrical equipment assemblies ensure compatibility with the equipment seismic qualifications test or analysis as described in Section 3.7.3.16.1. Design of these supports is in accordance with Section 3.9.3.4.2.

All floor/wall mounted Category I electric equipment assemblies such as battery racks, instrument racks, and control consoles are attached by TVA to the building structure. The attachments are made by bolting or welding to structural members. Anchorages to concrete are made by welding to embedded plates cast in the concrete with stud anchors, or by bolting to anchors set in the hardened concrete (self-drilling bolts, wedge bolts, undercut expansion anchors, or grouted anchors). 64

1. Foxboro Model E-11 pressure transmitter and Model E-13 differential pressure transmitter.

2. Foxboro Process Control Equipment cabinets.

3. Westinghouse Solid-State Protection System cabinets.

4. Nuclear Instrumentation System cabinets.

5. Safeguards Test Racks.

6. Resistance Temperature Detectors.

7. Power range Neutron Detectors.

8. Reactor trip breakers.

9. Barton Models 332 and 386 differential pressure transmitters.

10. Eagle-21 Process Protection System

Seismic qualification testing of ~~this equipment~~ items [1] through [9] is documented in references [1] through [10]. Reference [10] presents the theory and practice, as well as justification, for the use of single axis sine beat test inputs used in the seismic qualification of electrical equipment. In addition, it is noted that Westinghouse has conducted a seismic qualification "Demonstration Test Program" (Reference Letter NS-CE-692, C. Eicheldinger (W), to D. B. Vassallo (NRC), 7/10/75) to confirm equipment operability during a seismic event. This program is documented in references [12] through [15] (Proprietary) and references [16] through [20] (Non-Proprietary). 31.

The Watts Bar Nuclear Plant complies with paragraph IV, "Conclusions and Regulatory Positions" of the "Mechanical Engineering Branch Report on Seismic Audit of Westinghouse Electrical Equipment." All topical reports have been completed and are included in the reference list. The non-proprietary topical reports have been referenced as a group above. The structural capability of the NIS rack is discussed in references [14] and [19].

The Watts Bar Nuclear Plant does not use the Eagle Signal Timer that is under question by the NRC Staff.

This demonstration test program in conjunction with the justification for the use of single axis sine beat tests, presented in WCAP-8373, and the original tests, documented in references [2] through [10], meet the requirements of IEEE Standard 344-1975 "IEEE Recommended Practices for Seismic Qualification

Seismic qualification testing of item [10] to IEEE 344-1975 is documented in reference [21].

17. Jareck, S. J., "General Method of Developing Multifrequency Biaxial Test Inputs for Bistables," WCAP-8695 (Non-Proprietary) September, 1975.

18. Jareck, S. J. and Vogeding, E. L., "Multifrequency and Direction Seismic Testing of Relays," WCAP-8674 (Non-Proprietary) December, 1975.

19. Jareck, S. J., Coslow, B. J., Croasdaile, T. R., and Lipchak, J. B., "Seismic Operability Demonstration Testing of the Nuclear Instrumentation System Bistable Amplifier," WCAP-8831 (Non-Proprietary) October, 1976. 33

20. Jareck, S. J., Coslow, B. J., Ellis, A. E., and Miller, R. B., "Seismic Operability Demonstration Testing of the Foxboro H-Line Series Process Instrumentation System Bistables," WCAP-8849 (Non-Proprietary) November, 1976.

ADD: 21. WCAP-8687, Supplement 2-E69A, "Equipment Qualification Test Report, Eagle 21 Process Protection System," (Proprietary) May, 1988.

22. WCAP-8687, Supplement 2-E69B, "Equipment Qualification Test Report, Eagle 21 Process Protection System Components" (Proprietary), February 1990.

23. WCAP-8687, Supplement 2-E69C, "Equipment Qualification Test Report, Eagle 21 Process Protection System Components" (Proprietary), February 1991

4

0794 PKG

TABLE 3.10-2

QUALIFICATION OF INSTRUMENTATION AND CONTROL EQUIPMENT

Equipment	Qualification Method*	Standard to Which Qualified*	Organization Performance Testing/Analysis and Date of Completion
Reactor Trip and Bypass Breakers	1 & 3 testing		Westinghouse
Solid State Protection System	1 & 2 testing		Westinghouse
Eagle-21 Process Protection ~~Instrument~~ System	3 ~~1 & 2~~ testing		Westinghouse
Nuclear Instrument System	1 & 2 testing		Westinghouse
Neutron Detectors	1 testing		Westinghouse
Process Transmitters	1 & 2 testing		Westinghouse
Containment Pressure Transmitters			
Solid State Protection System Output Relays	1 & 2 testing		Westinghouse
Engineered Safeguards Test Cabinets	1 testing		Westinghouse
Control Room Panels	1 & 4 testing and analysis		Westinghouse
Safety System Status Monitoring System			
Post Accident Monitoring System	1 & 2 testing		Westinghouse
Post Accident Monitoring Recorders	2 & 5 Testing		Westinghouse 45

Revised by Amendment 45

0794 PKG

4.2.3.5 Instrumentation Applications

Instrumentation for determining reactor coolant average temperature (T_{avg}) is provided to create demand signals for moving groups of full length rod cluster control assemblies to provide load follow (determined as a function of turbine impulse pressure) during normal operation and to counteract operational transients. The hot and cold leg resistance temperature detectors (RTD's) are described in Section 7.2. ~~in the reactor coolant bypass loops.~~ The location of the RTD's in each loop is shown on the flow diagrams in Chapter 5. The Reactor Control System which controls the reactor coolant average temperature by regulation of control rod bank position is described in Section 7.3.

Rod position indication instrumentation is provided to sense the actual position of each control rod ~~(full length as well as part length)~~ so that the actual position of the individual rod may be displayed to the operator. Signals are also supplied by this system as input to the rod deviation comparator. The rod position indication system is described in Chapter 7.

The reactor makeup control system whose functions are to permit adjustment of the reactor coolant boron concentration for reactivity control (as well to maintain the desired operating fluid inventory in the volume control tank), consists of a group of instruments arranged to provide a manually preselected makeup composition that is borated or diluted as required to the charging pump suction header or the volume control tank. This system, as well as other systems including boron sampling provisions that are part of the Chemical and Volume Control System, are described in Section 9.3.

When the reactor is critical, the normal indication of reactivity status in the core is the position of the control bank in relation to reactor power (as indicated by the Reactor Coolant System loop ΔT) and coolant average temperature. These parameters are used to calculate insertion limits for the control banks to give warning to the operator of excessive rod insertion. Monitoring of the neutron flux for various phases of reactor power operation as well as of core loading, shutdown, startup, and refueling is by means of the Nuclear Instrumentation System. The monitoring functions and readout and indication characteristics for the following means of monitoring reactivity are included in the discussion on safety related display instrumentation in Section 7.5:

1. Nuclear Instrumentation System

2. Temperature Indicators

    a. T average (Measured)
    b. ΔT (Measured)
    c. Auctioneered T average
    d. T reference

relief valves are designed to limit the pressurizer pressure to a value below the high pressure trip setpoint for all design transients up to and including the design percentage step load decrease with steam dump but without reactor trip.

Isolated output signals from the pressurizer pressure protection channels are used for pressure control. These are used to control pressurizer spray and heaters and power-operated relief valves. Pressurizer pressure is sensed by fast response pressure transmitters with a time response of better than 0.2 seconds.

In the event of a complete loss of heat sink, e.g., no steam flow to the turbine, protection of the RCS against overpressure is afforded by pressurizer and steam generator safety valves along with any of the following reactor trip functions:

1. Reactor trip on turbine trip (if the turbine is tripped)
2. High pressurizer pressure reactor trip
3. Overtemperature ΔT reactor trip
~~4. Low feedwater flow reactor trip or~~
4 ~~5.~~ Low-low steam generator water level reactor trip

The ASME Code pressure limit is 110 percent of the 2485 psig design pressure. This limit is not exceeded as discussed in reference [4]. The report describes in detail the pressure relief devices, location, reliability, and sizing. Transient analysis data is provided for the worst cases that require safety valve actuation as well as those cases which do not.

A detailed functional description of the process equipment associated with the high pressure trip is provided in reference [5].

The upper limit of overpressure protection is based upon the positive surge of the reactor coolant produced as a result of turbine trip under full load, i.e. a 100 percent load mismatch assuming that the core continues to produce full power. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and a total accumulation of 3 percent. The actual installed capacity of the safety valves is always greater than the capacity calculated from the sizing analysis and is indicated so by the ratio of safety valve flow to peak surge rate being greater than 1.0. Note that no credit is taken for the relief capability provided by the power operated relief valves during this surge.

The RCS design and operating pressure together with the safety, power relief and pressurizer spray valve setpoints and the protection system setpoint pressures are listed in Table 5.2-7.

3. If all reactor coolant pumps have stopped for more than 5 minutes during plant heatup, and the reactor coolant temperature is greater than the charging and seal injection water temperature, do not attempt to restart a pump unless a steam bubble is formed in the pressurizer. This precaution will minimize the pressure transient when the pump is started and the cold water previously injected by the charging pumps is circulated through the warmer reactor coolant components. The steam bubble will accommodate the resultant expansion as the cold water is rapidly warmed.

4. If all reactor coolant pumps are stopped and the reactor coolant system is being cooled down by the residual heat exchangers, a non-uniform temperature distribution may occur in the reactor coolant loops. Do not attempt to restart a reactor coolant pump unless a steam bubble is formed in the pressurizer.

5. During plant cooldown, all steam generators should be connected to the steam header to assure a uniform cooldown of the reactor coolant loops.

6. At least one reactor coolant pump must remain in service until the reactor coolant temperature is reduced to 160°F. 163

These special precautions backup the normal operational mode of maximizing periods of steam bubble operation so that cold overpressure transient prevention or reduction is continued during periods of transitional operations.

The specific plant configurations of ECCS testing and alignment will also require procedures to prevent developing cold overpressurization transients. During these limited periods of plant operation, the following procedures will be followed:

1. To preclude inadvertent ECCS actuation during heatup and cooldown, procedures will require blocking the low pressurizer pressure, ~~high steamline differential pressure, and high steam line flow coincident~~ and ~~with~~ low steamline pressure ~~or low-low Tavg~~ safety injection signal actuation logic ~~at 1900 psig.~~ below Permissive P-11 (reference Table 7.3-3). 163

2. During further cooldown, closure and power lockout of the accumulator isolation valves and power lockout of the nonoperating charging pumps will be performed at 1000 psig, 425°F RCS conditions, RCS pressure, providing additional backup to step 1 above.

0794 Fr. G

Section 6.2.4 of this FSAR describes hot penetrations. The design of the guard pipe portion of hot penetrations is such that any process pipe leakage in the annulus is returned to the containment. All process piping which has potential for annulus pressurization upon rupture is routed through hot penetrations.

Inadvertent air return fan operation during normal operation opens the ice condenser lower inlet doors, which in turn, results in sounding an alarm in the MCR. Even with a hypothetical situation in which the operator cannot shut off the air return fan, the operator has the capability of opening an eight inch vacuum relief line (Penetration x-80, Section 6.2.4) to relieve the net external design pressure.

The logic and control circuits of the containment spray system are such that inadvertent containment spray would not take place with a single failure. The spray pump must start and the isolation valve must open before there can be any spray. In addition, the Watts Bar containment is so designed that even if an inadvertent spray occurs, containment integrity is preserved without the use of a vacuum relief.

The containment spray system is automatically actuated by a hi-hi containment pressure signal from the ~~sold~~ solid state protection system (SSPS). To prevent inadvertent automatic actuation, four ~~bistable inputs~~ comparator outputs, one from each protection set are processed through two coincidence gates. Both coincidence gates are required to have at least two high inputs before the output relays, which actuate the containment spray system, are energized. Separate output relays are provided for the pump start logic and discharge valve open logic. Additional protection is provided by an interlock between the pump and discharge valve, which requires the pump to be running before the discharge valve will automatically open.

FSAR Section 3.8 describes the structural design of the containment vessel. The containment vessel is designed to withstand a net external pressure of 2.0 psi. The containment vessel is designed to withstand the maximum expected net external pressure in accordance with ASME Boiler and Pressure and Vessel Code Section III, paragraph NE-7116.

6.2.1.2 Primary Containment System Design

The Containment consists of a Containment Vessel and a separate Reactor Building enclosing an annulus. The Containment Vessel is a freestanding, welded steel structure with a vertical cylinder, hemispherical dome, and a flat circular base. The Reactor Building is a reinforced concrete structure similar in shape to the Containment Vessel. The design of these structures is described in Section 3.8.

The design internal pressure for the containment is 13.5 psig, and the design temperature is 250°F. The design basis leakage rate

6.2.1.3.10 Steamline Break Inside Containment

Pipe Break Blowdowns - Spectra and Assumptions

A series of steam line breaks were analyzed to determine the most severe break condition for containment temperature and pressure response. The following assumptions were used in these analysis:

1. The following break types were evaluated:

   a. Double-ended ruptures[1] occurring at the nozzle on one steam generator.

   b. The largest split break which will not generate the low steamline ~~coincident/high-steam flow/low-steam~~ pressure signal for steamline isolation.

   c. Small split breaks of 0.6, 0.35, and 0.1 square feet.

2. Steam line isolation signals and feedwater line isolation signals are generated by either a low steamline ~~high-steam flow/low-steam~~ pressure signal or high-high containment pressure signal. ~~trips.~~ An allowance of 7 seconds is used for steam line isolation including generation, processing, and delay of the isolation signal and valve closure. An allowance of 8 seconds is used for feedwater line isolation including generation, processing, and delay of the isolation signal and valve closure.

3. Failure of a diesel generator is assumed in all cases. This results in the loss of one containment safeguards train resulting in minimum heat removal capability.

---

[1]Steam line flow restrictions in the stream generators limit the effective break area of full double - ended pipe rupture to a maximum of 1.4 square feet per steam generator.

0794 PKG 5

Containment isolation can be initiated by either of two signals, phase A and phase B.

Phase A signal is generated by either of the following:

1. Manual - Either of two momentary controls

2. Safety injection signal, generated by one or more of the following :

    a. Low steamline pressure in any steamline. ~~High main steam flow coincident with low steam line pressure or low-low primary coolant average temperature in two of four loops.~~

    ~~b. High differential pressure between any one main steam line and two of the other three lines.~~

    b ~~c.~~ Low pressurizer pressure.

    c ~~d.~~ ~~Two out of three~~ High containment pressure ~~signals~~.

    d ~~e.~~ Manual - Either of two momentary controls.

Phase B signal Is generated by either of the following:

1. Manual - Two sets (two switches per set) - actuation of both switches is necessary in either set for spray initiation.

2. ~~Two out of four~~ High-high containment pressure ~~signals~~.

Containment isolation phase A always exists if containment isolation phase B exists, when the phase B signal is initiated by automatic instrumentation. Phase A containment isolation does not occur when the phase B signal is initiated manually. The instrumentation circuits that generate both phase A and phase B signals are described in Chapter 7.

The Containment Isolation System provides for automatic, fast, and efficient closure of those valves required to close for containment integrity following a design basis event to minimize the release of any radioactive material. Closure times for isolation valves are included in Table 6.2.4-1.

6.2.4.2.1 Design Requirements

Containment isolation barrier design includes the following requirements:

1. As a minimum, containment barriers are designed to ASME Section III Class 2 requirements. This design meets the requirements of Regulatory Guide 1.26 for the Containment

0794 PKG 6

The cold leg injection accumulators can be isolated from the RCS by closure of their motor-operated isolation valves. Since these accumulators operate only after considerable RCS pressure loss, the injection of pressurized nitrogen via the cold legs is not considered a problem.

Injection Mode After Loss of Primary Coolant

The injection mode of emergency core cooling is initiated by the safety injection signal ("SI" signal). This signal is actuated by any of the following:

1. Low pressurizer pressure

2. High containment pressure

3. Low steamline pressure in any steamline. ~~High differential pressure between any two steam generators~~

~~4. High steam flow coincident with low T_{avg} or low steam pressure~~

4 ~~5.~~ Manual actuation

Operation of the ECCS during the injection mode is completely automatic. Refer to Figure 7.3-3 (Sheet 3) for complete safety injection logic and control diagrams. The safety injection signal in addition to activating the ESF equipment automatically initiates the following actions:

0794 PKG

6.3.5 Instrumentation Application

Instrumentation and associated ~~analog~~ process protection and logic channels employed for initiation of Emergency Core Cooling System operation is discussed in Section 7.3. This section describes the instrumentation employed for monitoring Emergency Core Cooling System components during normal plant operation and also Emergency Core Cooling System post accident operation. All alarms are annunciated in the control room.

6.3.5.1 Temperature Indication 52

Residual Heat Exchanger Inlet Temperature

The fluid temperature at the inlet and outlet of each residual heat exchanger is recorded in the control room.

Refueling Water Storage Tank (RWST) Temperature

Two temperature channels are provided to monitor the RWST temperature. Both are indicated in the Main Control Room. 52

6.3.5.2 Pressure Indication

Boron Injection Tank Pressure

Boron injection tank pressure is indicated in the control room. A high pressure alarm is provided.

Safety Injection Header Pressure

Safety injection pump discharge header pressure is indicated in the control room.

Cold Leg Accumulator Pressure

Duplicate pressure channels are installed on each cold leg

0794 PKG

6.5.3 Fission Product Control Systems

6.5.3.1 Primary Containment

The primary containment is designed to assure that an acceptable upper limit leakage of radioactive material is not exceeded under design basis accident conditions. For purposes of integrity, the primary containment is composed of both the freestanding steel shell containment vessel and the containment isolation system. This structure and system are directly relied upon to maintain containment integrity. The primary containment functional design is described in Section 6.2.1.

Containment isolation can be initiated by either of two signals: Phase A and Phase B.

Phase A signal is generated by either of the following:

1. Manual - Either of two momentary controls.

2. Safety injection signal generated by one or more of the following:

   a. Low steamline pressure in any steamline
   ~~High main steam flow coincident with low steam line pressure of low-low primary coolant average termperature in two of four loops.~~
   ~~b.~~
   ~~High differential pressure between any one main steam line and two of the other three lines.~~
   ~~c.~~
   b. Low pressurizer pressure.
   ~~d.~~
   c. ~~Two out of three~~ High containment pressure ~~signals.~~
   d. ~~e.~~
   Manual - Either of two momentary controls

Phase B signal is generated by either of the following:

1. Manual - Two sets (two switches per set) - actuation of both switches necessary in either set for spray initiation.

2. ~~Two out of four~~ High-high containment pressure ~~signals.~~

Containment isolation Phase A exists if containment isolation Phase B exists, when the Phase B signal is initiated by automatic instrumentation. Phase A containment isolation does not occur when the Phase B signal is initiated manually. The instrumentation circuits that generate both Phase A and Phase B signals are described in Section 7.1.2.1.2.

Containment purge system isolation (containment purge lines only) can be initiated by either of two signals:

1. Manual - Phase A or B manual initiate
   - SIS manual initiate

2. Automatic- SIS auto-initiate
   - High radiation (Train A or B sensor)
   - High purge exhaust radiation (1 of 2 sensors).

7.0 INSTRUMENTATION AND CONTROLS

7.1 INTRODUCTION

This chapter presents the various plant Instrumentation and Control Systems by relating the functional performance requirements, design bases, system descriptions, design evaluations, and tests and inspections for each. The information provided in this chapter emphasizes those instruments and associated equipment which constitute the protection system as defined in IEEE Std. 279-1971 "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations."

The primary purpose of the Instrumentation and Control Systems is to provide automatic protection against unsafe and improper reactor operation during steady state and transient power operations (Conditions I, II, III) and to provide initiating signals to mitigate the consequences of faulted conditions (Condition IV). For a discussion of the four conditions see Chapter 15. The information presented in this chapter emphasizes those Instrumentation and Control Systems which are essential to assuring that the reactor can be operated to produce power in a manner that insures no undue risk to the health and safety of the public.

It is shown that the applicable criteria and codes, such as the General Design Criteria and IEEE Standards, concerned with the safe generation of nuclear power are met by these systems.

Definitions

The definitions below establish the meaning of words in the context of their use in Chapter 7.

Channel - An arrangement of components and modules or software as required to generate a single protective action signal when required by a plant condition. A channel loses its identity where single action signals are combined.

DNBR - (Departure from Nucleate Boiling Ratio) - The ratio of the critical heat flux (defined as the transition from nucleate boiling to film boiling) to the actual local heat flux.

Module - Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Insert A

0794 PKG

Insert A to Page 7.1-1

<u>Software</u> - The entire set of programs, procedures, and related documentation associated with a system, especially a computer system.

accuracy, which means reference accuracy or the accuracy of that device at reference operating conditions: "Reference accuracy includes conformity, hysteresis and repeatability." To adequately define the accuracy of a system, the term reproducibility is useful as it covers normal operating conditions. The following terms, "trip accuracy," etc., will then include conformity and reproducibility under normal operating conditions. Where the final result does not have to conform to an actual process variable but is related to another value established by testing, conformity may be eliminated, and the term reproducibility may be substituted for accuracy.

Readout Devices - For consistency the final device of a complete channel is considered a readout device. This includes indicators, recorders, isolators (nonadjustable) and controllers.

Channel Accuracy - This definition includes accuracy of primary element, transmitter and rack modules. It does not include readout devices or rack environmental effects, but does include process and environmental effects on field mounted hardware. Rack environmental effects are included in the next two definitions to avoid duplication due to dual inputs.

Indicated and/or Recorded Accuracy - This definition includes channel accuracy, accuracy of readout devices and rack environmental effects.

Trip Accuracy - This definition includes comparator accuracy, channel accuracy for each input, and rack environmental effects. This is the tolerance expressed in process terms (or percent of span) within which the complete channel must perform its intended trip function. This includes all instrument errors but no process effects such as streaming. The term "actuation accuracy" may be used where the word "trip" might cause confusion (for example, when starting pumps and other equipment).

Actuation Accuracy - Synonymous with trip accuracy, but used where the word "trip" may cause ambiguity.

Cold Shutdown - The reactor is in the cold shutdown condition when the reactor is subcritical by at least 1 percent delta k/k and T(avg) is $\leq$200°F with T(avg) defined as the average temperature across a reactor vessel as measured by the hot and cold leg temperature detectors.

Hot Shutdown Condition - When the reactor is subcritical by an amount greater than or equal to the margin to be specified in the applicable technical specification and T(avg) is greater than or equal to the temperature to be specified in the applicable technical specification.

Phase A Containment Isolation - Closure of all nonessential process lines which penetrate containment initiated by the safety injection signal.

Phase B Containment Isolation - Closure of remaining process lines, initiated by containment Hi-Hi pressure signal (process lines do not include Engineered Safety Features lines).

System Response Times

Reactor Trip System Response Time

The time delays are defined as the time required for the reactor trip (i.e., the time the rods are free and begin to fall) to be initiated following a step change in the variable being monitored from at least 5 percent below (or above) to at least 5 percent above (or below) the trip setpoint. 45

Engineered Safety Features Actuation System Response Time

The interval required for the Engineered Safety Features sequence to be initiated subsequent to the point in time that the appropriate variable(s) exceed setpoints. The response time includes sensor~~/process~~ (analog) and process/ logic (digital) delay.

Normal Operating Conditions - For this document, these conditions cover all normal process temperature and pressure changes. Also included are ambient temperature changes around the transmitters and racks.

Control Accuracy - This definition includes channel accuracy, accuracy of readout devices (isolator, controller), and rack environmental effects. Where an isolator separates control and protection signals, the isolator accuracy is added to the channel accuracy to determine control accuracy, but credit is taken for tuning beyond this point; i.e., the accuracy of these modules (excluding controllers) is included in the original channel accuracy. It is simply defined as the accuracy of the control signal in percent of the span of that signal. This will then include gain changes where the control span is different from the span of the measured variable. Where controllers are involved, the control span is the input span of the controller. No error is included for the time in which the system is in a non-steady-state condition.

7.1.1 Identification of Safety-Related Systems

7.1.1.1 Safety-Related Systems

The Nuclear Steam Supply System (NSSS) instrumentation required

0794 PKG

to function to achieve the system responses assumed in the safety evaluations and those needed to shut down the plant are given in this section. Safety related systems are identified in Table 1.7-1 and Table 7.1-2 and compared to similar operating plants in Section 1.3.

~~Safety related instrumentation channels are processed with both analog and digital modules. Identification of which type of modules (analog or digital) used to process each protection instrumentation channel is provided in Table 7.1-3.~~ 63

DELETE

7.1.1.1.1 Reactor Trip System

The Reactor Trip System is a functionally defined system described in Section 7.2. The equipment which provides the trip functions is identified and discussed in Section 7.2. Design bases for the Reactor Trip System are given in Section 7.1.2.1. Figure 7.1-1 includes a block diagram of this system. 63

7.1.1.1.2 Engineered Safety Features Actuation System

The Engineered Safety Features Actuation System is a functionally defined system described in Section 7.3. The equipment which provides the actuation functions is identified and discussed in Section 7.3. Design bases for the Engineered Safety Features Actuation System are given in Section 7.1.2.1.

7.1.1.1.3 Vital Instrumentation and Control Power Supply System

Design bases for the Vital Control Power Supply System are given in Section 7.1.2.1. Further description of the system is provided in Section 8.3.

7.1.1.1.4 Auxiliary Control Air System

The Auxiliary Control Air System supplies essential control air to safety-related equipment such as the auxiliary feedwater control valves; dampers in the Auxiliary Building Gas Treatment System and the Emergency Gas Treatment System; and the Control Building HVAC System. Further description of the system is given in Section 9.3.1. 63

7.1.1.2 Safety-Related Display Instrumentation

The Post Accident Monitoring System (PAM) provides essential information required by the operator to diagnose and monitor significant accident conditions. The accident-monitoring instrumentation is designed with redundant channels so that a single failure does not prevent the operator from determining the nature of an accident, the functioning of the engineered safety features, the need for operator action, and the response of the plant to the safety measures in operation. This system is described in Section 7.5.

All other safety-related display instrumentation is discussed in Section 7.5.

The Bypassed and Inoperable Status Indication System (BISI) does not perform a safety function, nor do administrative procedures call for immediate 56

0794 PKG

operator action based solely on BISI indication. The BISI equipment is isolated from the associated safety-related equipment so as to preclude any abnormal or normal action of the BISI from preventing the performance of a safety function. The BISI is described in detail in Section 7.7. 56

7.1.1.3 Instrumentation and Control System Designers

All systems discussed in Chapter 7 have definitive functional requirements developed on the basis of the Westinghouse NSSS design. TVA is responsible for the total design of the WBN instrumentation and controls systems. The RPS, ESFAS, and SSPS are generally the instrumentation and controls systems within the scope of the Westinghouse supply. Figure 7.2-1 (Sheets 1 through 3) shows the logic for the Reactor Protection System. 63

7.1.1.4 Plant Comparison

System functions for all systems discussed in Chapter 7 are similar to those of Sequoyah Nuclear Plant. Detailed comparison is provided in Section 1.3.

7.1.2 Identification of Safety Criteria

Section 7.1.2.1 gives design bases for the systems given in Section 7.1.1.1, except for the Auxiliary Control Air System which is described in Section 9.3.1. Design bases for nonsafety-related systems are provided in the sections which describe the systems. Conservative considerations for instrument errors are included in the accident analyses presented in Chapter 15. Functional requirements, developed on the basis of the results of the accident analyses, which have utilized conservative assumptions and parameters are used in designing these systems and a preoperational testing program verifies the adequacy of the design. Accuracies are given in Sections 7.2, 7.3 and 7.5.

The documents listed below were considered in the design of the systems given in Section 7.1.1. In general, the scope of these documents is given in the document itself. This determines the systems or parts of systems to which the document is applicable. A discussion of compliance with each document for systems in its scope is provided in the referenced sections.

Because some documents were issued after design and testing had been completed, the equipment documentation may not meet the format requirements of some standards. Table 7.1-1 and Notes 1 through 5 identify the degree of conformance to applicable documents and justify exceptions. The documents considered are:

1. "General Design Criteria for Nuclear Power Plants," Appendix A to Title 10 CFR Part 50, July 7, 1971. (See Sections 7.2, 7.3, 7.4, and 7.6).

and the Safety-Related Display Instrumentation systems which are described in Section 7.5.

2. "Regulatory Guide 1.11 - Instrument Lines Penetrating Primary Reactor Containment," Regulatory Guides for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Atomic Energy Commission.

3. "Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions," Regulatory Guides for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Atomic Energy Commission. (See Table 7.1-1, Note 2).

4. Regulatory Guide 1.29 (Revision 1) - "Seismic Design Classification," Regulatory Guides for Water-Cooled Nuclear Power Plants," Directorate of Regulatory Standards, Atomic Energy Commission.

5. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971. (See Sections 7.2., 7.3, 7.6).

6. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Criteria for Class IE Electric Systems for Nuclear Power Generating Stations," IEEE Standard 308-1971.

7. The Institute of Electrical and Electronic Engineers, Inc.," IEEE Standard for Electrical Penetration Assemblies in Containment Structures for Nuclear Fueled Power Generating Stations," IEEE Standard 317-1971. (See Section 8.3.1.2.3) | 63

8. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Standard: General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations," IEEE Standard 323-1971. (See Table 7.1-1, Note 4).

I1

~~9.~~ 10 The Institute of Electrical and Electronic Engineers, Inc.," IEEE Trial-Use Guide for Type Tests of Continuous-Duty Class I Motors Installed Inside the Containment of Nuclear Power Generating Stations." IEEE Standard 334-1971. (See Section 8.3).

~~10.~~ 11 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations," IEEE Standard 336-1971. (See Chapter 10). | 63

~~11.~~ 12 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial-Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE Standard 338-1971. (See Section 7.3.2.2.5 and Table 7.1-1, Note 1).

I2

0794 PKG

Insert 1 to Page 7.1-7

9. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard for Qualifying Class 1-E Equipment for Nuclear Power Generating Stations", IEEE Std. 323-1974.

Insert 2 to Page 7.1-7

13. IEEE-Std. 338-1987 "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems".

0794 PKG

~~12.~~ 14 The Institute of Electrical and Electronic Engineers, Inc., 'IEEE Trial-Use Guide for Seismic Qualification of Class I Electric Equipment for Nuclear Power Generating Stations,' IEEE Standard 344-1971. (See Section 3.10.) 24

I3 ~~13.~~ 18 ~~17~~ The Institute of Electrical and Electronic Engineers, Inc., 'IEEE Trial-Use Guide for the Application of the Single-Failure Criterion to Nuclear Power Generating Station Protection Systems,' IEEE Standard 379-1972. (See Table 7.1-1, Note 3) 24

I4 ~~14.~~ ~~21~~ 22 'Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,' Regulatory Guides for Water-Cooled Nuclear Power Plants, Division of Reactor Standards, Atomic Energy Commission. (See Table 7.1-1, Note 3.) 24

I5

7.1.2.1 Design Bases

The technical design bases for the protection systems are provided by Westinghouse equipment specifications which consider the functional requirements for these systems and applicable criteria as identified in Table 7.1-1.

7.1.2.1.1 Reactor Trip System

The Reactor Trip System acts to limit the consequences of Condition II events (faults of moderate frequency such as loss of feedwater flow) by, at most, a shutdown of the reactor and turbine, with the plant capable of returning to operation after corrective action. The Reactor Trip System features impose a limiting boundary region to plant operation which ensures that the reactor safety limits analyzed in Chapter 15 are not exceeded during Condition II events and that these events can be accommodated without developing into more severe conditions. 52

The design requirements for the Reactor Trip System are derived by analyses of plant operating the fault conditions where automatic rapid control rod insertion is necessary in order to prevent or limit core or reactor coolant boundary damage. The design bases addressed in IEEE Standard 279-1971 are discussed in Section 7.2.1. The design limits for this system are:

1. Minimum DNBR shall not be less than 1.30 as a result of any anticipated transient or malfunction (Condition II faults).

2. Power density shall not exceed the rated linear power density for Condition II faults. See Chapter 4 for fuel design limits.

15. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Recommended Practices for Seismic Qualification of Class 1-E Equipment for Nuclear Power Generating Stations", IEEE Std. 344-1975.

~~15.~~ 16 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Recommended Practices for Seismic Qualification of Class 1-E Equipment for Nuclear Power Generating Stations", IEEE Std. 344-1987.

~~16.~~ 17 The Institute of Electrical and Electronic Engineers, Inc., "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Std. 352-1975

Insert 4 to Page 7.1-8

19 ~~18.~~ The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," IEEE Std. 379-1988

20 ~~19.~~ The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Std. 384-1981

21 ~~20.~~ The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603-1980

Insert 5 to Page 7.1-8

~~22. Regulatory Guide 1.22, February 1972 "Periodic Testing of Protection System Actuation Functions (Safety Guide 22)~~

~~23. Regulatory Guide 1.29, September 1978 "Seismic Design Classification"~~

23 ~~24.~~ Regulatory Guide 1.47, May 1973 "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"

~~25. Regulatory Guide 1.53, June 1973 "Application of the Single Failure Criteria to Nuclear Power Plant Protection Systems"~~

24 ~~26.~~ Regulatory Guide 1.75, September 1978 "Physical Independence of Electrical Systems"

25 ~~27.~~ Regulatory Guide 1.89, November 1974 "Qualification of Class 1E Equipment for Nuclear Power Plants"

26 ~~28.~~ Regulatory Guide 1.97, December 1980 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident"

0794 PKG

Insert 5 to Page 7.1-8 Continued

27 ~~29~~. Regulatory Guide 1.100, August 1977 "Seismic Qualification of Electrical Equipment for Nuclear Power plants".

28 ~~30~~. Regulatory Guide 1.105, November 1976 "Instrument Setpoints".

29 ~~31~~. Regulatory Guide 1.118, June 1978 "Periodic Testing of Electric Power and Protection Systems".

30 ~~32~~. Regulatory Guide 1.153, December 1985 "Criteria For Power, Instrumentation and Control Portions of Safety Systems".

- Regulatory Guide 1.153 endorses the guidance of IEEE-Std. 603-1980.

31 ~~33~~. ANSI/IEEE-ANS-7-4.3.2-1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations".

- ANSI/IEEE-ANS-7-4.3.2-1982 - expands and amplifies the requirements of IEEE-Std. 603-1980.

32 ~~34~~. Regulatory Guide 1.152, November 1985 "Criteria for Programmable Digital Computer System Software in Safety-Related Systems in Nuclear Plants".

- Regulatory Guide 1.152 endorses the guidance of ANSI/IEEE-ANSI-7-4.3.2-1982.

including all permissives and blocks. All blocks of a protective function are automatically cleared whenever the protective function would be required to function in accordance with General Design Criteria 20, 21, and 22, and Paragraphs 4.11, 4.12, and 4.13 of IEEE Standard 279-1971. Control interlocks (C) are identified on Table 7.7-1. Because control interlocks are not safety related, they have not been specifically designed to meet the requirements of IEEE Protection System Standards.

7.1.2.1.6 Bypasses

Bypasses are designed to meet the requirements of IEEE 279-1971, Sections 4.11, 4.12, 4.13 and 4.14. A discussion of bypasses provided is given in Sections 7.2 and 7.3.

7.1.2.1.7 Equipment Protection

The criteria for equipment protection are given in Chapter 3. Equipment related to safe operation of the plant is designed, constructed and installed to protect it from damage. This is accomplished by working to accepted standards and criteria aimed at providing reliable instrumentation which is available under varying conditions. As an example, certain equipment is seismically qualified in accordance with IEEE 344-1971. During construction, independence and separation are achieved, as required by IEEE 279-1971, either by barriers or physical separation. This serves to protect against complete destruction of a system by fires, missiles or other natural hazards.

7.1.2.1.8 Diversity

Functional diversity has been designed into the system. Generally, two or more diverse protection functions would automatically terminate an accident before unacceptable consequences could occur.

For example, there are automatic reactor trips based upon nuclear flux measurements, reactor coolant loop temperature and flow measurements, pressurizer pressure and level measurements, reactor coolant pump under frequency and under voltage measurements, ~~and feedwater flow~~ and steam generator water level measurements, as well as manually, and by initiation of a safety injection signal.

Regarding the Engineered Safety Features Actuation System for a loss-of-coolant accident, a safety injection signal can be obtained manually or by automatic initiation from two diverse parameter measurements.

1. Low pressurizer pressure

15

0794 PKG

2. High containment pressure.

~~For a steam break accident, injection signal actuation is provided by:~~

1. ~~High steam line flow coincident with low steam line pressure or low low T_{avg}~~

2. ~~High steam line differential pressure~~.

3. ~~For a steam break inside containment, high containment pressure provides an additional parameter for generation of the signal.~~

~~All of the above sets of signals are redundant and physically separated and meet the requirements of IEEE 279-1971.~~

INSERT 8

7.1.2.1.9 ~~Bistable~~ Trip Setpoints

The design of the Reactor Protection and Engineered Safety Features Systems is such that the ~~bistable~~ trip setpoints do not require process transmitters to operate within 5 percent of the high and low end of their calibrated span or range. Functional requirements established for every channel in the Reactor Protection and Engineered Safety Features Systems stipulate the maximum allowable errors on accuracy, linearity, and reproducibility. The protection channels have the capability for and are tested to ascertain that the characteristics throughout the entire span in all aspects are acceptable and meet functional requirements specifications. As a result, no protection channel operates normally within 5 percent of the limits of its specified span.

In this regard, it should be noted that the specific functional requirements for response time, setpoints, and operating span are determined from the results and evaluation of safety studies to be carried out using data pertinent to the plant. Emphas~~es~~ is is placed on establishing adequate performance requirements under both normal and faulted conditions. This will include consideration of process transmitters margins such that even under a highly improbable situation of full power operation at the limits of the operating map (as defined by the high and low pressure reactor trip, ΔT overpower and overtemperature trip lines (DNB protection) and the steam generator safety valve pressure setpoint) that adequate instrument response is available to ensure plant safety.

7.1.2.2 Independence of Redundant Safety-Related Systems

The safety-related systems in Section 7.1.1.1 are designed to meet the independence and separation requirements of criterion 22 of the 1971 General Design Criteria and Paragraph 4.6 of IEEE 279-1971. The administrative responsibility and control

Insert 8 to Page 7.1-12

The Reactor Protection System trip setpoints have been selected to ensure that core damage and loss of integrity of the Reactor Coolant System are prevented during anticipated operational events. These setpoints were analytically determined in accordance with the methodology described in Reference 6. Both the nominal and limiting settings have been incorporated into the Technical Specifications. Nominal settings are more conservative than the limiting setpoints. This allows for measurement and calibration uncertainties and instrument channel drift which may occur between periodic tests without exceeding the limiting setpoints.

provided during the design and installation is discussed in Chapter 17 which addresses the Quality Assurance programs applied by Westinghouse and TVA.

The electrical power supply instrumentation and control conductors for redundant circuits of a nuclear plant have physical separation including PAM Category I and protection set I, II, III and IV instrumentation and control. Their cables are run in separate raceways to preserve divisional integrity and to ensure that no single credible event will prevent operation of the associated function due to electrical conductor damage. Detailed information pertaining to electrical cable for safety-related systems is given in Section 8.3.1.4. Critical circuits and functions include: power, control, and Process protection ~~instrumentation~~ channels associated with the operations of the Reactor Trip System or Engineered Safety Features Actuation System. Credible events shall include, but not be limited to, the effects of short circuits, pipe rupture, missiles, etc., and are considered in the basic plant design. Control board details are given in Section 7.7.1.10. In the control board, separation of redundant circuits is maintained as described in Section 7.1.2.2.2.

Instrument sensing lines (including capillary systems) which serve safety-related systems identified in Section 7.1.1.1 are designed to meet the independence requirements of criterion 22 of the 1971 General Design Criteria and IEEE 279-1971 Section 4.6. The requirements consider the following events: (1) normal activities in the area (e.g., maintenance); (2) high and moderate energy jet streams, missiles, and pipe whip; and (3) possible damage caused by falling loads from the plant lifting systems (e.g., cranes, monorails). Exceptions to these requirements shall be evaluated for technical adequacy and documented in Design Basis Documents.

7.1.2.2.1 General

1. Cables of redundant circuits are run in separate cable trays, conduits, ducts, penetrations, etc.

2. Circuits for nonredundant functions should be run in cable trays or conduit separated from those used for redundant circuits. Where this can not be accomplished, nonredundant circuits may be run in a cable tray, conduit, etc., assigned to a redundant function. When so routed, it must remain with that particular redundant circuit routing and shall not cross over to other redundant groups.

3. Horizontal and vertical separation shall be maintained between cable trays associated with redundant circuits.

4. Where it is impractical for reasons of equipment arrangement to provide separate cable trays, cables of redundant circuits may be isolated by physical barriers or be installed in separate metallic conduit or proven safe by test or analysis.

5. Power and control cables rated at 600V or below shall not be placed in cable trays with cables rated above 600V.

6. Low-level type signal cables shall not be routed in cable trays containing power cables. Higher level protection instrumentation analog and signal cables (above 100 mV) may be

routed in the same tray with control cables if a tray barrier is provided between cables.

7.1.2.2.2 Specific Systems

Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. 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. Each redundant channel is energized from a separate ac power feed.

INSERT 7

Within the protection instrument channels, there are four separate sets of protection channel racks. Redundant instrumentation channels are separated by locating modules of redundant instrument channels in different protection channel racks. Separation of redundant channels begins at the sensors and is maintained in the field wiring, containment penetrations, and protection channel racks. Since all modules and components within any one of the four racks are associated with a single protection channel, there is no necessity for separation of wiring, modules, and components within each rack.

In the Nuclear Instrumentation System, ~~Process Protection Instrumentation Racks,~~ and the Solid State Protection System ~~input PCS,~~ racks where redundant channels of protection instrumentation are physically adjacent, there are no wireways or cable penetrations which would permit, for example, a fire resulting from electrical failure in one channel to propagate into redundant channels in the logic racks. Redundant protection instrumentation channels are separated by locating redundant modules in different racks. Since all equipment within any rack is associated with a single protection set, there is no requirement for separation of wiring and components within the rack.

Independence of the logic trains is discussed in Sections 7.2 and 7.3. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all full-length control rod drive mechanisms, permitting the rods to free fall into the core.

1. Reactor Trip System

   a. Separate routing is maintained between the four Reactor Trip System ~~instrumentation~~ channels, including the sensor signals, ~~bistable~~ comparator signals, and associated power supplies.

   process protection

Insert 7 to Page 7.1-14

Within the process protection system there are four separate protection channel sets. Redundant protection channels are separated by locating the processing electronics of the redundant channels in different protection channel rack sets. Separation of redundant channels begins at the sensors and is maintained in the field wiring, containment penetrations, and process protection channel racks. Thus any single failure within a channel will not prevent initiation of a required protection system action.

0794 PKG

b. Separate routing of the reactor trip signals from the two redundant logic system cabinets is maintained. In addition, they are separated (by spatial separation, by provision of barrier, or by separate cable trays or wireways) from the four protection instrumentation channels.

2. Engineered Safety Features Actuation System

a. Separate routing is maintained for the four redundant sets of ESF Actuation System process protection ~~instrumentation~~ channels, comparator ~~bistable~~ output signals and power supplies for such systems. The separation of these four redundant and independent protection channel sets is maintained from sensors through process protection ~~instrument~~ racks ~~and~~ to logic system cabinets.

b. Separate routing of the ESF actuation signals from the two redundant logic system cabinets is maintained. The ESF actuation signals are also separated from the four process protection ~~instrumentation~~ channels.

c. Separate routing of redundant control and power circuits associated with the operation of engineered safety features equipment is required to retain redundancies provided in the system design and power supplies.

3. Vital Control Power Supply System

The separation criteria presented above also apply to the power supplies for the load centers and buses distributing power to redundant components and to the control of these power supplies.

4. Control Board

Control board switches and associated lights are generally furnished in modules. Modules provide a degree of physical protection for the switches, associated lights and wiring. Teflon wire is used within the module and between the module and the first termination point.

Modular train column wiring is formed into wire bundles and carried to metal wireways (gutters). Gutters are run into metal vertical wireways (risers). The risers are the interface between field wiring and control board wiring. Risers are arranged to maintain the separated routing of the field cable trays.

Certain wiring within control boards has been designed and installed to maintain physical independence. Design features include enclosed modular switches, metal wireways, use of cable rated at 600V-200°C temperature rating and with noncombustible insulation of teflon type E or K per

0794 PKG

MIL-W-16878 and metallic woven braid applied to the outer jacket of critical wires. PVC type tubing (Ty-gon) has been used in some installations to insulate up to approximately 6 inches of the drain wire where signal cable is broken out to terminate the cable at termination points.

Figure 7.1-2 shows the details of the control boards critical wiring braid installation. Wiring for each train is routed from the field to separate vertical risers, separated horizontally in enclosed horizontal wireways, and then routed from the wireway to the enclosed switch module in metallic braid. Maximum air space between cables of different trains has been maintained and in no case do cables from different trains touch nor can they migrate with time to touch.

In order to maintain separation between wiring associated with different logic trains, mutually redundant safety train wiring is not terminated on a single device. Backup manual actuation switches link the separate trains by mechanical means to provide greater reliability of operator action for the manual reactor trip function and manual Engineered Safety Features actuations. The linked switches are themselves redundant so that operation of either set of linked switches will actuate safety trains "A" and "B" simultaneously.

Safety-related indicators, e.g., postaccident monitoring indicators are separated by metallic barrier plates and/or air separation. Teflon wire is used between the indicators and the first termination point. The wire routing method is similar to that used for the modules.

Reactor Trip System and Engineered Safety Features Actuation System process protection ~~instrumentation~~ channels may be routed in the same wireways provided circuits have the same power supply and channel set identity (I, II, III or IV).

7.1.2.2.3 Fire Protection

Details of fire protection are provided in Section 9.5.1.

7.1.2.3 Physical Identification of Safety-Related Equipment

There are four separate sets of process protection channels racks identifiable with equipment associated with the Reactor Trip System and with the Engineered Safety Features Actuation System. A process protection channel set may consist of more than one instrumentation rack. The color coding of each instrumentation rack nameplate coincides with the color code established for the protection instrumentation channel of which it is a part. Redundant channels are separated by locating them in different protection channel racks. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and ~~equipment~~ process protection racks to the redundant trains in process protection the logic racks. The Solid State Protection System input cabinets are divided into four isolated compartments, each serving one of the four redundant ~~input~~ channels. Horizontal 1/8-inch thick solid steel barriers, coated with fire-retardant paint, separate the compartments. Four solid steel wireways coated with fire-retardant paint enter the input cabinets vertically. The wireway for a particular compartment is open into that compartment so that flame could not propagate to affect other channels. At the logic racks the protection set color coding for redundant channels is clearly maintained until the channel loses its identity in the redundant logic trains. The color-coded nameplates described below provide identification of equipment associated with protective functions and their channel set association.

Protection Set	Color Coding
I	Red ~~Black~~ with white lettering
II	Black with white lettering
III	Blue with white lettering
IV	Yellow with black lettering

Post Accident Monitoring and train-oriented modules are identified as follows:

	Color
Train A	Orange and white
Train B	Brown and White
Special[1]	Gold and Black
Postaccident Monitoring Channel 1	Purple and White
Postaccident Monitoring Channel 2	Green and Black
Nondivisional (Nonsafety-related)	White and Black
Normal Offsite PWR Supply	White and Black
Alt Offsite PWR Supply	White and Black

All nonrack-mounted protective equipment and components are provided with an identification tag or nameplate. Small electrical components such as relays have nameplates on the enclosure which houses them. All cables are numbered with identification tags. In congested areas, such as under or over the control boards, instrument racks, etc., cable trays and conduits containing redundant circuits are ~~shall be~~ identified using permanent markings. The purpose of such markings, discussed in detail Section 8.3.1.4, is to facilitate cable routing identification for future modifications or additions. Positive permanent identification of field routed cables ~~shall be~~ is provided by nameplates on the input panels of the solid state logic protection system.

[1] The circuits requiring special separations are suffix S and described in Section 8.3.1.4.3.

0794 PKG

REFERENCES

1. W. C. Gangloff and W. D. Luftus, 'An Evaluation of Solid State Logic Reactor Protection in Anticipated Transients,' WCAP-7706-L, July 1971, (Westinghouse NES Proprietary), and WCAP-7706, July 1971. 52

2. T. W. T. Burnett, 'Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors,' WCAP-7306, April 1969.

3. D. N. Katz, Solid State Logic Protection System Description, WCAP-7672, June 1971.

4. W. C. Gangloff, 'An Evaluation of Anticipated Operational Transient in Westinghouse Pressurized Water Reactors,' WCAP-7486-L, December 1970, (Westinghouse NES Proprietary), and WCAP-7486, May 1971. 52

I6

Insert 6 to Page 7.1-19

5. Erin, L. E., "Topical Report Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374, Rev. 1, December 1991 (Westinghouse Proprietary Class 2); WCAP-12375, Rev. 1, December 1991 (Westinghouse Proprietary Class 3).

6. Reagan, J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version, "WCAP-12096, Rev. 5 (Westinghouse Proprietary Class 2).

0794 PKG

TABLE 7.1-1

WATTS BAR NUCLEAR PLANT
NRC REGULATORY GUIDE CONFORMANCE

The extent to which the recommendations of the applicable NRC regulatory guides and IEEE standards are followed for the Class IE instrumentation and control systems is shown below. The symbol (F) indicates full compliance. Those which are not fully implemented are discussed in the referenced sections of the FSAR and in the footnotes as indicated.

Regulatory Guide 1.11, "Instrument Lines Penetrating Primary Containment" (F)

Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions" (F, see note 2)

Regulatory Guide 1.29, "Seismic Design Classification" (F)

Regulatory Guide 1.30, "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment" (F)

Regulatory Guide 1.40, "Qualification Tests of Continuous Duty Motors Installed Inside the Containment of Water-Cooled Nuclear Power Plants (F)

Regulatory Guide 1.45, "Reactor Coolant Pressure Boundary Leakage Detection systems" (F, See Note 7)

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems" (F see note 5)

Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems" (F see note 3)

Regulatory Guide 1.62, "Manual Initiation of Protective Actions" (F)

Regulatory Guide 1.63, "Electrical Penetration Assemblies in Containment Structures for Water-Cooled Nuclear Power Plants" (See Watts Bar FSAR Section 8.1 for compliance)

Regulatory Guide 1.68, "Preoperational and Initial Startup Test Program for Water-Cooled Power Reactors" (See Table 14.2-3)

Regulatory Guide 1.73, "Qualification Tests for Electric Valve Operators Installed Inside the Containment of Nuclear Power Plants" (F)

Regulatory Guide 1.75, "Physical Independence of Electric Systems" (See Watts Bar FSAR Sections 7.1.2.2, 7.1.2.3, 8.3.1.4, 8.3.2.4, and 8.3.2.5 for compliance)

Regulatory Guide 1.79, (ECCS Testing) See Section 6.3.4

Regulatory Guide 1.80, "Preoperational Testing of Instrument Air Systems" (F)

Regulatory Guide 1.89, "Environmental Qualification of Certain Electrical Equipment Important to Safety for Nuclear Power Plants" (See note 4)

I8

0794 PKG

Regulatory Guide 1.97, December 1980 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident" (See Watts Bar FSAR Section 7.5).

Regulatory Guide 1.100, August 1977 "Seismic Qualification of Electrical Equipment for Nuclear Power plants" (See Note 8).

Regulatory Guide 1.105, November 1976 "Instrument Setpoints" (See Note 8).

Regulatory Guide 1.118, June 1978 "Periodic Testing of Electric Power and Protection Systems" (See Note 8).

Regulatory Guide 1.153, December 1985 "Criteria For Power, Instrumentation and Control Portions of Safety Systems" (See Notes 8 and 9).

ANSI/IEEE-ANS-7-4.3.2-1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations" (See Notes 8 and ~~11~~ 10).

TABLE 7.1-1 (Continued) 0794 PKG

WATTS BAR NUCLEAR PLANT
NRC REGULATORY GUIDE CONFORMANCE

Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants" (P) (See note 6)

IEEE Standard 279-1971, "Protection Systems for Nuclear Power Generating Stations" (F)

IEEE Standard 308-1971, "Class 1E Power Systems for Nuclear Power Generating Stations" (F)

I9 IEEE Standard 338-1971, "Periodic Testing of Nuclear Power Generating Station Safety Systems" (See note 1 and WBNP FSAR Section 7.3.2.2.5 for compliance)

I10 IEEE Standard 344-1971, "Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations" (F) (For clarification of conformance to IEEE Standard 344-1975, See Section 3.10.1) move up

I11

Insert 9 to Table 7.1-1, Sheet 2 of 5

IEEE Std. 323-1974
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Standard for Qualifying Class 1~~e~~E Equipment for Nuclear Power Generating Stations", ~~IEEE Std. 323-1974~~ (See Note 8).

Insert 10 to Table 7.1-1 Sheet 2 of 5

IEEE-Std. 338-1987, "IEEE Standard Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems" (see Note 8).

Insert 11 to Table 7.1-1 Sheet 2 of 5

IEEE Std. 344-1987
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Recommended Practices for Seismic Qualification of Class 1~~e~~E Equipment for Nuclear Power Generating Stations", ~~IEEE Std. 344-1987~~ (See Note 8).

IEEE Std. 352-1975
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," ~~IEEE Std. 352-1975~~ (See Note 8).

IEEE Std. 379-1988
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems," ~~IEEE Std. 379-1988~~ (See Note 8).

IEEE Std. 384-1981
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," ~~IEEE Std. 384-1981~~ (See Note 8).

IEEE Std. 603-1980
~~The Institute of Electrical and Electronic Engineers, Inc.~~, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," ~~IEEE Std. 603-1980~~ (See Note 8).

0794 PKG

TABLE 7.1-1 (Continued)

WATTS BAR NUCLEAR PLANT
NRC REGULATORY GUIDE CONFORMANCE

Note 2 Conformance to Regulatory Guide 1.22

Periodic testing of the Reactor Trip and Engineered Safety Features Actuation Systems, as described in Sections 7.2.2 and 7.3.2, complies with NRC Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions." Under the present design, there are functions which are not tested at power because to do so would render the plant in a less safe condition. These are as follows:

1. Turbine trip equipment that causes a reactor trip;
   ~~Note to TVA:~~ tThe trip of turbine from this same turbine trip equipment also is taken credit for on an S.I. or R.T.;

2. Generation of a reactor trip by use of the manual trip switch;

3. Generation of a reactor trip by use of the manual safety injection switch;

4. Closing the main steam line stop valves; (part-stroke testing will be performed once per 92 days);

5. Closing the feedwater control valves; (part-stroke movement will be monitored during modulation of feedwater once per 92 days);

6. Closing the feedwater isolation valves;

7. Reactor coolant pump component cooling water isolation valves (close);

8. Reactor coolant pump seal water return valves (close).

The actuation logic for the functions listed is tested as described in Sections 7.2 and 7.3. As required by Regulatory Guide 1.22, where actuated equipment is not tested during reactor operation it has been determined that:

1. There is no practicable system design that would permit testing of the equipment without adversely affecting the safety or operability of the plant;

2. The probability that the protection system will fail to initiate the operation of the equipment is, and can be maintained, ~~acceptability~~ acceptably low without testing the equipment during reactor operation; and

3. The equipment will be routinely tested when the reactor is shutdown as defined in the Technical Specification.

Where the ability of a system to respond to a bona fide accident signal is intentionally bypassed for the purpose of performing a test during reactor operation, each bypass condition is automatically indicated to the reactor operator in the Main Control Room by a separate annunciator for the train in test. Test circuitry does not allow trains to be tested at the same time so that extension of the bypass condition to redundant systems is prevented.

~~0791 PKG~~ 0794 PKG

TABLE 7.1-1 (Continued)

WATTS BAR NUCLEAR PLANT
NRC REGULATORY GUIDE CONFORMANCE

Note 3 Conformance to IEEE 379-1972 and Regulatory Guide 1.53

The principles described in IEEE Standard 379-1972 were used in the design of the Westinghouse protection system. The system complies with the intent of this standard and the additional requirements of Regulatory Guide 1.53. The formal analyses required by the standard have not been documented exactly as outlined although parts of such analyses are published in various documents. Westinghouse has gone beyond the required analyses and has performed a fault-tree analysis reference [1].

The referenced Topical Reports provide details of the analyses of the protection systems previously made to show conformance with single failure criterion set forth in Paragraph 4.2 of IEEE Standard 279-1971. The interpretation of single failure criterion provided by IEEE-379 does not indicate substantial differences with the Westinghouse interpretation of the criterion except in the methods used to confirm design reliability. Established design criteria in conjunction with sound engineering practices form the bases for the Westinghouse protection systems. The Reactor Trip and Engineered Safeguards Actuation Systems are each redundant safety systems. The required periodic testing of these systems will disclose any failures or loss of redundancy which could have occurred in the interval between tests, thus ensuring the availability of these systems.

Note 4 Conformance to Regulatory Guide 1.89

Watts Bar Nuclear Power Plant 1E equipment within the scope of 10 CFR 50.49 is qualified in accordance with IEEE 323-1971 or IEEE 323-1974. (See reference 1 of Section 3.11). Reference 5 provides additional information for the Eagle 21 Process Protection System.

Note 5 Conformance to Regulatory Guide 1.47

Watts Bar Nuclear Plant will be in full compliance with the requirements to Regulatory Guide 1.47 (BISI) Revision 0.

Note 6 Conformance to Regulatory Guide 1.152

Watts Bar Nuclear Plant process protection ~~instrumentation~~ racks are qualified by procedures and testing to Westinghouse's interpretation of Regulatory Guide 1.152 (WCAP-~~12271~~ 13191, Watts Bar Nuclear Plant Eagle 21 Process Protection System Replacement Hardware Verification and Validation Report, April ~~1989~~ 1992).

Note 7 Conformance to Regulatory Guide 1.45

Compliance to Regulatory Guide 1.45 is as identified in Section 5.2.7.3.

Regulatory Guide 1.152 endorses the guidance of ANSI/IEEE-ANSI-7-4.3.2-1982.

I12

Insert 12 to Table 7.1-1 Sheet 5 of 5

Note 8 These Rules, Regulations and standards are applicable to the design of the Eagle 21 Process Protection System. Unless stated otherwise, the revision in effect on December 1, 1983 is applicable to the design.

Note 9 Regulatory Guide 1.153 endorses the guidance of IEEE-Std. 603-1980.

~~Note 10 Regulatory Guide 1.152 endorses the guidance of ANSI/IEEE-ANSI-7-4.3.2-1982~~

Note ~~11~~ 10 ANSI/IEEE-ANS-7-4.3.2-1982 - expands and amplifies the requirements of IEEE-Std. 603-1980.

0794 PKG

DELETE

TABLE 7.1-3

ANALOG PROTECTION INSTRUMENTATION CHANNELS

A. Pressurizer Pressure Protection Channels

B. Pressurizer Water Level Protection Channels

C. Steam/Feedwater Flow Protection Channels

D. Steam Generator Narrow Range Water Level Protection Channels

E. Reactor Coolant Low Flow Protection Channels

F. Impulse Chamber Protection Channels

G. Steam Pressure Protection Channels

H. Containment Pressure Protection Channels

I. Boric Acid Tank Level Protection Channel

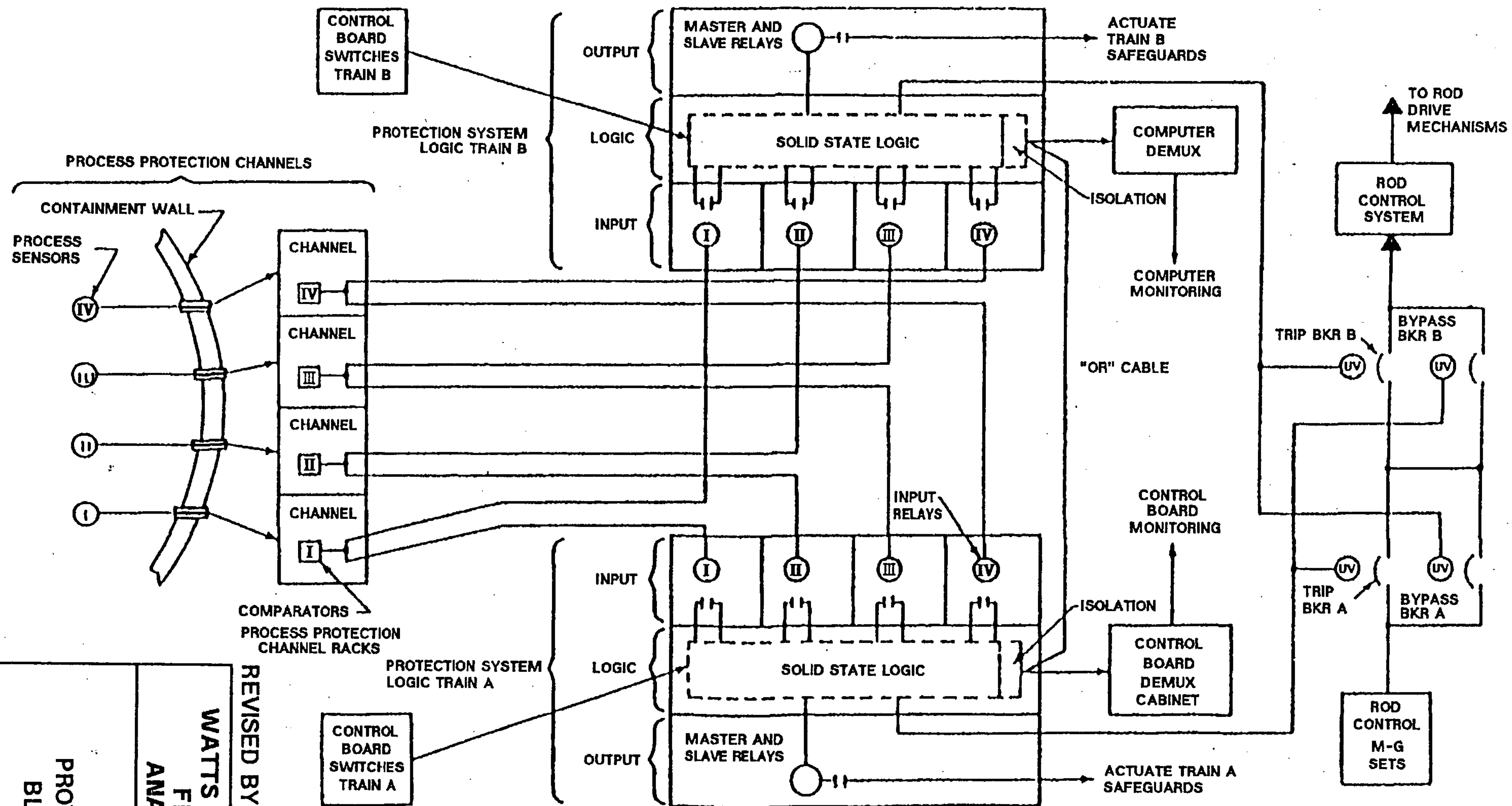
DIGITALLY PROCESSED PROTECTION INSTRUMENTATION CHANNELS

A. T_{Avg} and Delta T Protection Channels

B. Reactor Coolant (Wide Range) Temperature and Pressure Protection Channels

C. Pressurizer Liquid and Vapor Temperature Protection Channels (PAM)

D. Steam Generator Wide Range Water Level Protection Channels (PAM) 63



REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

PROTECTION SYSTEM
BLOCK DIAGRAM
FIGURE 7.1-1

0794 PKG

7.2 REACTOR TRIP SYSTEM

7.2.1 Description

7.2.1.1 System Description

The Reactor Trip System automatically keeps the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached. The safe operating region is defined by several considerations such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. Therefore, the Reactor Trip System keeps surveillance on process variables which are directly related to equipment mechanical limitations, such as pressure, pressurizer water level (to prevent water discharge through safety valves, and uncovering heaters) and also on variables which directly affect the heat transfer capability of the reactor (e.g. flow and reactor coolant temperatures). Still other parameters utilized in the Reactor Trip System are calculated from various process variables. In any event, whenever a direct process or calculated variable exceeds a setpoint the reactor will be shutdown in order to protect against exceeding the specified fuel design limit, gross damage to fuel cladding or loss of system integrity which could lead to release of radioactive fission products into the containment. 63

The following systems make up the Reactor Trip System:

1. Process ~~Instrumentation~~ PROTECTION and Control System ~~[1]~~ [1, 11]
2. Nuclear Instrumentation System [2]
3. Solid State Logic Protection System [3]
4. Reactor Trip Switchgear [3]
5. Manual Actuation Circuit

The Reactor Trip System consists of two to four redundant ~~instrumentation~~ process protection channels, which monitor various plant variables, and two redundant logic trains, which receive input protection action signals from the ~~instrumentation~~ process protection channels to complete the logical decisions necessary to automatically open the reactor trip breakers. 63

Each of the two trains, A and B, is capable of opening a separate and independent reactor trip breaker, RTA and RTB, respectively. The two trip breakers in series connect three phase AC

0794 PKG

2. Core Thermal Overpower Trips

The specific trip functions generated are as follows:

a. Overtemperature delta-T trip

This trip protects the core against low DNBR and trips the reactor on coincidence as listed in Table 7.2-1 with one set of temperature measurements per loop. The setpoint for this trip is continuously calculated by protection ~~instrumentation~~ circuitry for each loop by solving the following equation:

the EAGLE-21 Process

$$OT\Delta T\ Setpoint_i = \Delta T_{0_i} \left[K_1 - K_2 \left(\frac{1 + \tau_1 S}{1 + \tau_2 S} \right) \left(T_{avg_i} - T'_{avg_i} \right) + K_3 (P - P') - f_1 (\Delta I) \right]$$

An overtemperature delta T reactor trip occurs when

$$\Delta T_i \left(\frac{1 + \tau_4 S}{1 + \tau_5 S} \right) > OT\Delta T\ Setpoint_i$$

~~(See Note to Reviewer)~~

I13

where:

$T_{h_{ji}}$ = jth narrow range T_{hot} input signal from loop i

$$T^f_{h_{ji}} = T_{h_{ji}} \left(\frac{1}{1 + \tau_6 S} \right)$$

$$T^f_{h_{ave_i}} = \left(T^f_{h_{j-1_i}} + T^f_{h_{ji}} + T^f_{h_{j+1_i}} \right) / 3 \text{ (3 valid RTDs)}$$

T_{c_i} = narrow range T_{cold} input signal from loop i

$$T^f_{c_i} = T_{c_i} \left(\frac{1}{1 + \tau_7 S} \right)$$

$$\Delta T_i = T^f_{h_{ave_i}} - T^f_{c_i}$$

$$T_{avg_i} = \left(T^f_{h_{ave_i}} + T^f_{c_i} \right) / 2$$

63

0794 PKG

where: ΔT_i° = Indicated ΔT at Rated Thermal Power

$K_1 \leq 1.0952$

$K_2 = 0.0133/°F$

τ_1, τ_2 = Time constants utilized in the lead-lag compensator for T_{avg}, $\tau_1 = 33$ secs; $\tau_2 = 4$ secs

s = Laplace transform operator, sec^{-1}

T_{avg} = Average Temperature of loop i (i = 1 to 4)

T°_{avg} = Nominal T_{avg} at Rated Thermal Power (Calibration temperature for ΔT instrumentation, $\leq$ 588.2°F)

$K_3 = 0.000647$/psig

P = Pressurizer Pressure, ~~lb/in²g~~ psig

P° = 2235 ~~lb/in²g~~ psig (Nominal RCS operating pressure)

f_1 ~~f~~ (ΔI) = is a function of the indicated difference between the top and bottom detectors of the power range neutron ion chambers. Gains are selected based on measured instrument response during plant startup tests such that:

(i) for $I_t - I_b$ between -32% and +10% $f_1(\Delta I) = 0$ (where I_t and ~~&~~ I_b are percent RATED THERMAL POWER in the top and bottom halves of the cores respectively and $I_t + I_b$ is the total THERMAL POWER in percent of RATED THERMAL POWER)

(ii) for each percent that the magnitude of $(I_t - I_b)$ is less than ~~exceeds~~ -32%, the ΔT trip setpoint shall be automatically reduced by 1.34% of its value at RATED THERMAL POWER

(iii) for each percent that the magnitude of $(I_t - I_b)$ exceeds +10%, the ΔT trip setpoint shall be automatically reduced by 1.22% of its value at RATED THERMAL POWER.

ΔT_i = Temperature delta between hot leg and cold leg in loop i (i = 1 to 4)

τ_4, τ_5 = Time constants utilized in the lead-lag compensator for measured ΔT. $\tau_4 = 12$ seconds; $\tau_5 = 3$ seconds

0794 PKG

Insert 13 to Page 7.2-5 Continued

Note:~~to Reviewer:~~ Additional information on associated tau values (τ_6 and τ_7) are provided in Sections 7.2.1.1.4.

0794 PKG

τ_4, τ_5 - Time constants utilized in the lead-lag compensator for ΔT, $\tau_4 = 8$ s, $\tau_5 = 3$ s,

τ_6 - Time constant utilized in the lag compensator for T_{hot}, τ_6, = 0.0S,

$\Delta T_1°$ - Indicated ΔT at RATED THERMAL POWER,

K_1 - 1.0952,

K_2 - 0.0133/°F,

τ_1, τ_2 - Time constants utilized in the lead-lag compensator for T_{avg}, τ_1, = 33 S, τ_2 = 4S,

63

Note to Reviewer:

Please be advised that the equations for the Overtemperature and Overpower delta-T trip setpoints are effectively identical to the equations shown in previous amendments to this FSAR. However, the format has been modified to provide a more exact representation of the actual implementation and to allow for consistency of nomenclature between the Functional Requirements, Technical Specifications and FSAR.

τ_7 = Time constant utilized in the measured T_{cold} lag compensator, τ_7 = 0.0S, 63

T'_{avg_1} ≤ 588.2°F (Nominal T_{avg} at RATED THERMAL POWER), 63

K_3 = 0.000647/psig,

P = Pressurizer pressure, psig,

P' = 2235 psig (Nominal RCS operating pressure),

S = Laplace transform operator, s^{-1},

and f_1 (ΔI) is a function of the indicated difference between top and bottom detectors of the power range neutron ion chambers; with gains to be selected based on measured instrument response during plant startup tests such that:

(i) for q_t - q_b between -32% an +10% f_1 (ΔI) = 0 (where q_t and q_b are percent RATED THERMAL POWER in the top and bottom halves of the core respectively, and q_t + q_b is total THERMAL POWER in percent of RATED THERMAL POWER);

(ii) for each percent that the magnitude of (q_t - q_b) exceeds 32%, the ΔT Trip Setpoint shall be automatically reduced by 1.34% of its value at RATED THERMAL POWER;

(iii) for each percent that the magnitude of (q_t - q_b) exceeds +10%, the ΔT Trip Setpoint shall be automatically reduced by 1.22% of its value at RATED THERMAL POWER.

A separate long ion chamber unit supplies the flux signal for each overtemperature ΔT trip channel.

Increases in Δ beyond a predefined deadband result in a decrease in trip setpoint. Refer to Figure 7.2-2.

ΔI

The required one pressurizer pressure parameter per loop is obtained from separate sensors connected to three pressure taps at the top of the pressurizer. Four pressurizer pressure signals are obtained from the three taps by connecting one of the caps to two pressure transmitters. Refer to Section 7.2.2.3.3 for an analysis of this arrangement.

 0794 PKG

A detailed functional description of the process equipment associated with this function is contained in reference (11).

b. Overpower delta-T trip

This trip protects against excessive power (fuel rod rating protection) and trips the reactor on coincidence as listed in Table 7.2-1, with one set of temperature measurements per loop. The setpoint for each channel is continuously calculated using the following equation :

$$\text{OP}\Delta\text{T Setpoint}_i = \Delta T_i^{\circ} \left[K_4 - K_5 \left(\frac{\tau_3 S}{1 + \tau_3 S}\right) \left(T_{avg_i}\right) - K_6 \left(T_{avg_i} - T^{\circ}_{avg_i}\right) - f_2(\Delta I) \right]$$

An overpower ΔT reactor trip occurs when

$$\Delta T_i \left(\frac{1 + \tau_4 S}{1 + \tau_5 S}\right) > \text{OP}\Delta\text{T Setpoint}_i$$

I14

Where:

ΔT_i	=	As defined for overtemperature ΔT trip,
$\tau_4\ \tau_5$	=	As defined for overtemperature ΔT trip,
ΔT_i°	=	As defined for overtemperature ΔT trip,
K_4	=	1.09,
K_5	=	0.02/°F for increasing average temperature and 0 for decreasing average temperature,
τ_7	=	Time constant utilized in the lead-lag compensator for T_{avg} $\tau_7 = 5$ S,
K_6	=	0.00126/°F for $T > T_{avg_i}$ and $K_6 = 0$ for $\tau \leq T_{avg_i}$
T_{avg_i}	=	As defined for overtemperature delta-T trip
τ_3	=	Time constant used in lag compensator for T_{avg}, $\tau_3 = 0.0$S

<u>Note to Reviewer:</u>

Please be advised that the equations for the Overtemperature and Overpower delta-T trip setpoints are effectively identical to the equations shown in previous amendments to this FSAR. However, the format has been modified to provide a more exact representation of the actual implementation and to allow for consistency of nomenclature between the Functional Requirements, Technical Specifications and FSAR.

Insert 14 to Page 7.2-7

where: The following parameters have been defined in Section 7.2.1.1.2 (2)(a) ~~the~~ Overtemperature delta-T trip: ΔT°_{i}; T_{avgi}; T°_{avgi}; ΔT_{i}; τ_4; τ_5; s

$K_4 \leq 1.09$

$K_5 = 0.02/°F$ for increasing average temperature (T_{avgi}) and 0 for decreasing average temperature (T_{avgi})

$\tau_3 =$ Time constant used in lag compensator for T_{avg}, $\tau_3 =$ ~~0.0~~ 5 secs

$K_6 = 0.00126/°F$ for $T > T^{\circ}_{avgi}$ and 0 for $T \leq T^{\circ}_{avgi}$

$f_2(\Delta I) = 0$ for all ΔI.

Note: ~~to Reviewer:~~ Additional information on associated tau values (τ_6 and τ_7) are provided in Sections 7.2.1.1.4.

~~$T^{\circ}_{avg_i}$ = Indicated T_{avg} at RATED THERMAL POWER (Calibration temperature for ΔT instrumentation, $\leq 588.2°F$)~~ a 63

~~S = As defined for overtemperature ΔT trip.~~

~~$f_2(\Delta I)$ = 0 for all ΔI.~~

The source of temperature and flux information is identical to that of the overtemperature ΔT trip and the resultant overpower ΔT setpoint is compared to the same ΔT. A detailed functional description of the process equipment associated with this function is contained in reference [11]. 63

3. Reactor Coolant System Pressurizer Pressure and Water Level Trips

The specific trip functions generated are as follows:

a. Pressurizer low pressure trip

The purpose of this trip is to protect against low pressure which could lead to DNB. The parameter being sensed is reactor coolant pressure as measured in the pressurizer. Above P-7 the reactor is tripped when the pressurizer pressure measurements (compensated for rate of change) fall below present limits. This trip is blocked below P-7 to permit startup. The trip logic and interlocks are given in Table 7.2-1.
Preset

The trip logic is shown on Figure 7.2-1, Sheet 2. A detailed functional description of the process equipment associated with the function is contained in references ~~[1]~~.
[5] and [11].

0794 PKG

b. Pressurizer High Pressure Trip

The purpose of this trip is to protect the Reactor Coolant System against system overpressure.

COMPARATORS

The same sensors and transmitters used for the pressurizer low pressure trip are used for the high pressure trip except that separate bistables are used for trip. These bistables trip when uncompensated pressurizer pressure signals exceed preset limits on coincidence as listed in Table 7.2-1. There are no interlocks or permissives associated with this trip function. COMPARATORS

The logic for this trip is shown on Figure 7.2-1, Sheet 2. The detailed functional description of the process equipment associated with this trip is provided in references ~~[7]~~.

c. Pressurizer High Water Level Trip [5] and [11]

This trip is provided as a backup to the high pressurizer pressure trip and serves to prevent water relief through the pressurizer safety valves. This trip is blocked below P-7 to permit startup. The coincidence logic and interlocks of pressurizer high water level signals are given in Table 7.2-1.

The trip logic for this function is shown on Figure 7.2-1, Sheet 2. A detailed description of the process equipment associated with this function is contained in references ~~[7]~~.

4. Reactor Coolant System Low Flow Trips [5] and [11].

These trips protect the core from DNB in the event of a loss of coolant flow situation. The means of sensing the loss of coolant flow are as follows:

a. Low Reactor Coolant Flow

The parameter sensed is reactor coolant flow. Four elbow taps in each coolant loop are used as flow devices that indicate the status of reactor coolant flow. The basic function of this device is to provide information as to whether or not a reduction in flow has occurred. An output signal from two out of the three bistables in a loop would indicate a low flow in that loop.

COMPARATORS

The coincidence logic and interlocks are given in Table 7.2-1. The logic for this trip is shown on Figure 7.2-1, Sheet 3. The detailed functional description of the process equipment associated with the trip function is contained in references ~~[7]~~. 62

[5] and [11]

0794 PKG

b. Reactor Coolant Pump Undervoltage Trip

This trip is required in order to protect against low flow which can result from loss of voltage to more than one reactor coolant pump motor (e.g. from plant loss of voltage or reactor coolant pump breakers opening).

There is one undervoltage sensing relay ~~connected~~ for each pump motor connected at the load side of each reactor coolant pump breaker. These relays provide an output signal when the pump voltage goes below approximately 70 percent of rated voltage. Signals from these relays are time delayed to prevent spurious trips caused by short term voltage perturbations. The coincidence logic and interlocks are given in Table 7.2-1. The trip logic is shown on Figure 7.2-1, Sheet 3. 62

c. Reactor Coolant Pump Underfrequency Trip

There is no safety-related requirement for a direct trip of the RCP's for underfrequency. Credit is taken for reactor trip on underfrequency in the loss of flow accident. The reactor is tripped for an underfrequency on more than one reactor coolant pump motor (e.g. from a decay in grid frequency).

There is one underfrequency sensing relay for each pump motor connected at the load side of each reactor coolant pump breaker. These relays provide an output signal when the pump frequency decays to approximately 57 Hz. Signals from these relays are time delayed to prevent spurious trips caused by short term frequency perturbations. The coincidence logic and interlocks are given in Table 7.2-1. The trip logic is shown on Figure 7.2-1, Sheet 3. 62

The RCP breakers are not qualified to the criteria applicable to equipment performing a safety function.

The basis for not having qualified breakers is that the tripping of RCP's is not a safety function. Westinghouse topical report WCAP-8424 - "An Evaluation of Loss of Flow Accidents Caused by Power System Frequency Transients in Westinghouse PWR's," states in part that "... Westinghouse reactors are adequately protected for frequency of decay rates up to 5 Hz/sec. without taking credit for the RCP power supply breaker trip..." A TVA study performed in 1977 and described below determined the maximum system frequency decay rate to be less than 5 Hz/sec.

The Watts Bar Nuclear units are connected into the 500-kV bulk power transmission system as integral parts of TVA's total installed generating capacity. System loads are served

0794 PKG

with 1639 miles of 500-kV transmission line and 8906 miles of 161-kV transmission line. The 500- and 161-kV transmission systems are interconnected networks necessary for the distribution of power to concentrated area loads. A high percentage of the energy is supplied to area loads through 500-161-kV stepdown transformer banks connected to the bulk power transmission system.

Without advancing a hypothesis as to how the Watts Bar units could be islanded since there are no loads connected directly to 500-kV switchyards, it was necessary to open six 500-kV lines, twenty-three 161-kV lines, and to remove three operating units from the system to form an island to investigate frequency decay rates for a Watts Bar generator. All of the above conditions were imposed on the system without applying faults to the transmission grid. Because of the large number of simultaneous contingencies necessary ~~to the large number of simultaneous contingencies necessary~~ to form any island on the TVA transmission network so that loads exceed the generating capability of a Watts Bar Nuclear unit, the subsequent analysis is extremely conservative.

The simulated island used included 500-kV lines from Watts Bar to stepdown substations connected to the 500-kV bulk power transmission system so that loads within the island exceeded generation. With reasonable changes in load/generation ratios, changes in line charging MVA from open-ended 500-kV lines terminating within the island, and being cognizant that transmission facilities which are overly stressed above maximum design voltage ratings result in equipment failures and system faults to decrease frequency decay rates, maximum values of less than 5 Hz/sec. were calculated. Systems investigated included winter peak and summer offpeak conditions on the TVA system with actual loads and generation patterns identical to those which TVA uses for planning its future transmission facilities. 39

The only anticipatory trip input signal to the reactor protection system is in the reactor trip on turbine trip. This trip is anticipatory in that it is not assumed to occur in any of the Chapter 15 accident analysis. ~~As discussed in~~ Section 7.2.1.1.2 (item 6) describes how this trip meets ~~all of~~ the requirements of IEEE 279-1971 including separation, redundancy, and testability.

See reference [6] for an evaluation of loss of flow accidents caused by power system frequency transients in Westinghouse PWR's.

 0794 PKG

5. Steam Generator Trips 33

The specific trip functions generated are as follows:

a. Low feedwater flow trip

This trip protects the reactor from a sudden loss of heat sink. The trip is actuated by steam/feedwater flow mismatch (one out of two) in coincidence with low water level (one out of two) in any steam generator.

Figure 7.2-1, Sheet 3, shows the logic for this trip function. 52

There are no interlocks associated with this trip.

A detailed functional description of the process equipment associated with this function is provided in reference [1].

b. Low-low steam generator water level trip

This trip protects the reactor from loss of heat sink in the event of a sustained steam/feedwater flow mismatch of insufficient magnitude to cause a low feedwater flow reactor trip. This trip is actuated on two out of three low-low water level signals occurring in any steam generator.

The logic is shown on Figure 7.2-1, Sheet 3. A detailed functional description of the process equipment associated with this trip is provided in reference [1]. 52

I34

5. Low-Low Steam Generator Water Level Trip (including Trip Time Delay)

This trip protects the reactor from loss of heat sink in the event of a loss of feedwater to one or more steam generators or a major feedwater line rupture. This trip is actuated on two out of three low-low water level signals occurring in any steam generator. If a low-low water level condition is detected in one steam generator, signals shall be generated to trip the reactor and start the motor-driven auxiliary feedwater pumps. If a low-low water level condition is detected in two or more steam generators, a signal is generated to start the turbine-driven auxiliary feedwater pump as well.

The signals to actuate the reactor trip and start auxiliary feedwater pumps are delayed through the use of a Trip Time Delay (TTD) system for reactor power levels below 50% of RTP. Low-Low water level in any protection set in any steam generator will generate a signal which starts an elapsed time trip delay timer. The allowable trip time delay is based upon the prevailing power level at the time the low-low level trip setpoint is reached and the number of steam generators that are affected. If power level rises after the trip time delay setpoints have been determined, the trip time delay is re-determined (i.e., decreased) according to the increase in power level. At this point the timer will continue timing from the original timer initiation. However, the trip time delay setpoints are not increased if the power level decreases after the setpoints have been determined. The use of this delay allows added time for natural steam generator level stabilization or operator intervention to avoid an undesirable inadvertent protection system actuation.

The logic for this protective function is shown on Figure 7.2-1.

0794 PKG.

Figure 7.2-1, Sheet 1, shows the logic for this trip. A detailed functional description of the process equipment associated with this trip function is provided in references ~~[1]~~. [5] and [11]

8. Manual Trip

The manual trip consists of two switches with two outputs on each switch. One output is used to actuate the train A trip breaker, the other output actuates the train B trip breaker. Operating a manual trip switch removes the voltage from the undervoltage trip coil and energizes the shunt trip coil.

There are no interlocks which can block this trip. Figure 7.2-1, Sheet 2, shows the manual trip logic. 62

7.2.1.1.3 Reactor Trip System Interlocks

1. Power Escalation Permissivies

The overpower protection provided by the out of core nuclear instrumentation consists of three discrete, but overlapping, ranges. Continuation of startup operation or power increase requires a permissive signal from the higher range instrumentation channels before the lower range level trips can be manually blocked by the operator.

A one of two intermediate range permissive signal (P-6) is required prior to source range trip blocking and detector high voltage cutoff. Source range level trips are automatically reactivated and high voltage restored when both intermediate range channels are below the permissive (P-6) level. There are two manual reset switches for administratively reactivating the source range trip and detector high voltage when between permissive P-6 and P-10 if required. Source range trip block and high voltage cutoff are always maintained when above permissive P-10.

The intermediate range trip and power range (low setpoint) trip can only be blocked after satisfactory operation and permissive information are obtained from two of four power range channels. Four individual blocking switches are provided so that the low range power range trip and intermediate range trip can be independently blocked (one switch for each train). These trips are automatically reactivated when any three of the four power range channels are below permissive P-10 thus ensuring automatic activation to more restrictive trip protection.

0794 PKG

The development of permissives P-6 and P-10 is shown on Figure 7.2-1, Sheet 2. All of the permissives are digital; they are derived from analog signals in the nuclear power range and intermediate range channels.

See Table 7.2-2 for the list of protection system interlocks.

2. Blocks of Reactor Trips at Low Power

Interlock P-7 blocks a reactor trip at low power (below approximately 10 percent of full power) on a low reactor coolant flow in more than one loop, reactor coolant pump undervoltage, reactor coolant pump underfrequency, pressurizer low pressure, or pressurizer high water level. See Figure 7.2-1, Sheets 2 and 3 for permissive applications. The low power signal is derived from three out of four power range neutron flux signals below the setpoint in coincidence with two out of two turbine impulse chamber pressure signals below the setpoint (low plant load). See Figure 7.2-1, Sheet 2, for the derivation of P-7.

The P-8 interlock blocks a reactor trip when the plant is below approximately 48 percent of full power, on a low reactor coolant flow in any one loop. The block action (absence of the P-8 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-8 setpoint, the reactor will be allowed to operate with one inactive loop and trip will not occur until two loops are indicating low flow. See Figure 7.2-1, Sheet 3, for derivation of P-8 and applicable logic.

The P-9 interlock blocks a reactor trip when the plant is below approximately 50 percent of full power, on a turbine-tripped signal. The block action (absence of the P-9 interlock signal) occurs when three out of four neutron flux power range signals are below the setpoint. Thus, below the P-9 setpoint, the reactor will not trip directly from a turbine-tripped signal but will allow the reactor control system, utilizing steam dump to the condenser as an artificial load, to bring the reactor to zero power. See Figure 7.2-1, Sheet 2 for derivation of P-9 and Sheet 3 for logic applications.

See Table 7.2-2 for the list of protection system blocks.

APR

7.2.1.1.4 Reactor Coolant Temperature Sensor Arrangement and Calculational Methodology

The individual narrow range cold and hot leg temperature signals required for input to the reactor trip circuits and interlocks are obtained using RTDs installed in each reactor coolant loop.

The cold let leg temperature measurement on each loop is accomplished with two narrow range RTDs mounted in thermowells. The cold leg sensors are inherently redundant in that either sensor can adequately represent the cold leg temperature measurement. ~~Temperature streaming in the cold leg is not a concern due to the mixing action of the reactor coolant pump.~~

The hot leg temperature measurement on each loop is accomplished with three narrow range RTDs mounted in thermowells spaced 120 degrees apart around the circumference of the reactor coolant pipe for spatial variations.

These cold and hot leg narrow range RTD signals are input to the process protection system digital electronics and are processed as follows:

The two cold leg temperature signals are subjected to range and consistency checks and then averaged to provide a group value for T cold.

I15 ~~If either T cold input signal is out of range high or low, it will be set to the high or low limit respectively.~~ 63

Each of the three hot leg temperature signals is subjected to a range check, and utilized to calculate an estimated average hot leg temperature which is then consistency checked against the other two estimates for average hot leg temperature.

I16 ~~If any T hot input is out of range high or low, it will be set to the offscale high or low limit respectively. Next, an~~ The estimated average hot leg temperature is derived from each T hot input signal as follows:

$$\overline{T_{h_{ji}}} = T^{f}_{h_{ji}} - P_{B_i} S^{*}_{ji}$$ = ESTIMATED Thot AVERAGE

Where:

~~$T^{f}_{h_{ji}}$ is the filtered T hot signal for the jth RTD (j = 1 to 3) in the ith loop (i = 1 to 4)~~

P_{B_i} = power fraction being used to correct the bias value being used for any power level

$$P_{B_i} = (T^{f}_{h_{ave_i}} - T^{f}_{c_i})/\Delta T^{\circ}_i$$

A consistency check is performed on the T_{cold} input signals. If these signals agree within an acceptance interval (DELTAC), the group quality is set to GOOD. If the signals ~~so~~ do not agree within the acceptance tolerance DELTAC, the group quality is set to BAD and the individual signal qualities are set to POOR. The average of the two signals is used to represent the group in either case. If an input signal is manually disabled or subject to a diagnosed hardware failure, the group is represented by the active signal. DELTAC is a fixed input parameter based on operating experience. ~~Once~~ One DELTAC value is required for each loop/protection set.

The following parameters are used in conjunction with the Overtemperature Delta-T and Overpower Delta-T reactor trips:

T_{cji} ($j = 1, 2$; $i = 1$ to 4) = jth narrow range T_{cold} input signal from loop i

T^f_{cji} ($j = 1, 2$; $i = 1$ to 4) = Filtered T_{cold} signal for the jth RTD;
= $T_{cji}\,(1/(1 + \tau_7 s))$

τ_7 = Time constant utilized in the lag compensator for T_{cold}. Typically set to 0.0 secs.

T^f_{ci} ($i = 1$ to 4) = Group average of the valid input signals

= $(T^f_{c(j-1)i} + T^f_{cji})/2$ for two valid input signals

= T^f_{cji} for one valid input signal

where: $j = 1, 2$; and $i = 1$ to 4

s is defined in Section 7.2.1.1.2

signals

Then an average of the three estimated hot leg temperatures is computed and the individual signals are checked to determine if they agree within ±DELTAH of the average value. If all of the signal do agree within ±DELTAH of the average value, the group quality is set to GOOD. The group value ($T^f_{have,i}$) is set to the average of the three estimated average hot leg temperatures.

If the signal values do not all agree within ±DELTAH of the average, the algorithm will delete the signal value which is furthest from the average. The quality of this signal will be set to POOR and a consistency check will then be performed on the remaining GOOD signals. If these signals pass the consistency check, the group value will be taken as the average of these GOOD signals and the group quality will be set to POOR. However, if these signals again fail the consistency check (within ±DELTAH),then the group value will be set to the average of these two signals; but the group quality will be set to BAD. All of the individual signals will have their quality set to POOR. If one or two input signals is manually disabled or subject to a diagnosed hardware failure, the group value is based on the unaffected signal(s). DELTAH is a fixed input parameter based on temperature distribution tests with the hot leg and operating experience. One DELTAH value is required for each loop/protection set.

The following parameters are used in conjunction with the Overtemperature Delta-T and Overpower Delta-T reactor trips:

T_{hji} (j = 1 to 3; i = 1 to 4) = jth narrow range T_{hot} input signal from loop i

T^f_{hji} (j = 1 to 3; i = 1 to 4) = Filtered T_{hot} signal for the jth RTD;
= T_{hji} $(1/(1 + \tau_6 s))$

τ_6 = Time constant utilized in the lag compensator for T_{hot}. Typically set to 0.0 secs.

$T^f_{have,i}$ (i = 1 to 4) = Group average of the valid input signals

= $(T^f_{h(j-2)i} + T^f_{h(j-1)i} + T^f_{hji})/3$ for three valid input signals (j = 3)

= $(T^f_{h(j-1)i} + T^f_{hji})/2$ for two valid input signals (j = 2)

= $T^f_{h(j)i}$ for one valid input signal (j = 1)

where ~~j = 1 to 3 and~~ i = 1 to 4

0794 PKG

Where:

ΔT_i° ~~has been~~ is defined in the equation for Overtemperature Delta-T trip ~~is the full power ΔT in the ith loop~~ in Section 7.2.1.1.2, Subsections 2 and 3.

S_{ji}° = manually input bias which corrects the individual T hot RTD value to the loop average.

The individual temperature signals are subjected to a quality checking routine to establish a quality status of the group value.

ΔT and T_{ave} are calculated as follows:

$$\Delta T_i = T_h^f{}_{ave_i} - T_{c_i}^f$$ (temperature delta between hot leg and cold leg in loop i (i = 1 to 4))

$$T_{avg_i} = (T_h^f{}_{ave_i} + T_{c_i}^f)/2.0$$ (temperature delta between hot leg and cold leg in loop i (i = 1 to 4))

The calculated values for ΔT and T_{ave} are then utilized for both the remainder of the Overtemperature and Overpower ΔT protection channel and channel outputs for control purposes.

7.2.1.1.5 Pressurizer Water Level Reference Leg Arrangement

The design of the pressurizer water level instrumentation includes a slight modification of the usual tank level arrangement using differential pressure between an upper and a lower tap. The modification consists of the use of a sealed reference leg instead of the conventional open column of water. Refer to Section 7.2.2.3.4 for an analysis of this arrangement.

0794 PKG

7.2.1.1.6 Protection Process ~~Instrumentation~~ System

→ The process PROTECTION instrumentation system is described in references [1] and [11]. The Nuclear Instrument System is described in reference [2].

7.2.1.1.7 Solid State Logic Protection System

→ The Solid State Logic Protection System takes binary inputs (voltage/no voltage) from the process PROTECTION and nuclear instrument channels corresponding to conditions (normal/abnormal) of plant parameters. The system combines these signals in the required logic combination and generates a trip signal (no voltage) to the undervoltage coils and the shunt trip relays (which energize the shunt trip coils) of the reactor trip circuit breakers when the necessary combination of signals occur. The system also provides annunciator, status light and computer input signals which indicate the condition of ~~bistable~~ comparator input signals, partial trip and full trip functions and the status of the various blocking, permissive and actuation functions. In addition, the system includes means for semi-automatic testing of the logic circuits. A detailed description of this system is given in reference [3].

7.2.1.1.8 Isolation ~~Amplifiers~~ Devices

In certain applications, Westinghouse considers it advantageous to employ control signals derived from individual protection channels through isolation devices ~~amplifiers~~ contained in the protection channel, as permitted by IEEE Standard 279-1971.

In all of these cases, signals derived from protection channels for non-protective functions are obtained through isolation devices ~~amplifiers~~ located in the process ~~the~~ protection ~~instrumentation~~ racks. By definition, non-protective functions include those signals used for control, remote process indication, and computer monitoring.

Isolation device ~~amplifier~~ qualification type tests are described in references [7] [8], and [11].

7.2.1.1.9 Energy Supply and Environmental Variations

The energy supply for the Reactor Trip System is described in Chapter 8. The environmental variations, throughout which the system will perform, ~~is~~ are given in Section 3.11 and Chapter 8.

7.2.1.1.10 Setpoints

The setpoints that require trip action are given in the Technical Specifications.

I17

As documented in Reference 7, testing was performed on the Eagle 21 Process Protection System to demonstrate that the Eagle 21 system remained operational before, during and after applied noise, fault, surge withstand, electro-magnetic interference (EMI) and Radiated Frequency Interference (RFI) operating conditions. Objectives accomplished by the test demonstrated that the physical independence of the class non-1E and Class 1-E circuitry was maintained and that the system was designed to withstand worst-case noise environment conditions.

0794 PKG

7.2.1.1.11 Seismic Design

The seismic design considerations for the Reactor Trip System are given in Section 3.10. This design meets the requirements of Criterion 2 of the 1971 General Design Criteria (GDC).

7.2.1.2 Design Bases Information

The information given below presents the design bases information requested by Section 3 of IEEE Standard 279-1971, reference [9]. The reactor trip logic is presented in Figure 7.2-1 Sheets 1 through 3. 62

7.2.1.2.1 Generating Station Conditions

The following are the generating station conditions requiring reactor trip.

1. DNBR approaching 1.30.

2. Power density (kilowatts per foot) approaching rated value for Condition II faults (See Chapter 4 for fuel design limits).

3. Reactor Coolant System overpressure creating stresses approaching the limits specified in Chapter 5.

7.2.1.2.2 Generating Station Variables

The following are the variables required to be monitored in order to provide reactor trips (see Table 7.2-1).

1. Neutron flux

2. Reactor coolant temperature

3. Reactor Coolant System pressure (pressurizer pressure)

4. Pressurizer water level

5. Reactor coolant flow

6. Reactor coolant pump bus voltage and frequency

~~7. Steam generator feedwater flow~~

7 ~~8~~. Steam generator water level

0794 PKG

~~9. Steam generator steam flow~~

8 ~~10~~. Turbine-generator operational status (autostop oil pressure and stop valve position).

7.2.1.2.3 Spatially Dependent Variables

The following variable is spatially dependent:

1. Reactor coolant temperature: See Section 7.3.1.2.3 for a discussion of this variable spatial dependence. 52

7.2.1.2.4 Limits, Margins and Levels

The parameter values that will require reactor trip are given in the Technical Specifications and in Chapter 15, Accident Analyses. Chapter 15 proves that the setpoints used in the Technical Specifications are conservative. 52

The setpoints for the various functions in the Reactor Trip System have been analytically determined such that the operational limits so prescribed will prevent fuel rod clad damage and loss of integrity of the Reactor Coolant System as a result of any ANS Condition II incident (anticipated malfunction). As such, during any ANS Condition II incident, the Reactor Trip System limits the following parameters to:

1. Minimum DNBR = 1.3

2. Maximum system pressure = 2750 psia

3. Fuel rod maximum linear power for determination of protection setpoints = 18.0 kw/ft

The accident analyses described in Section 15.2 demonstrate that the functional requirements as specified for the Reactor Trip System are adequate to meet the above considerations, even assuming, for conservatism, adverse combinations of instrument errors (Refer to Table 15.1-3). A discussion of the safety limits associated with the reactor core and Reactor Coolant System, plus the limiting safety system setpoints, are presented in the technical specifications. The technical specifications ~~will~~ incorporate both nominal and limiting setpoints. ~~Instrument spans are selected such that limiting setpoints are at least 5% from the end of the instrument span.~~ Nominal settings of the setpoints are more conservative than the limiting settings. This allows for calibration uncertainty

0794 PKG

and instrument channel drift without violating the limiting setpoint. Automatic initiation of protective functions occurs at the nominal setpoints (plus or minus the allowed tolerances). 35
A further discussion on trip setpoints is given in Section 7.2.2.1.1.

The methodology used to derive the setpoints is documented in reference 13.

7.2.1.2.5 Abnormal Events

The malfunctions, accidents or other unusual events which could physically damage Reactor Trip System components or could cause environmental changes are as follows:

1. Earthquakes (See Chapters 2 and 3).

2. Fire (See Section 9.5 and the September 8, 1980, fire protection submittal to NRC from TVA) 44 52

3. Explosion (hydrogen buildup inside containment). (See Section 6.2).

4. Missiles (See Section 3.5).

5. Flood (See Chapters 2 and 3).

6. Wind and Tornadoes (See Section 3.3).

The Reactor Trip System fulfills the requirements of IEEE Standard 279-1971 to provide automatic protection and to provide initiating signals to mitigate the consequences of faulted conditions. The Reactor Trip System provides protection against destruction of the system from fires, explosions, floods, wind, and tornadoes (see each item above). The discussions in Section 7.1.2.1.7 and this section adequately address or reference the Safety Analysis Report coverage of the affects of abnormal events, on the Reactor Trip System in conformance with applicable General Design Criteria.

7.2.1.2.6 Minimum Performance Requirements

1. Reactor Trip System response times

   Reactor Trip System response time is defined in Section 7.1. Typical maximum allowable time delays in generating the reactor trip signal are tabulated in Table 7.2-3. (See Table 7.1-1 Note 1 for a discussion of periodic response time verification capabilities.)

2. Reactor trip accuracies

0794 PKG

Accuracy is defined in Section 7.1. Typical reactor trip accuracies are tabulated in Table 7.2-3. 52

3. Protection System ranges

Typical Protection System ranges are tabulated in Table 7.2-3.

7.2.1.3 Final Systems Drawings

Functional block diagrams, electrical elementaries and other drawings required to assure electrical separation and perform a safety review are provided in Section 1.7. 24

7.2.2 Analyses

I18

A failure mode and effects analysis (FMEA) of the logic portion of the Reactor Trip System has been performed. 52 The basis of the FMEA is that the reactor protection system is designed to sense abnormal plant conditions and to initiate action necessary to assure that acceptable fuel design limits are not exceeded for anticipated operational occurrences. Results of this study and a fault tree analysis are presented in reference [4]. 41 The results of the study show that the probability of protection system failure in anticipated transient is sufficiently low that no provision need be made in plant design to accommodate such hypothetical failure.

7.2.2.1 Evaluation of Design Limits

While most setpoints used in the Reactor Protection System are fixed, there are variable setpoints, most notably the overtemperature ΔT and overpower ΔT~~, and steam generator water level low and low-low setpoints?~~ All setpoints in the Reactor Trip System have been selected on the basis of engineering design or safety studies. The capability of the Reactor Trip System to prevent loss of integrity of the fuel cladding and/or Reactor Coolant System pressure boundary during Condition II and III transients is demonstrated in Chapter 15. These accident analyses are carried out using those setpoints determined from results of the engineering design studies. Setpoint limits are presented in the technical specifications. ~~A~~ discussion of the intent for each of the various reactor trips and the accident analyses (where appropriate) which utilizes this trip is presented below. ~~It should be noted that~~ The selection of trip setpoints ~~all~~ provides for margin before protection action is actually required to allow for uncertainties and instrument errors (Reference 13). The design meets the requirements of Criteria 10 and 20 of the 1971 GDC.

7.2.2.1.1 Trip Setpoint Discussion

It has been pointed out previously that below a DNBR of 1.30 there is likely to be significant local fuel cladding failure. The DNBR existing at any point in the core for a given core

Insert 18 to Page 7.2-19

A reliability study for the reactor trip and engineered safety features function of the Eagle 21 process protection system hardware has been performed. The basis for this study was to compare the availability of the Eagle 21 digital system with the existing implementation of the same function using analog hardware. Availability is defined as the probability of a system to perform its intended function (e.g., actuate a partial trip) at a randomly selected instant in time. Results of the availability study determined that the Eagle 21 digital system is commensurate with an equivalent analog process protection system availability although no credit was given to the Eagle 21 process protection features of automatic surveillance testing, self calibration and self diagnostics when the study was performed. It is expected that if credit were given to the Eagle 21 self diagnostic features (EPSOM checksums, RAM checks, Math Co-Processor checks and Loop Cycle Time checks), automatic surveillance testing and self calibration capabilities, system availability would be improved. Therefore, the impact on the system operation due to channel drift being corrected by the Eagle 21 self-calibration feature and the impact on system downtime because of the automatic surveillance/self-diagnostic features, will be minimized. Additionally, with the MMI test unit provided with the Eagle 21 system, the amount of technician and engineering time required for maintenance and troubleshooting will be minimized. Thus, large quantities of engineering time required for the review of the quarterly functional tests, prior to restoring the channel to an operable condition, is eliminated because of the user-friendly printout provided from the MMI. In total, interface with the Eagle 21 process protection system will be reduced, resulting in a decreased potential for technician induced error which results in improved system reliability and availability.

In the Eagle 21 process protection system design, there are failure modes which could result in the failure of an entire protection rack. During these conditions, the rack will fail to the preferred failure mode (tripped/not tripped condition) providing maximum protection for the plant. The failure of a single rack is considered to be bounded by the loss of an entire protection set, which is the existing licensing basis. This failure has been shown not to adversely impact plant safety due to the existence of redundancy, functional diversity and defense-in-depth design measure employed in the design of the process protection system. Use of these design measures ensures that in the event of a single failure, the remaining protection system channels would be available for plant protection if required. Additional discussion of the defense-in-depth, redundancy and functional diversity design measures used in the design of the Eagle 21 process protection system can be found in References [5] and [14].

the corresponding technical specification on safety limits and safety system settings and the appropriate accident discussed in the safety analyses in which the trip could be utilized.

It should be noted that the Reactor Trip System automatically provides core protection during non-standard operating configuration, i.e. operation with a loop out of service. Although operating with a loop out of service over an extended time is considered to be an unlikely event, no protection system setpoints need to be reset. This is because the nominal value of the power (P-8) interlock setpoint restricts the power levels such that DNB ratios less than 1.30 will not be realized during any Condition II transients occurring during this mode of operation. This restricted power level is considerably below the boundary of permissable values as defined by the core safety limits for operation with a loop out of service. Thus the P-8 interlock acts essentially as a high nuclear power reactor trip when operating with one loop not in service. By first resetting the coefficient setpoints in the overtemperature ΔT function to more restrictive values as listed in the technical specifications, the P-8 setpoint can then be increased to the maximum value consistent with maintaining DNBR above 1.30 for Condition II transients in the one loop shutdown mode. The resetting of the ΔT overtemperature trip and P-8 will be carried out under prescribed administrative procedures and only under the direction of authorized supervision with the plant in a hot shutdown condition.

The Reactor Trip System design was evaluated in detail with respect to common mode failure and is presented in references [4] and [5]. The design meets the requirements of Criterion 21 of the 1971 GDC.

Preoperational testing is performed on Reactor Trip System components and systems to determine equipment readiness for startup. This testing serves as a further evaluation of the system design.

Analyses of the results of Condition I, II, III and IV events, including considerations of instrumentation installed to mitigate their consequences are presented in Chapter 15. The instrumentation installed to mitigate the consequences of load rejection and turbine trip is given in Section 7.4.

7.2.2.1.2 <u>Reactor Coolant Flow Measurement</u>

The elbow taps used on each loop in the primary coolant system are instrument devices that are used to indicate the status of the reactor coolant flow. The basic function of this measurement is to provide information as to whether or not a reduction in flow has occurred. The correlation between flow and elbow tap signal is given by the following equation:

$$\frac{\Delta P}{\Delta P_o} = \left(\frac{w}{w_o}\right)^2,$$

where ΔP_o is the pressure differential at the reference flow w_o, and ΔP is the pressure differential at the corresponding flow, w. The full flow reference point is established during initial plant startup. The low flow trip point is then established by extrapolating along the correlation curve. The expected absolute accuracy of the channel is within $\pm$ 10 percent of full flow and field results have shown the repeatability of the trip point to be within $\pm$ 1 percent.

7.2.2.1.3 Evaluation of Compliance to Applicable Codes and Standards

The Reactor Trip System meets the criteria of the General Design Criteria as indicated. The Reactor Trip System meets the requirements of Section 4 of IEEE Standard 279-1971, reference [9], as indicated below.

1. General Functional Requirement

   The Protection System automatically initiates appropriate protective action whenever a condition monitored by the system reaches a preset value. Functional performance requirements are given in Section 7.2.1.1.1. Section 7.2.1.2.4 presents a discussion of limits, margins and setpoints; Section 7.2.1.2.5 discusses unusual (abnormal) events; and Section 7.2.1.2.6 presents minimum performance requirements.

2. Single Failure Criterion

   The Protection process protection System is designed to provide two, three, or four ~~instrumentation~~ channels for each protective function and two logic train circuits. These redundant channels and trains are electrically isolated and physically separated. Thus, any single failure within a channel or train will not prevent protective system action when required. Loss of input power, the most likely mode of failure, to a channel or logic train will result in a signal calling for a trip. This design meets the requirements of Criterion 23 of the 1971 GDC.

To prevent the occurrence of common mode failures, such additional measures as functional diversity, physical separation, and testing as well as administrative control during design, production, installation and operation are employed, as discussed in reference [4]. The design meets the requirements of Criteria 21 and 22 of the 1971 GDC.

3. Quality of Components and Modules

For a discussion on the quality of the components and modules used in the Reactor Trip System, refer to Chapter 17. The quality assurance applied conforms to Criterion 1 of the 1971 GDC.

4. Equipment Qualification

For a discussion of the type tests made to verify the performance requirements, refer to Section 3.11. The test results demonstrate that the design meets the requirements of Criterion 4 of the 1971 GDC.

5. Channel Integrity

Protection System channels required to operate in accident conditions maintain necessary functional capability under extremes of conditions relating to environment, energy supply, malfunctions, and accidents. The energy supply for the Reactor Trip System is described in Chapter 8. The environmental variations, throughout which the system will perform is given in Section 3.11.

6. Independence

Channel independence is carried throughout the system, extending from the sensor through to the devices actuating the protective function. 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 channels are
redundant channel. Redundant protection ~~instrumentation equipment is~~ separated by locating ~~modules~~ in different protection ~~cabinets.~~ Each redundant protection channel set is energized from a separate AC power feed. This design meets the requirements of Criterion 21 of the 1971 GDC. 63
the processing electronics of the redundant channels
channel rack sets.

Independence of the logic trains is discussed in reference[3]. Two reactor trip breakers are actuated by two separate logic matrices which interrupt power to the control rod drive mechanisms. The breaker main contacts are connected in series with the power supply so that opening either breaker interrupts power to all ~~full length~~ control rod drive mechanisms, permitting the rods to free fall into the core. See Figure 7.1-1.

The design philosophy is to make maximum use of a wide variety of measurements. The Protection System continuously monitors numerous diverse system variables. The extent of this diversity has been evaluated for a wide variety of postulated accidents and is discussed in reference [5]. Generally, two or more diverse protection functions would terminate an accident before intolerable consequences could occur. This design meets the requirements of Criterion 22 of the 1971 GDC.

7. Control and Protection System Interaction

The Protection System is designed to be independent of the Control System. In certain applications the control signals and other non-protective functions are derived from individual protective channels through isolation ~~amplifiers~~. The isolation ~~amplifiers~~ are classified as part of the Protection System and are located in the process protection ~~instrumentation~~ racks. Non-protective functions include those signals used for control, remote process indication, and computer monitoring. The isolation ~~amplifiers~~ are designed such that a short circuit, open circuit, or the application of credible fault voltages ~~from within the cabinets~~ on the isolated output portion of the circuit (i.e., the non-protective side of the circuit) will not affect the input (protective) side of the circuit. The signals obtained through the isolation ~~amplifiers~~ are never returned to the ~~protective~~ racks. This design meets the requirements of Criterion 24 of the 1971 GDC and paragraph 4.7 of IEEE Standard 279-1971, reference [9]. 63

devices

Process protection

A detailed discussion of the design and testing of the protection system ~~instrumentation~~ isolation ~~amplifiers~~ are given in references [7], [8], and [11]. These reports include the results of applying various malfunction conditions on the output portion of the isolation ~~amplifiers~~. The results show that no significant disturbance to the isolation ~~amplifier~~ input signal occurred. 63

devices

Add

Where failure of a protection system component can cause a process excursion which requires protective action, the protection system can withstand another, independent failure without loss of protective action. This is normally achieved by means of two-out-of-four (2/4) trip logic for each of the protective functions except Steam Generator Protection. The Steam Generator Low Water Level protective function relies upon two-out-of-three (2/3) trip logic and a control system Median Signal Selector (MSS). The use of a control system MSS prevents any protection system failure from causing a control system reaction resulting in a need for subsequent protective action. This meets the requirements of Criterion ~~25~~ 24 of the 1971 GDC.

8. Derivation of System Inputs

To the extent feasible and practical, Protection System inputs are derived from signals which are direct measures of the desired variables. Variables monitored for the various reactor trips are listed in Section 7.2.1.2.2.

9. Capability for Sensor Checks

The operational availability of each system input sensor during reactor operation is accomplished by cross checking between channels that bear a known relationship to each other and that have read-outs available. Channel checks are discussed in the Technical Specifications.

10. Capability for Testing

The Reactor Trip System is capable of being tested during power operation. Where only parts of the system are tested at any one time, the testing sequence provides the necessary overlap between the parts to assure complete system operation. The testing capabilities are in conformance with Regulatory Guide 1.22 as discussed in Table 7.1-1.

TVA will conduct tests to determine that the Reactor Trip System instrumentation and engineered safety feature response times (excluding the nuclear instrumentation channels and/or sensors), including the sensor, are less than or equal to those response times specified in the Technical Specifications. These tests will be conducted for both the preoperational tests and at the periodic tests specified in the Technical Specifications. 62

The Protection System is designed to permit periodic testing of the process protection ~~instrumentation~~ channel portion of the Reactor Trip System during reactor power operation without initiating a protective action unless a trip condition actually exists. This is because of the coincidence logic required for reactor trip. These tests may be performed at any plant power from cold shutdown to full power. Before starting any of these tests with the plant at power, all redundant reactor trip channels associated with the function to be tested must be in the normal (untripped) mode in order to avoid spurious trips. Setpoints are ~~referenced in the precautions, limitations and setpoints portion of the plant technical manual~~ documented in Reference 13 and incorporated into the Technical Specifications. 63

0794 PKG

~~Analog Channel Tests~~

~~Analog channel testing is performed at the protection instrumentation channel rack set by individually introducing dummy input signals into the instrumentation channels and observing the tripping of the appropriate output bistables. Output to the logic circuitry is interrupted during individual channel test by a test switch which, when thrown, de-energizes (except containment spray, which energizes) the associated logic input and inserts a proving lamp in the bistable output. Interruption of the bistable output to the logic circuitry for any cause (test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated (partial trip) accompanied by a partial trip alarm and channel status light actuation in the control room. Each channel contains those switches, test points, etc. necessary to test the channel. See Reference [1] for additional information.~~ 63

~~Digital Channel Tests~~

~~Automatic digital channel testing is performed at the digital protection instrumentation racks via a portable Man Machine Interface (MMI) terminal. The portable MMI terminal is connected to the protection instrumentation rack by inserting a connector into the protection instrumentation test panel. Using the MMI touch screen, the "Surveillance Test" option will be selected. Following instructions entered through the MMI, the rack test processor will automatically perform the tests. The MMI provides a printout of the test results.~~

IA

~~"Channel Trip" or interruption of the bistable output to the logic circuitry for any reason (test, maintenance purposes, or removed from service) will cause that portion of the logic to be actuated and accompanied by a channel trip alarm and channel status light actuation in the control room. Each channel is fully testable via the portable MMI terminal.~~ 63

Nuclear Instrumentation Channel Tests

The power range channels of the Nuclear Instrumentation System are tested by using the actual detector input to the channel and injecting test currents obtained from the detector response curves at various power levels. The output of the bistable is not placed in a tripped condition prior to testing. Also, since the power range channel logic is two out of four, bypass of this reactor trip function is not required.

To test a power range channel, a "Operation Selector" switch is provided to require deliberate operator action and operation of

Process Protection Channel Tests

The Eagle 21 Process Protection System accommodates automatic or manual surveillance testing of the digital process protection racks via a portable Man Machine Interface (MMI) test cart. The MMI test cart is connected to the process rack by inserting a cable/connector assembly into the process rack test panel. The rack installed test processor permits performance of operations such as channel calibration, channel response time tests, partial trip actuation tests, and maintenance activities. Administrative controls and multiple levels of security are provided to limit access to setpoint and tuning constant adjustments. The system is designed to permit testing of any protection channel during power operations without initiating a protective action at the systems level.

Individual channels can be tested in either the "Channel Trip" or "Bypass" mode:

The Channel Trip mode interrupts the individual channel comparator output. Interruption of a comparator output in this mode for any reason (test, maintenance purposes or removed from service) causes that portion of the logic to be actuated and initiates a channel trip alarm and status light in the control room. Status lights on the process rack test panel indicate when the associated comparators have tripped.

The Bypass mode disables the individual channel comparator trip circuitry. Interruption of a comparator output in this mode effectively "bypasses" the channel in test causing the associated logic relays to remain in the non-tripped state until the "bypass" is removed. This feature of the protection system eliminates the potential for an unwarranted actuation in the event of a failure. This condition is also accompanied by an alarm in the control room.

~~channel~~ protection system channel ~~instrumentation~~ testing is complete, the logic matrices are tested from the train A and train B logic rack test panels. This ~~stop~~ step provides overlap between the channelized process protection ~~instrumentation~~ system and trained logic portions of the test program. During this test, all of the logic inputs are actuated automatically in all combinations of trip and non-trip logic. Trip logic is not maintained sufficiently long enough to permit opening of the reactor trip breakers. The reactor trip undervoltage coils are 'pulsed' in order to check continuity. During logic testing of one train, the other train can initiate any required protective functions. Annunciation is provided in the control room to indicate when a train is in test (train output bypassed) and when a reactor trip breaker is bypassed. Logic testing can be performed in less than 30 minutes. Details of the logic system testing are given in reference [3]. 63

A direct reactor trip resulting from undervoltage or underfrequency on the pump side of the reactor coolant pump breakers is provided as discussed in Section 7.2.1 and shown on Figure 7.2-1. The logic for these trips is capable of being tested during power operation. When parts of the trip are being tested, the sequence is such that an overlap is provided between parts so that a complete logic test is provided.

This design complies with the testing requirements of IEEE Standard 279-1971 and IEEE Standard 338-1971 discussed in Table 7.1-1. Details of the method of testing and compliance with these standards are provided in references [1], [3], and [11]. 63

The permissive and block interlocks associated with the Reactor Trip System and Engineered Safety Features Actuation System are given on Tables 7.2-2 and 7.3-3 and designated protection or 'P' interlocks. As a part of the protection system, these interlocks are designed to meet the testing requirements of IEEE Standards 279-1971 and 338-1971.

Testability of the interlocks associated with reactor trips for which credit is taken in the accident analyses is provided by the logic testing and semi-automatic testing capabilities of the Solid State Protection System. In the Solid State Protection System the undervoltage coils (Reactor Trip) and master relays (Engineered Safeguards Actuation) are pulsed for all combinations of trip or actuation logic with and without the interlock signals. For example reactor trip on low flow (2 out of 4 loops showing 2 out of 3 low flow) is tested to verify operability of the trip above P-7 and non-trip below P-7. (See Figure 7.2-1, Sheet 3) Interlock testing may be performed at power.

0794 PKG.

Testing of the logic trains of the Reactor Trip System includes a check of the input relays and a logic matric check. The following sequence is used to test the system:

1) Check of input relays

comparator/bistable protection

During testing of the process ~~instrumentation~~ system and nuclear instrumentation system channels, each channel ~~bistable~~ is placed in a trip mode causing one input relay in train A and one in train B to de-energize. A contact of each relay is connected to a universal logic printed circuit card. This card performs both the reactor trip and monitoring functions. Each reactor trip input relay contact causes a status lamp and an annunciator on the control board to operate. Either the Train A or Train B input relay operation will light the status lamp and annunciator.

Each train contains a multiplexing test switch. Train A is normally operated in the A + B position and train B in the normal position. This allows information to be 52
transmitted to the control intervals. A steady status lamp indicates that both trains are receiving a trip mode logic input for the channel being tested. A flashing lamp indicates a failure in one train. Contact inputs to the logic protection system such as reactor coolant pump bus underfrequency relays operate input relays which are tested by operating the remote contacts as described above and using the same type of indications as those provided for comparator/bistable input relays.

Actuation of the input relays provides the overlap between the testing of the logic protection system and the testing of those systems supplying the inputs to the logic protection system. Test indications are status lamps and annunciators on the control board. Inputs to the logic protection system are checked one channel at a time, leaving the other channels in service. For example, a function that trips the reactor when two out of four channels trip becomes a one out of three trip when one channel is placed in the trip mode. Both trains of the logic protection system remain in service during this portion of the test.

' 0794 PKG

2) Check of logic matrices

Logic matrices are checked one train at a time. Input relays are not operated during this portion of the test. Reactor trips from the train being tested are inhibited with the use of the input error inhibit switch on the semi-automatic test panel in the train. Details of semi-automatic tester operation are given in reference [3]. At the completion of the logic matrix tests, one comparator ~~bistable~~ in each channel of the process ~~instrumentation~~ protection system or nuclear instrumentation is tripped to check closure of the input error inhibit switch contacts.

The logic test scheme uses pulse techniques to check the coincidence logic. All possible trip and non trip combinations are checked. Pulses from the tester are applied to the inputs of the universal logic card at the same terminals that connect to the input-relay contacts. Thus there is an overlap between the input relay check and the logic matrix check. Pulses are fed back from the reactor trip breaker undervoltage coil to the tester. The pulses are of such short duration that the reactor trip breaker undervoltage coil armature cannot respond mechanically.

Test indications that are provided are an annunciator in the control room indicating that reactor trips from the train have been blocked and that the train is being tested, and green and red lamps on the semi-automatic tester to indicate a good or bad logic matrix test. Protection capability provided during this portion of the test is from the train not being tested.

The general design features and details of the testability of the logic system are described in reference [3]. The testing capability meets the requirements of Criterion 21 of the 1971 GDC.

Testing of Reactor Trip Breakers

Normally, reactor trip breakers 52/RTA and 52/RTB are in service, and bypass breakers 52/BYA and 52/BYB are withdrawn (out of service). In testing the protection logic, pulse techniques are used to avoid tripping the reactor trip breakers thereby eliminating the need to bypass them during this testing. The following procedure describes the method used for testing the trip breakers:

1. With bypass breaker 52/BYA racked out, manually close and trip it to verify its operation.

0794 PKG

2. Rack in and close 52/BYA. Manually trip 52/RTA through protection system logic matrix.

3. Reset 52/RTA.

4. Trip and rack out 52/BYA.

5. Repeat above steps to test trip breaker 52RTB using bypass breaker 52/BYB.

Auxiliary contacts of the bypass breakers are connected into the alarm system of their respective trains such that if either train is placed in test while the bypass breaker of the other train is closed, both reactor trip breakers and both bypass breakers will automatically trip.

Auxiliary contacts of the bypass breakers are also connected in such a way that if an attempt is made to close the bypass breaker in one train while the bypass breaker of the other train is already closed, both bypass breakers and both reactor trip breakers will automatically trip.

The Train A and Train B alarm systems operate separate annunciators in the control room. The two bypass breakers also operate an annunciator in the control room. Bypassing of a protection train with either the bypass breaker or with the test switches will result in audible and visual indications.

The complete Reactor Trip System is normally required to be in service. However, to permit online testing of the various protection channels or to permit continued operation in the event of a subsystem instrumentation channel failure, the Technical Specifications define the minimum number of operable channels. The Technical Specifications also define the required restriction to operation in the event that the channel operability requirements cannot be met. 63

11. Channel Bypass or Removal from Operation

The ~~Protection~~ System is designed to permit periodic testing of the protection instrumentation channel ~~portion~~ of the Reactor Trip System during reactor power operation without initiating a ~~protective~~ action unless a trip condition actually exists. This is because of the coincidence logic ~~required~~ for reactor trip. 63

I20

0794 PKG

Insert 20 to Page 7.2-31

The Eagle 21 Process Protection System is designed to permit any channel to be maintained in a Bypassed condition, and when required, tested during power operation without initiating a protective action at the systems level. This is accomplished without lifting electrical leads or installing temporary jumpers. If a channel in an Eagle 21 protection system rack has been bypassed for any purpose, a signal (1 per protection set) is provided to allow this condition to be continuously indicated in the control room. In addition, the Eagle 21 design has provided for administrative controls and multiple levels of security for bypassing a protection channel.

The Channel Bypass feature of the ~~Watts Bar Unit 1~~ Eagle 21 system will be used for the following purposes:

1. To allow for an inoperable Reactor Trip (RT) or Engineered Safety Features Actuation System (ESFAS) channel to be maintained in a Bypassed condition up to six hours for the purpose of troubleshooting,

2. To allow for a failed RT or ESFAS Channel to be Bypassed up to four hours for the purpose of surveillance testing a redundant channel of the same function,

3. To routinely allow testing of a RT or ESFAS Channel in the Bypassed condition instead of the tripped condition for the purpose of surveillance testing,

The Nuclear Instrumentation System (NIS) is designed to permit routine periodic testing of the Source Range and Intermediate Range portion of the Reactor Trip system during reactor power operation. To enable testing of the one-out-of-two channel logic for the NIS Source Range and Intermediate Range during reactor power operation, a channel bypass feature has been provided. Use of this feature will permit routine required surveillance testing to be completed without initiating a protective action unless a trip condition exists.

0794 PKG

12. Operating Bypasses

Where operating requirements necessitate automatic or manual bypass of a protective function, the design of the protection system is such that the bypass is removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are considered part of the protection system and are designed in accordance with the criteria of this section. Indication is provided in the control room if some part of the system has been administratively bypassed or taken out of service. ~~The protection system has the capability for testing one channel in bypass, with the bypass remaining in effect until completion of testing.~~ 63

13. Indication of Bypasses

INSERT 21 → ~~Bypass indication is discussed in Table 7.1-1, Note 5.~~

14. Access to Means for Bypassing

The design provides for administrative control of access to the means for manually bypassing channels or protective functions. For details, refer to referen~~ces~~ [1] and [11]. 63

15. Multiple Setpoints

For monitoring neutron flux, multiple setpoints are used. When a more restrictive trip setting becomes necessary to provide adequate protection for a particular mode of operation or set of operating conditions, the protective system circuits are designed to provide positive means or administrative control to assure that the more restrictive trip setpoint is used. The devices used to prevent improper use of less restrictive trip settings are considered part of the protective system and are designed in accordance with the criteria of this section.

16. Completion of Protective Action

The protection system is so designed that, once initiated, a protective action goes to completion. Return to normal operation requires action by the operator.

17. Manual Initiation

Switches are provided on the control board for manual initiation of protective action. Failure in the automatic system does not prevent the manual actuation of the protective functions. Manual actuation relies on the operation of a minimum of equipment.

Insert 21 to Page 7.2-32

Bypass of a process protection channel during testing is indicated by an alarm in the control room. This is discussed further in Section 7.2.2.1.3., subsections 10 and 11.

0794 PKG

18. Access

The design provides for administrative control of access to all setpoint adjustments, processing electronics ~~module~~ calibration adjustments, and test points. For details refer to reference [1], [2], and [11].

19. Identification of Protective Actions

Protective channel identification is discussed in Section 7.1.2.3. Indication is discussed in Item 20 below.

20. Information Read Out

The protective system provides the operator with complete information pertinent to system status and safety. All transmitted signals (flow, pressure, temperature, etc.) which can cause a reactor trip will be either indicated or recorded for every channel, including all neutron flux power range currents (top detector, bottom detector, algebraic difference and average of bottom and top detector currents).

Any reactor trip will actuate an alarm and an annunciator. Such protective actions are indicated and identified by the parameter being measured.

Alarms and annunciators are also used to alert the operator of deviations from normal operating conditions so that he may take appropriate corrective action to avoid a reactor trip. Actuation of any rod stop or trip of any reactor trip channel will actuate an alarm.

21. System Repair

The system is designed to facilitate the recognition, location, replacement, and repair of malfunctioning components or modules. Refer to the discussion in Item 10 above.

7.2.2.3 Specific Control and Protection Interactions

7.2.2.3.1 Neutron Flux

Four power range neutron flux channels are provided for overpower and overtemperature ΔT protection. An isolated auctioneered high signal is derived by auctioneering of the four channels for automatic rod control. If any channel fails in such a way as to produce a low output, that channel is incapable of proper overpower or overtemperature delta-T protection but will not cause control rod movement because of the auctioneer. Two out of four overpower or overtemperature delta-T trip logic will ensure overpower or overtemperature delta-T trip if needed even with an independent failure in another channel.

In addition, channel deviation signals in the control system will give an alarm if any neutron flux channel deviates significantly from the average of the flux signals. Also, the control system will respond only to rapid changes in indicated neutron flux; slow changes or drifts are compensated by the temperature control signals. Finally, an overpower or overtemperature delta-T signal from any two nuclear power range channels will block manual and automatic rod withdrawal. The setpoint for this rod stop is below the reactor trip setpoint.

7.2.2.3.2 Reactor Coolant Temperature

The accuracy of the narrow range resistance temperature detector loop temperature measurements is demonstrated during plant startup tests by comparing temperature measurements from the narrow range resistance 63
temperature detectors with one another as well as with the temperature measurements ~~obtained~~ from the wide range resistance temperature detectors located in the hot leg and cold leg piping of each loop. The comparisons ~~are~~ done with the Reactor Coolant System in an isothermal condition. The linearity of the delta-T measurements obtained from the hot leg and cold leg narrow 63
range loop resistance temperature detectors as a function of plant power is also checked during plant startup tests. The absolute value of delta-T versus plant power is not important, per se, as far as reactor protection is concerned. Reactor Trip System setpoints are based upon percentages of the indicated delta-T at nominal full power rather than on absolute values of delta-T. This is done to account for loop differences which are inherent. Therefore the percent delta-T scheme is relative, not absolute, and therefore provides better protective action without the expense of accuracy. For this reason, the linearity of the delta-T signals as a function of power is of importance rather than the absolute values of the delta-T. As part of the plant startup tests, the narrow range resistance temperature detector signals 63
will be compared with the core exit thermocouple signals.

Reactor control is based upon signals derived from protection system channels after isolation by isolation ~~amplifiers~~ such that no feedback effect from the control system can perturb the protection channels.

devices

0794 PKG

Overpressure protection is based upon the positive surge of the reactor coolant produced as a result of turbine trip under full load, assuming the core continues to produce full power. The self-actuated safety valves are sized on the basis of steam flow from the pressurizer to accommodate this surge at a setpoint of 2500 psia and an accumulation of 3%. Note that no credit is taken for the relief capability provided by the power-operated relief valves during this surge.

In addition, operation of any one of the power-operated relief valves can maintain pressure below the high pressure trip point for most transients. The rate of pressure rise achievable with heaters is slow, and ample time and pressure alarms are available to alert the operator of the need for appropriate action.

7.2.2.3.4 <u>Pressurizer Water Level</u>

Three pressurizer water level channels are used for reactor trip. Isolated signals from these channels are used for pressurizer water level control. A failure in the level control system could fill or empty the pressurizer at a slow rate (on the order of half an hour or more).

Experience has shown that hydrogen gas can accumulate in the upper part of the condensate pot on conventional open reference leg systems in pressurizer water level service. At RCS operating pressures, high concentrations of dissolved hydrogen in the reference leg water are possible. On sudden depressurization accidents, it has been hypothesized that rapid effervescence of the dissolved hydrogen could blow water out of the reference leg and cause a large level error, measuring higher than actual level. Accurate calculations of this effect have been difficult to obtain. To eliminate the possibility of such effects, a bellows is used in a pot at the top of the reference leg to provide an interface seal and prevent dissolving of hydrogen gas into the reference leg water. ~~Supplier tests were run which confirmed a time response of less than 1.0 second for return to system accuracy requirements.~~

The reference leg is uninsulated and will remain at local ambient temperature. This temperature will vary somewhat over the length of the reference leg piping under normal operating.

0794 PKG 44

7.2.2.3.5 Steam Generator Water Level ~~and Feedwater Flow~~

The basic function of the reactor protection circuits associated with low steam generator water level ~~and low feedwater flow~~ is to preserve the steam generator heat sink for removal of long term residual heat. Should a complete loss of feedwater occur, the reactor would be tripped on ~~coincidence of steam/feedwater flow mismatch and low level or~~ on low-low steam generator water level. In addition, redundant auxiliary feedwater pumps are provided to supply feedwater in order to maintain residual heat removal after trip. This ~~These~~ reactor trips acts before the steam generators are dry to reduce the required capacity and increase the starting time requirements of these auxiliary feedwater pumps and to minimize the thermal transient on the Reactor Coolant System and steam generators. ~~Therefore, the following reactor trip circuits are provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient:~~

1. ~~A mismatch in steam and feedwater flow coincident with low steam generator water level;~~

2. ~~A low-low steam generator water level regardless of steam - feedwater flow mismatch;~~

~~It is desirable to minimize thermal transients on a steam generator for credible loss of feedwater accidents. Hence, it should be noted that controller malfunctions caused by a protection system failure affect only one steam generator; the steam generator level signal used in the feedwater control originates separately from that used in the low feedwater reactor trip.~~

~~A spurious high signal from the feedwater flow channel being used for control would cause a reduction in feedwater flow preventing that channel from ultimately tripping. However, the mismatch between steam demand and feedwater flow produced by this spurious signal will actuate alarms to alert the operator of this situation in time for manual correction or, if the condition continues and the mismatch is not sufficient to trip the reactor on low feedwater flow, the reactor will eventually trip on a low-low water level signal independent of indicated feedwater flow.~~

I22

0794 PKG

Insert 22 to Page 7.2-38

Therefore, a low-low steam generator water level reactor trip is provided for each steam generator to ensure that sufficient initial thermal capacity is available in the steam generator at the start of the transient. It is desirable to minimize thermal transients on a steam generator for a credible loss of feedwater accident. To minimize perturbations on the Feedwater Control System, a control grade Median Signal Selector (MSS) is installed in the control system. Implementation of the MSS will prevent a single failed steam generator water level channel from perturbating the control system that may result in an unwarranted plant transient being initiated. The application of the MSS in the Feedwater Control system will improve system reliability by providing a "median" signal for use by the control system to initiate control system actions based on this signal and eliminate the need for the low feedwater flow previously required to meet the intent of Control and Protection System~~s~~ Interaction~~s~~, ~~as required by~~ IEEE-Std. 279 Section 4.7, Thus, because of the design of the MSS (accepting ~~there~~ level channel inputs and providing a "median" signal to the control system), the potential for a control and protection system interaction is eliminated~~, as required by IEEE Std 279 Section 4.7.~~

three isolated

0794 PKG

~~A spurious low signal from the feedwater flow channel being used for control would cause an increase in feedwater flow. The mismatch between steam flow and feedwater flow produced by the spurious signal would actuate alarms to alert the operator of the situation in time for manual correction. If the condition continues, a two out of three high-high steam generator water level signal in any loop, independent of the indicated feedwater flow, will cause feedwater isolation and trip the turbine. The turbine trip will result in a subsequent reactor trip. The high-high steam generator water level trip is an equipment protective trip preventing excessive moisture carry-over which could damage the turbine blading.~~

~~In addition, the three element feedwater controller incorporates reset action on the level error signal, such that with expected controller settings a rapid increase or decrease in the flow signal would cause only a small change in level before the controller would compensate for the level error. A slow change in the feedwater signal would have no effect at all. A spurious low or high steam flow signal would have the same effect as high or low feedwater signal, discussed above.~~

~~A spurious high steam generator water level signal from the protection channel used for control will tend to close the feedwater valve. However, before a reactor trip would occur, two out of three channels for a steam generator would have to indicate a low water level. A spurious low steam generator water level signal will tend to open the feedwater valve. Again, before a reactor trip would occur, two out of three channels in a loop would have to indicate a high water level. Any slow drift in the water level signal will permit the operator to respond to the level alarms and take corrective action. Automatic protection is provided in case the spurious high level reduces feedwater flow sufficiently to cause low level in the steam generator. The reactor will trip either on low feedwater flow coincident with low level or, ultimately, on low-low steam generator water level. Automatic protection is also provided in case the spurious low level signal increases feedwater flow sufficiently to cause high level in the steam generator. A turbine trip and feedwater isolation would occur on two out of three high-high steam generator water level in any loop.~~

7.2.2.4 Additional Postulated Accidents

Loss of plant instrument air or loss of component cooling water is discussed in Section 7.3.2. Load rejection and turbine trip are discussed in further detail in Section 7.7.

0794 PKG

The control interlocks, called rod stops, that are provided to prevent abnormal power conditions which could result from excessive control rod withdrawal are discussed in Section 7.7.1.4.1 and listed on Table 7.7-1. Excessively high power operation (which is prevented by blocking of automatic rod withdrawal), if allowed to continue, might lead to a safety limit (as given in the Technical Specifications) being reached. Before such a limit is reached, protection will be available from the Reactor Trip System. At the power levels of the rod block setpoints, safety limits have not been reached; and therefore these rod withdrawal stops do not come under the scope of safety-related systems, and are considered as control systems.

7.2.3 Tests and Inspections

The Reactor Trip System meets the testing requirements of IEEE Standard 338-1971, reference [10], as discussed in Section 7.1.2. The testability of the system is discussed in Section 7.2.2.1.3. The initial test intervals are specified in the Technical Specifications. Written test procedures and documentation, conforming to the requirements of reference [10], will be available for audit by responsible personnel. Periodic testing complies with Regulatory Guide 1.22 as discussed in Sections 7.1.2 and 7.2.2.1.3. 62

Insert 35

REFERENCES

1. J. A. Nay, "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems," WCAP 7671 May 1971.

2. Lipchak, J. B., "Nuclear Instrumentation System," WCAP-8255, January 1974.

3. Katz, D. N., "Solid State Logic Protection System Description," WCAP-7488-L, January 1971 (Proprietary) and WCAP-7672, June 1971 (Non-Proprietary).

4. Gangloff, W. C. and Loftus, W. D., "An Evaluation of Solid State Logic Reactor Protection In Anticipated Transients," WCAP-7706-L, July 1971 (Proprietary) and WCAP-7706, July 1971 (Non-Proprietary).

5. Burnett, T. W. T., "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," WCAP-7306, April 1969.

6. Baldwin, M. S. et al., "An Evaluation of Loss of Flow Accidents Caused by Power System Frequency Transients in Westinghouse PWR's," WCAP-8424, Revision 1, May 1975.

Insert 35 to Page 7.2-40

To ensure the Median Signal Selector (MSS) will function as described in Section 7.2.2.3.5, operability of the MSS will be verified commensurate with the Technical Specification surveillance interval for the associated low-low steam generator level channels.

The signal selector has been provided with the capability for on-line testing. Signal selector testing consists of monitoring the three input signals and the one output signal via test points. Comparison of the output signal to the input signals permits determination of whether or not the median signal is being passed and, consequently, whether the signal selector is functioning properly. Any output signal at a value other than that corresponding to the median signal is indicative of a unit failure.

The signal selector will be tested concurrently with the process protection channels which provide inputs to the unit. Test signals are received from the protection system, as would normal process signals, when the individual protection channels are placed in the test mode. As the test signal magnitude is varied, that protection channel which represents the median signal will also be altered allowing the technician to determine the presence of proper signal selector action.

0794 PKG

7. Garber, I., "Topical Report, Test Report on Isolation Amplifier," WCAP-7685, June 15, 1971.

I23

8. Lipchak, J. B. and Bartholomew, R. R., "Test Report Nuclear Instrumentation System Isolation Amplifier," WCAP-7506-P-A, April 1975 (Proprietary) and WCAP-7819-Revision 1-A, April 1975 (Non-Proprietary).

9. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Standard 279-1971.

10. The Institute of Electrical and Electronic Engineers, Inc., "IEEE Trial Use Criteria for the Periodic Testing of Nuclear Power Generating Station Protection Systems," IEEE Standard 339-1971.

11. Erin, L. E. "Eagle 21 Microprocessor Based Process Protection System." (Westinghouse Topical Report, January 1987). 63

I24

Insert 23 to Page 7.2-41

7. Doyle, J. P., "Noise, Fault, Surge and Radio Frequency Interference Test Report for Westinghouse Eagle 21 Process Protection Upgrade System," WCAP-11733 June 1988 (Westinghouse Proprietary Class 2); WCAP-11896 June 1988 (Westinghouse Proprietary Class 3)

Insert 24 to Page 7.2-41

11. Erin, L. E., "Topical Report, Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374 Rev. 1 December 1991 (Westinghouse Proprietary Class 2); WCAP-12375 Rev. 1 December 1991 (Westinghouse Proprietary Class 3)

12. Mermigos, J. F., "Median Signal Selector for Foxboro Series Process Instrumentation Application to Deletion of Low Feedwater Flow Reactor Trip," WCAP-12417 October 1989 (Westinghouse Proprietary Class 2); WCAP-12418 October 1989 (Westinghouse Proprietary Class 3)

13. Reagan. J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version," WCAP-12096 Rev. 5 (Westinghouse Proprietary Class 2)

14. "Summary Report Process Protection System Eagle 21 Upgrade, RTDBE, NSLB, MSS, and TTD Implementation, Watts Bar Unit 1 and 2"*

* To be issued at a later date.

TABLE 7.2-1 (Continued)

LIST OF REACTOR TRIPS

	Reactor Trip	Coincidence Logic	Interlocks	Comments	
12.	Reactor coolant pump bus undervoltage	2/4	Interlocked with P-7	Low voltage on all pumps permitted below P-7.	46
13.	Reactor coolant pump bus underfrequency	2/4	Interlocked with P-7	Under frequency on 2 pumps will trip all reactor coolant pump breakers and cause reactor trip; reactor trip and pump trip blocked below P-7.	31
~~14.~~	~~Low feedwater flow~~	~~1/2 in any loop*~~	~~No Interlocks~~		
14 ~~15.~~	Low-low steam generator water level	2/3 in any loop	No interlocks		
15 ~~16.~~	Safety injection signal	Coincident with actuation of safety injection	No interlocks	(See Section 7.3 for Engineered Safety Features actuation conditions)	

~~* 1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level.~~

Revised by Amendment 46

TABLE 7.2-1 (Continued)

LIST OF REACTOR TRIPS

	Reactor Trip	Coincidence Logic	Interlocks	Comments
16 ~~17~~.	Turbine-generator trip** a) Low auto stop oil pressure	2/3	Interlocked with P-9	Blocked below P-9
	b) Turbine stop valve close	4/4	Interlocked with P-9	Blocked below P-9
17 ~~18~~.	Manual	1/2	No interlocks	

** Reactor trip on turbine trip is anticipatory in ~~on~~ that no credit is taken for it in this accident analysis.

Revised by Amendment 52
Sheet 3

0794 PKG

0794 PKG

TABLE 7.2-3

REACTOR TRIP SYSTEM INSTRUMENTATION

Reactor Trip Signal	Typical Range	Typical Trip Accuracy	Typical Maximum Time Response sec	
1. Power range high neutron	1 to 120% power	Reference 13 ~~1% of full power~~	0.5	55
2. Intermediate range high neutron flux	8 decades of neutron flux overlapping source range by 2 decades and including 100% power	~~Later~~ Reference 13	~~Later~~ 0.5	63
3. Source range high neutron flux	6 decades of neutron flux (1 to 10^6 counts/sec)	~~Later~~ Reference 13	~~Later~~ 0.5	
4. Power range high positive neutron flux rate	+ 2 to +30% of full power	~~± 5 percent (1)~~ Reference 13	0.5	
5. Power range high negative neutron flux rate	-2 to -30% of full power	~~± 5 percent (1)~~ Reference 13	0.5	
6. Overtemperature ΔT:	T_H 530 to 650°F T_C 510 to 630°F T_{AVG} 530 to 630°F P_{PRZR} 1700 to 2500 psi F(Δϕ) ~~-50 to +50%~~ -60 to +60% ΔT Setpoint 0 to ~~100 %~~ 150% power	~~Later~~ Reference 13	~~Later~~ 7.0	63
7. Overpower ΔT	T_H 530 to 650°F T_C 510 to 630°F T_{AVG} 530 to 630°F ΔT Setpoint 0 to ~~100~~ 150% power	~~Later~~ Reference 13	~~Later~~ 7.0	

TABLE 7.2-3 (Continued)

REACTOR TRIP SYSTEM INSTRUMENTATION

	Reactor Trip Signal	Typical Range	Typical Trip Accuracy	Typical Time Response (sec)
8.	Pressurizer low pressure	1700 to 2500 psig	± 18 psi (Compensated signal)	2.0
9.	Pressurizer high pressure	1700 to 2500 psig	± 18 psi (non-compensated signal)	2.0
10.	Pressurizer high water level	Entire cylindrical portion of pressurizer	± 2.25 percent of full range Δp between taps at design temperature and pressure.	2.0
11.	Low reactor coolant flow	0 to 120% of rated flow	± 2.75 percent of full flow within range of 70 percent to 100 percent of full flow (1)	~~1.0~~ 1.2
12.	Reactor coolant pump bus undervoltage	0 to 100% rated voltage	± 1%	1.5
13.	Reactor coolant pump bus underfrequency	50 to 65 Hz	± 0.1 Hz	0.6
~~14.~~	~~Steamflow feedwater flow mismatch~~	~~0 to 120% Max. Calc. feedwater flow~~	~~± 6.5% (2)~~	~~2.0~~
14 ~~15.~~	Low-low steam generator water level	+ 6 ft., - 12 ft. from nominal full load water	± 2.75 percent of Δp signal over pressure range of 700 to 1200 psig	2.0 (2)
15 ~~16.~~	Turbine Trip (3)			1.0

0794 PKG

TABLE 7.2-3 (Continued)

REACTOR TRIP SYSTEM INSTRUMENTATION

NOTES:

(1) Reproducibility (see definitions in Section 7.1)

~~(2) 1/2 steam/feedwater flow mismatch in coincidence with 1/2 low steam generator water level.~~

~~(3) Channel accuracy of feedwater flow analog signal is ±2.5 percent of maximum calculated feedwater flow.~~

~~Accuracy of steam flow signal is ±3 percent of maximum calculated flow over the pressure range of 700 to 1200 psig.~~

~~(4)~~ (3) The reactor trip on turbine trip ~~are~~ is anticipatory in that no credit is taken for ~~them~~ it in the accident analyses. 40

(2) *Low-low steam generator water level trip response time does not include Trip Time Delay function.*

Revised by Amendment 40

Sheet 3

TABLE 7.2-4

REACTOR TRIP CORRELATION

TRIP[a]	ACCIDENT[b]	TECH SPEC.
1. Power Range High Neutron Flux Trip (Low Setpoint)	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	2.2.1 Table 2.2-1 #2
	2. Uncontrolled Boron Dilution (15.2.4) (Modes 1 and 2)	
	~~2.~~ 3. Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
	~~3.~~ 4. Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)	
2. Power Range High Neutron Flux Trip (High Setpoint)	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	2.2.1 Table 2.2-1 #2
	2. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	
	3. Uncontrolled Boron Dilution (15.2.4) (Modes 1 and 2)	
	~~3.~~ 4. Startup of an Inactive Reactor Coolant Loop (15.2.6)	
	~~4.~~ 5. Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
	~~5.~~ 6. Excessive Load Increase Incident (15.2.11)	
	~~6. Accidental Depressurization of the Main Steam System (15.2.13)~~	

0794 PKG

TABLE 7.2-4 (Continued)

REACTOR TRIP CORRELATION

TRIP[a]	ACCIDENT[b]	TECH SPEC.	
	~~7. Major Secondary System Pipe Ruptures (15.4.2)~~		
	7 ~~8~~. Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)		
3. Intermediate Range High Neutron Flux Trip	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	2.2.1 Table 2.2-1 #5	
4. Source Range High Neutron Flux Trip	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)	2.2.1 Table 2.2-1 #6	2. Uncontrolled Boron Dilution (15.2.4) (Modes 2, 3, 4, and 5)
5. Power Range High Positive Neutron Flux Rate Trip	~~1~~ 2. Rupture of a Control Rod Drive Mechanism Housing (Rod Cluster Control Assembly Ejection) (15.4.6)	2.2.1 Table 2.2-1 #3	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition (15.2.1)
6. Power Range High Negative Flux Rate Trip	1. Rod Cluster Control Assembly Misalignment (15.2.3)	2.2.1 Table 2.2-1 #4	
7. Overtemperature ΔT Trip	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	2.2.1 Table 2.2-1 Note 1	
	2. Uncontrolled Boron Dilution (15.2.4)		
	3. Loss of External Electrical Load and/or Turbine Trip (15.2.7)		
	~~4. Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)~~		
	4 ~~5~~. Excessive Load Increase Incident (15.2.11)		

0794 PKG

57

TABLE 7.2-4 (Continued)

REACTOR TRIP CORRELATION

TRIP[a]	ACCIDENT[b]	TECH SPEC.
	5 ~~6~~. Accidental Depressurization of the Reactor Coolant System (15.2.12)	
	6 ~~7~~. Accidental Depressurization of the Main Steam System (15.2.13)	
	7 ~~8~~. Loss of Reactor Coolant From Small Ruptured Pipes or From Cracks in Large Pipes Which Actuates ECCS (15.3.1)	
	8. Single Rod Cluster Control Assembly Withdrawal (15.3.6)	
	9. Major Rupture of a Main Steam Line (15.4.2.1)	
	10. Major Rupture of a Main Feedwater pipe (15.4.2.2)	
8. Overpower ΔT Trip	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2)	2.2.1 Table 2.2-1 Note 2
	2. Loss of External Electrical Load and/or Turbine Trip (15.2.7)	
	3 ~~2~~. Excessive Heat Removal Due to Feedwater System Malfunctions (15.2.10)	
	~~3. Excessive Load Increase Incident (15.2.11).~~	
	4. Accidental Depressurization of the Main Steam System (15.2.13)	
	5. Major Rupture of a Main Steam Line (15.4.2.1)	
	~~5. Major Secondary System Pipe Ruptures (15.4.2)~~	
9. Pressurizer Low Pressure Trip	1. Excessive Load Increase Incident (15.2.11)	2.2.1 Table 2.2-1 #9
	2 ~~1~~. Accidental Depressurization of the Reactor Coolant System (15.2.12)	
	3. Accidental Depressurization of the Main Steam System (15.2.13)	
	4. Inadvertent operation of Emergency Core Cooling System (15.2.14)	
	5 ~~2~~. Loss of Reactor Coolant From Small Ruptured Pipes or From Cracks in Large Pipes Which Actuates ECCS (15.3.1)	
	6 ~~3~~. Major Reactor Coolant System Pipe Ruptures (LOCA) (15.4.1)	
	7. Major Rupture of a Main Steam Line (15.4.2.1)	
	8. Major Rupture of a Main Feedwater Pipe (15.4.2.2)	
	9 ~~4~~. Steam Generator Tube Rupture (15.4.3)	

0794 PKG

TABLE 7.2-4 (Continued)

REACTOR TRIP CORRELATION

TRIP[a]	ACCIDENT[b]	TECH SPEC.
10. Pressurizer High Pressure Trip	1. Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power (15.2.2) 2. Loss of External Electrical Load and/or Turbine Trip (15.2.7) 3. Loss of Normal Feedwater (15.2.8) 4. Loss of Offsite Power to Station Auxiliaries (Station Blackout) (15.2.9) 5. Major Rupture of a Main Feedwater Pipe (15.4.2.2)	2.2.1 Table 2.2-1 #10
11. Pressurizer High Water Level Trip	1. Uncontrolled Rod Cluster Control Assembly Bank withdrawal at Power (15.2.2) 2. Loss of External Electrical Load and/or Turbine Trip (15.2.7)	2.2.1 Table 2.2-1 #11
12. Low Reactor Coolant Flow	1. Partial Loss of Forced Reactor Coolant Flow (15.2.5) ~~2. Loss of Offsite Power to the Station Auxiliaries (Station Blackout) (15.2.9)~~	2.2.1 Table 2.2-1 #12
13. Reactor Coolant Pump Bus Undervoltage Trip	1. Complete Loss of Forced Reactor Coolant Flow (15.3.4)	2.2.1 Table 2.2-1 #15
14. Reactor Coolant Pump Bus Underfrequency Trip	1. Complete Loss of Forced Reactor Coolant Flow (15.3.4)	2.2.1 Table 2.2-1 #16
~~15. Low Feedwater Flow Trip~~	~~1. Loss of Normal Feedwater (15.2.8)~~	~~2.2.1~~ ~~Table 2.2-1 #14~~
15 ~~16.~~ Low-low Steam Generator Water Level Trip	1. Loss of Normal Feedwater (15.2.8)	2.2.1 Table 2.2-1 #13
16 ~~17.~~ Turbine Trip-Reactor Trip	1. Loss of External Electrical Load and/or Turbine Trip (15.2.7) 2. Loss of Offsite Power to the Station Auxiliaries (Station Blackout) (15.2.9) 3. Major Rupture of a Main Feedwater Pipe (15.4.2.2)	2.2.1 Table 2.2-1 ~~2.2.1~~ ~~Table 2.2-1~~

0794 PKG

59

TABLE 7.2-4 (Continued)

REACTOR TRIP CORRELATION

TRIP[a]	ACCIDENT[b]	TECH SPEC.
17 ~~25.~~ Safety Injection Signal Actuation Trip	1. Accidental Depressurization of the Main Steam System (15.2.13) 2. Inadvertent operation of Emergency Core Cooling System (15.2.14) 3. Major Rupture of a Main Steam Line (15.4.2 4. Major Rupture of a Main Feedwater Pipe (15.4.2.2)	See Note d
18 ~~26.~~ Manual Trip	1 Available for all Accidents (Chapter 15)	See Note c

NOTES:

a. Trips are listed in order of discussion in Section 7.2

b. References refer to accident analyses presented in Chapter 15.

c. A technical specification is not required because this trip is not assumed to function in the accident analyses.

~~d. Accident assumes that the reactor is tripped at end of life (EOL) which is the worst initial condition for this case.~~

0794 PKG

60

7.3 ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

In addition to the requirements for a reactor trip for anticipated abnormal transients, the facility shall be provided with adequate instrumentation and controls to sense accident situations and initiate the operation of necessary Engineered Safety Features. The occurrence of a limiting fault, such as a loss-of-coolant accident or a ~~steam~~ steamline break, requires a reactor trip plus actuation of one or more of the Engineered Safety Features in order to prevent or mitigate damage to the core and Reactor Coolant system components, and ensure containment integrity.

In order to accomplish these design objectives the Engineered Safety Features system shall have proper and timely initiating signals which are to be supplied by the sensors, transmitters and logic components making up the various ~~instrumentation~~ channels of the Engineered Safety Features Actuation System. protection system

7.3.1 Description

The Engineered Safety Features Actuation System uses selected plant parameters, determines whether or not predetermined safety limits are being exceeded and, if they are, combines the signals into logic matrices sensitive to combinations indicative of primary or secondary system boundary ruptures (Class III or IV faults). Once the required logic combination is completed, the system sends actuation signals to the appropriate Engineered Safety Features components. The Engineered Saafety Features Actuation System meets the requirements of Criteria 13, 20, 27, 28 and 38 of the 1971 General Design Criteria (GDC).

7.3.1.1 System Description

The Engineered Safety Features Actuation System is a functionally defined system described in this section. The equipment which provides the actuation functions identified in Section 7.3.1.1.1 is listed below and discussed in this section and the references.

1. Process Protection ~~Instrumentation~~ and Control System (reference [1] and [5]) | 63

2. Solid State Logic Protection System (reference [2])

3. Engineered Safety Features Test Cabinet

4. Manual Actuation Circuits

0794 PKG

The Engineered Safety Features process Actuation System consists of two discrete portions of circuitry: 1) A process protection ~~instrumentation~~ portion consisting of three or four redundant channels per parameter or variable to monitor various plant parameters such as the Reactor Coolant System and steam system pressure, temperatures and flows and containment pressures; and 2) a ~~digital~~ logic portion consisting of two redundant ~~logic~~ trains which receive inputs from the process protection ~~instrumentation~~ channels and perform the logic needed to actuate the Engineered Safety Features. Each ~~digital~~ logic train is capable of actuating the Engineered Safety Features equipment required. The intent is that any single failure within the Engineered Safety Features Actuation System shall not prevent system action when required. 63

The redundant concept is applied to both the process protection ~~instrumentation~~ and logic portions of the system. Separation of redundant process protection ~~instrumentation~~ channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations and ~~analog~~ process protection racks terminating at the redundant safeguards logic racks. The design meets the requirements of Criteria 20, 21, 22, 23 and 24 of the 1971 GDC. 63

The variables are sensed by the process protection ~~instrumentation~~ circuitry as discussed in reference [1] and in Section 7.2. The outputs from the process protection ~~instrumentation~~ channels are combined into actuation logic as shown ~~an~~ in Figure 7.3-3, Sheets 1, 2, 3, and 4, and Figure 7.2-1, Sheets 1, 2, and 3. Tables 7.3-1 and 7.3-2 give additional information pertaining to logic and function. 63

The interlocks associated with the Engineered Safety Features Actuation System are outlined in Table 7.3-3. These interlocks satisfy the functional requirements discussed in Section 7.1.2.

Manual actuation from the control board of containment isolation Phase A is provided by operation of either one of the redundant momentary containment isolation Phase A controls. Each control consists of two backup linked actuation switches. The separate trains are thereby linked by mechanical means. Also on the control board is manual actuation of safety injection by one of the redundant controls and a manual activation of containment isolation Phase B by either of the two sets of controls.

Manual controls are also provided to switch from the injection to the recirculation phase after a loss-of-coolant accident.

0794 PKG

13 ~~14.~~ Containment spray actuation which performs the following functions:

a. Initiates containment spray to reduce containment pressure and temperature following a loss-of-coolant or steamline break accident inside of containment.

b. Initiates Phase B containment isolation which isolates the containment following a loss of reactor coolant accident, or a steam or feedwater line break within containment to limit radioactive releases. (Phase B isolation together with Phase A isolation results in isolation of all but safety injection and spray lines penetrating the containment).

14 ~~15.~~ Automatic switchover of the RHR pumps from the injection to the recirculation mode (Post-LOCA).

7.3.1.1.2 Process Protection ~~Instrumentation~~ Circuitry

The process protection system ~~instrumentation~~ sensors and racks for the Engineered Safety Feature~~s~~ Actuation System are covered in References [1] and [5]. Discussed in ~~this~~ these reports are the parameters to be measured including pressures, flows, tank and vessel water levels, and temperatures as well as the measurement and signal transmission considerations. These latter considerations include the transmitters, orifice plates and flow elements, resistance temperature detectors, as well as automatic calculations, signal conditioning/processing and location and mounting of the devices.

The sensors monitoring the primary system are located as shown on the piping flow diagrams in Chapter 5, Reactor Coolant System. The secondary system sensor locations are shown on the steam system flow diagrams given in Chapter 10.

7.3.1.1.3 Logic Circuitry 63

The Engineered Safety Features logic racks are discussed in detail in reference [2]. The description includes the considerations and provisions for physical and electrical separation as well as details of the circuitry. Reference [2] also covers certain aspects of on-line test provisions, provisions for test points, considerations for the instrument power source, considerations for accomplishing physical separation. The outputs from the process protection ~~instrumentation~~ channels are combined into actuation logic as shown on Sheets 1 (T_{avg}), 3 (Pressurizer Pressure), 3 (Steam ~~Flow and Differential~~ Pressure), 3 and 4 (Engineered Safety Features Actuation), and 3 (Auxiliary Feedwater)) of Figure 7.3-3. 63
and Steam Pressure Rate

To facilitate Engineered Safety Features Actuation testing, four cabinets (two per train) are provided which enable operation, to the maximum practical extent, of safety features loads on a group by group basis until actuation of all devices has been checked. Final actuation testing is discussed in detail in Section 7.3.2.

7.3.1.1.4 Final Actuation Circuitry

The outputs of the Solid State Logic Protection System (the slave relays) are energized to actuate, as are most final actuators and actuated devices. These devices are listed as follows:

1. Safety Injection System pump and valve actuators. See Chapter 6 for flow diagrams and additional information.

2. Containment isolation (Phase A - "T" signal isolates all non-essential process lines on receipt of safety injection signal; Phase B - "P" signal isolates remaining process lines (which do not include safety injection lines) on receipt of 2/4 high-high containment pressure signal). For further information, Section 6.2.4.

3. Essential raw cooling system and component cooling water and valve actuators. (See component cooling system, Chapter 9).

4. Auxiliary feed pumps start (See Chapter 10).

5. Diesel start (See Chapter 8).

0794 PKG

c. Steam generator tube rupture

2. Secondary System

a. Minor secondary system pipe breaks resulting in steam release rates equivalent to a single dump, relief or safety valve

b. Rupture of a major steam pipes

7.3.1.2.2 Generating Station Variables

The following list summarizes the generating station variables required to be monitored for the automatic initiation of Safety Injection during each accident identified in the preceding section. Post accident monitoring requirements are given in Table 7.5-1 .

1. Primary System Accidents

a. Pressurizer pressure

b. Containment pressure (not required for steam generator tube rupture)

2. Secondary System Accidents

a. Pressurizer pressure

b. Steamline pressures

c. Containment pressure 63

~~d. Steamline differential pressure rate~~

~~e. Steam flows~~

~~f. Reactor coolant average temperature (T_{avg})~~

7.3.1.2.3 Spatially Dependent Variables

The only variable sensed by the Engineered Safety Features Actuation System which has spatial dependence is reactor coolant temperature. The effect on the measurement is negated by taking multiple samples from the reactor coolant hot leg and electronically averaging these samples in the ~~instrumentation~~ process protection channel electronics. 63

0794 PKG

7.3.1.2.4 Limits, Margin and Levels

Prudent operational limits, available margins and setpoints before onset of unsafe conditions requiring protective action are discussed in Chapter 15 and the Technical Specifications.

7.3.1.2.5 Abnormal Events

The malfunctions, accidents, or other unusual events which could physically damage protection system components or could cause environmental changes are as follows:

1. Loss-of-Coolant Accident (See Section 15.3 and 15.4)
2. ~~Steam~~ Steamline Breaks (See Sections 15.3 and 15.4)
3. Earthquakes (See Chapters 2 and 3)
4. Fire (Section 9.5.1)
5. Explosion (Hydrogen buildup inside containment) (See Section 15.4)
6. Missiles (See Section 3.5)
7. Flood (See Chapters 2 and 3)

7.3.1.2.6 Minimum Performance Requirements

Minimum performance requirements are as follows:

1. System Response Times

   The Engineered Safety Features Actuation System (ESFAS) response time is defined as the interval required for the engineered safety feature sequence to be initiated subsequent to the time that the appropriate variables exceed the setpoints. The engineered safety feature sequence is initiated by the output of the ESFAS which is by the operation of the dry contacts of the slave relays (600 series relays) in the output cabinets of the Solid State Protection System (SSPS). The response times listed below include the interval of time which will elapse between the time the parameter as sensed by the sensor exceeds the safety setpoint and the time the SSPS slave relay dry contacts are operated. The values listed below are maximum allowable values

APR [illegible] 1988

0794 PKG

consistent with the safety analyses and the Technical Specifications and are systematically verified during plant preoperational startup tests. These maximum delay times thus include all compensation and therefore require that any such network be aligned and operating during verification testing. For the overall engineered safety features response time, refer to the Technical Specifications. In a similar manner, for the overall reactor trip system instrumentation response time, refer to the Technical Specifications.

The Engineered Safeguards Actuation System is always capable of having response time tests performed using the same methods as those tests performed during the preoperational test program or following significant component changes.

Maximum allowable time delays in generating the actuation signal for loss-of-coolant protection ~~is 2.0 seconds for pressurizer pressure.~~

I25

Typical maximum allowable time delays in generating the actuation signal for steamline break protection are:

~~a. Steamline flow~~	~~2.0 seconds~~
a ~~b~~. Low Steamline pressure (SAFETY INJECTION ~~(assume other signals present)~~ AND STEAMLINE ISOLATION)	2.0 seconds
c. Reactor Coolant System T_{avg} as measured at the resistance temperature detector sensor outputs	~~Later~~
b ~~c~~ ~~d~~. High-high containment pressure for closing main steamline stop valves (STEAMLINE ISOLATION)	2.0 seconds
c ~~d~~ ~~e~~. Actuation signals for auxiliary feedwater pumps	2.0 seconds
d ~~e~~ ~~f~~. ~~Steamline differential pressure~~ High STEAMLINE PRESSURE RATE (STEAMLINE ISOLATION)	2.0 seconds

I26

63

Insert 25 to Page 7.3-10 0794 PKG

are:

a. Pressurizer Pressure 2.0 seconds

b. Containment Pressure 2.0 seconds

Insert 26 to Page 7.2-10

e ~~f.~~ Low Pressurizer Pressure (Safety Injection) 2.0 seconds

f ~~g.~~ High Containment Pressure (Safety Injection) 2.0 seconds

0794 PKG

2. System accuracies:

Typical accuracies required for generating the required actuation signals for loss-of-coolant protection are:

a. Pressurizer pressure (uncompensated) ~~± 14 psi~~ Ref. 6
b. Containment pressure Ref. 6

Typical accuracies required in generating the required actuation signals for ~~steam~~ steamline break protection are given:

a. Steamline pressure	~~± 4% of span~~	Ref. 6
~~b. Steam flow signals~~	~~± 4.5% of maximum guarantee flow over pressure range 700 to 1300 psig~~	
b. steamline pressure rate		
~~c. T_{avg}~~	~~± 2°F~~	Ref. 6
c ~~d~~. Containment pressure ~~signal~~	~~± 1.8% of full scale~~	Ref. 6
d. Pressurizer pressure		Ref. 6

3. Ranges of sensed variables to be accommodated until conclusion of protective action is assured:

Typical ranges required in generating the required actuation signals for loss-of-coolant protection are given:

a. Pressurizer pressure	1700 to 2500 psig
b. Containment pressure	~~-1 to 17 psig~~ -2 to 15 psig (Ice Condenser System)

Typical ranges required in generating the required actuation signals for steamline break protection are given:

~~a. T_{avg}~~	~~530° to 630°F~~
a ~~b~~. Steamline pressure (from which steamline pressure is derived)	0 to 1300 psig
~~c. Steamline flow~~	~~0 to 120% maximum calculated steam flow~~
b. Pressurizer pressure	1700 to 2500 psig

0794 PKG

c. Containment pressure (Ice Condenser System) ~~1 to 17 psig~~ -2 to 15 psig

7.3.1.3 Final System Drawings

The schematic diagrams and other drawings for the systems discussed in this section are referenced in Section 1.7.

7.3.2 Analysis

I 28

7.3.2.1 System Reliability/Availability and Failure Mode and Effect Analyses

A failure mode and effects analysis (FMEA) has ~~have~~ been performed [4] on the logic portion of a generic Engineered Safety Features Actuation System (ESFAS) equipment similar to the Watts Bar Solid State Protection System (SSPS). ~~and Process Control System (PCS)~~ The FMEA has been performed down to the replaceable component level (e.g. ~~i.e.~~, transmitter, relay, module, etc.) for the SSPS ~~and PCS~~. Concerning the output actuation functions considered, the analysis addressed ~~extended from the sensors to~~ the output functions available from the output cabinets of the SSPS. These output functions involve output slave relays contacts which in some cases close for final device actuation and in other cases open for final device actuation. The results of the FMEA show that the ESFAS does indeed comply with the Single Failure Criterion. No single failure was found which could prevent the ESFAS from generating the proper actuation signal on demand for an engineered safety feature. Failures are either in the safe direction, or a redundant channel or train insures the necessary actuation capability. The actuation functions ~~as well as the input functions from which the actuation functions are derived~~ are the same for the Watts Bar Nuclear Plant as for the generic system analyzed, although in the translation of these functions into the system design a few minor differences in the hardware cannot be precluded. The Watts Bar ESFAS has been designed to equivalent safety design criteria as the generic system analyzed, and all the specific design features of the Watts Bar ESFAS as well as design features of each Watts Bar Class 1E ESF system in the scope of the Westinghouse NSSS are reviewed for failure modes and effects. This ESFAS FMEA applies to all Watts Bar engineered safety features both NSSS and BOP related, that are automatically actuated by the dry contacts of the slave relays in the output cabinets of the SSPS. These reviews have resulted in those conclusions documented in the FSAR and supplementary documentation referenced to the docket. It is noted that Appendix B and C of Reference [4] provide interface criteria for

0794 PKG

Insert 28 to Page 7.3-12

A discussion on the reliability/availability of the Eagle 21 process protection system is provided in Section 7.2.~~4~~ 2.

0794 PKG

In the ESF, a loss of instrument power will call for actuation of ESF equipment controlled by the specific ~~bistable~~ comparator that lost power (containment spray excepted). The actuated equipment must have power to comply. The power supply for the protection systems is discussed in Chapter 8. For containment spray, the final ~~bistables~~ comparators are energized to trip to avoid spurious actuation. In addition, manual containment spray requires a simultaneous actuation of two manual controls. This is considered acceptable because spray actuation on high-high containment pressure signal provides automatic initiation of the system via protection channels meeting the criteria in Reference [3]. Moreover, two sets (two switches per set) of containment spray manual initiation switches are provided to meet the requirements of IEEE Standard 279-1971. Also, it is possible for all ESF equipment (valves, pumps, etc.) to be individually manually actuated from the control board. Hence, a third mode of containment spray initiation is available. The design meets the requirements of Criteria 21 and 23 of the 1971 GDC.

7.3.2.2.2 Equipment Qualification

Equipment qualifications are discussed in Sections 3.10 and .11.

7.3.2.2.3 Channel Independence

The discussion presented in Section 7.2.2.1.3 (Item 6) is applicable. The ESF slave relay outputs from the solid state logic protection cabinets are redundant, and the actuations associated with each train are energized up to and including the final actuators by the separate ac power supplies which power the logic trains.

7.3.2.2.4 Control and Protection System Interaction

The discussions presented in Section 7.2.2.1.3 (Item 7) are applicable.

7.3.2.2.5 Capability for Sensor Checks and Equipment Test and Calibration

The discussions of system testability in section 7.2.2.1.3 (Item 9) are applicable to the sensors, process protection ~~instrumentation~~ system circuitry, and logic trains of the ESFAS, and meet the requirements of IEEE 338-1971.

The following discussions cover those areas in which the testing provisions differ from those for the Reactor Trip System.

Testing of ESFAS

The ESFASs are tested to provide assurance that the systems will operate as designed and will be available to function properly in the unlikely event of an accident. The testing program meets the requirements of Criteria 21, 37, 40, and 43 of the 1971 GDC and RG 1.22 as discussed in Table 7.1-1. The tests described in this Section and further discussed in Section 6.3.4 meet the requirements on testing of the ECCS as stated in GDC 37 except for the operation of those components that will cause an actual safety injection. The test, as described, demonstrates the performance of the full operational sequence that brings the system into operation, the transfer between normal and emergency power sources and the operation of associated cooling water systems. The safety injection and RHR pumps are started and operated and their performance verified in a separate test discussed in Section 6.3.4. When the pump tests are considered in conjunction with the ECCS test, the requirements of GDC 37 on testing of the ECCS are met as closely as possible without causing an actual safety injection.

Testing as described in Sections 6.3.4., 7.2.2.1.3 (Item 10) and this section provides complete periodic testability during reactor operation of all logic and components associated with the ECCS. This design meets the requirements of RG 1.22 as discussed in the above sections. The program is as follows:

1. Prior to initial plant operation, ESFAS tests will be conducted.

2. Subsequent to initial startup, ESFAS tests will be conducted during each regularly scheduled refueling outage.

3. During on-line operation of the reactor, all of the ESF process protection ~~instrumentation~~ and logic circuitry will be fully tested. In addition, essentially all of the ESF final actuators will be fully tested. The remaining few final actuators whose operation is not compatible with continued on-line plant operation will be checked by means of continuity testing.

0794 PKG

4. During normal operation, the operability of testable final actuation devices of the ESFAS will be tested by manual initiation from the control room.

Performance Test Acceptability Standard for the "S" (Safety Injection Signal) and for the "P" (the Automatic Demand Signal for Containment Spray Actuation) Actuation Signals Generation

During the reactor operation the basis for ESFAS acceptability will be the successful completion of the overlapping tests performed on the initiating system and the ESFAS, see Figure 7.3-1. Checks of process indications verify operability of the sensors. Protection system ~~instrumentation~~ checks and tests verify the operability of the circuitry from the input of these circuits through to and including the logic input relays except for the input relays associated with the containment spray function which are tested during the solid state logic testing. Solid state logic testing also checks the ~~digital~~ signal path from and including logic input relay contacts through the logic matrices and master relays and performs continuity tests on the coils of the output slave relays; final actuator testing operates the output slave relays and verifies operability of those devices which require safeguards actuation and which can be tested without causing plant upset. A continuity check is performed on the actuators of the untestable devices. Operation of the final devices is confirmed by control board indication and visual observation that the appropriate pump breakers close and automatic valves shall have completed their travel.

The basis for acceptability for the ESF interlocks will be control board indication of proper receipt of the signal upon introducing the required input at the appropriate setpoint.

Maintenance checks (performed during regularly scheduled refueling outages), such as resistance to ground signal cables in radiation environments are based on qualification test data which identifies what constitutes acceptable radiation, thermal, etc. degradation.

0794 PKG

Train A, and Train B, respectively, for the redundant counterparts. The master and slave relay circuits operate various pump and fan circuit breakers or starters, motor operated valve contractors, solenoid operated valves, emergency generator starting, etc.

Protection Process ~~Instrumentation~~ System Testing

Protection Process ~~instrumentation~~ System testing is identical to that used for reactor trip circuitry and is described in Section 7.2.2.1.3 (Item 10).

An exception to this is containment spray, which is energized to actuate 2/4 and reverts to 2/3 when one channel is in test.

Solid State Logic Testing

Except for containment spray channels solid state logic testing is the same as that discussed in Section 7.2.2.1.3 (Item 10). During logic testing of one train, the other train can initiate the required ESF function. For additional details, see reference [2].

Actuator Testing

At this point, testing of the initiation circuits through operation of the master relay and its contacts to the coils of the slave relays has been accomplished. Slave relays (K601, K602, etc.) do not operate because of reduced voltage.

The ESFAS final actuation device or actuated equipment testing shall be performed from the engineered safeguards test cabinets. These cabinets are located near the solid state logic protection system equipment. There is one set of test cabinets provided for each of the two protection Trains A and B. Each set of cabinets contains individual test switches necessary to actuate the slave relays. To prevent accidental actuation, test switches are of the type that must be rotated and then depressed to operate the slave relays. Assignments of contacts of the slave relays for actuation of various final devices or actuators has been made such that groups of devices or actuated equipment can be operated individually during plant operation without causing plant upset or equipment damage. In the unlikely event that a safety injection signal is initiated during the test of the final device that is actuated by this test, the device will already be in its safeguard position.

circuits will be energized, and green test lamp "DS*" will be de-energized. Typical Circuit path for white lamp "DS*" will be through the normally closed solid state logic output relay contact "K*" and through test lamp connections 1 to 3. Coils "Y1" and "Y2" will be capable of being de-energized for protection function actuation upon opening of solid state logic output relay contacts "K*". Coil "Y2" is typical for a solenoid valve coil, auxiliary relay, etc. When the contacts "K*" are closed to block de-energizing of coils "Y1" and "Y2", the green test lamp is energized to verify operation (opening of its contacts). To verify operability of the blockage relay contact to the green lamp - the green test lamp should now be energized also; open this blocking relay contact - the green test lamp should be de-energized, which verifies that the circuit is now in its normal, i.e., operable position.

Time Required for Testing

It is estimated that process protection system ~~instrumentation~~ testing can be performed at a rate of several channels per hour. Logic testing of either Trains A and B can be performed in less than 2 hours. Testing of actuated components (including those which can only be partially tested) will be a function of control room operator availability. It is expected to require several shifts to accomplish these tests. During this procedure automatic actuation circuitry with a single slave override testing, except for those few devices associated with a single slave relay whose outputs must be blocked and then only while blocked. It is anticipated that continuity testing associated with a blocked slave relay could take several minutes. During this time the redundant devices in the other trains would be functional.

Summary of On-Line Testing Capabilities

The procedures described provide capability for checking completely from the process signal to the logic cabinets and from there to the individual pump and fan circuit breakers or starters, valve contactors, pilot solenoid valves, etc., including all field cabling actually used in the circuitry called upon to operate for an accident condition. For those few devices whose operation could adversely affect plant or equipment operation, the ~~dame~~ same procedure provides for checking from the process signal to the logic rack. To check the final actuation device a continuity test of the individual control circuits is performed.

The procedure requires testing at various locations.

1. Process Protection system ~~instrumentation~~ testing and verification of comparator ~~bistable~~ setpoints are accomplished at protection system ~~instrumentation channel~~ racks. Verification of comparator ~~bistable~~ relay operation is done at the MCR status lights.

the Engineered Safety Features. The system must sense the accident condition and generate the signal actuating the protection function reliably and within a time determined by and consistent with the accident analyses in Chapter 15.

Much longer times are associated with the actuation of the mechanical and fluid system equipment associated with Engineered Safety Features. This includes the time required for switching, bringing pumps and other equipment to speed and the time required for them to take load.

Operating procedures require that the complete Engineered Safety Features Actuation System normally be operable. However, redundancy of system components is such that the system operability assumed for the safety analyses can still be met with certain ~~instrumentation~~ protection channels out of service. Channels that are out of service are to be placed in the tripped mode or bypass mode in the case of containment spray.

7.3.2.4.1 Loss-of-Coolant Protection

By analysis of loss-of-coolant accident and in system tests it has been verified that except for very small coolant system breaks which can be protected against by the charging pumps followed by an orderly shutdown, the effects of various loss-of-coolant accidents are reliably detected by the low pressurizer pressure signal; the Emergency Core Cooling System is actuated in time to prevent or limit core damage.

For large coolant system breaks the passive accumulators inject first because of the rapid pressure drop. This protects the reactor during the unavoidable delay associated with actuating the active Emergency Core Cooling System phase. 63

High containment pressure also actuates the Emergency Core Cooling System. Therefore, emergency core cooling actuation can be brought about by sensing this other direct consequence of a primary system break; that is, the Engineered Safety Features Actuation System detects the leakage of the coolant into the containment. The generation time of the actuation signal of about 1.5 seconds, after detection of the consequences of the accident, is adequate.

Containment spray will provide additional emergency cooling of containment and also limit fission product release upon sensing elevated containment pressure (high-high) to mitigate the effects of a loss-of-coolant accident.

The delay time between detection of the accident condition and the generation of the actuation signal for these systems is assumed to be about 1.0 second; well within the capability of the protection system equipment. However, this time is short compared to that required for startup of the fluid systems.

The analyses in Chapter 15 show that the diverse methods of detecting the accident condition and the time for generation of the signals by the protection systems are adequate to provide reliable and timely protection against the effects of loss-of-coolant.

7.3.2.4.2 Steam Line Break Protection

The Emergency Core Cooling System is also actuated in order to protect against a steam line break. About 2.0 seconds elapses between sensing low steam line pressure ~~and high steam line flow~~ and generation of the actuation signal. Analysis of steam break accidents assuming this delay for signal generation shows that the Emergency Core Cooling System is actuated for a steam line break in time to limit or prevent further core damage for steam line break cases. There is a reactor trip but the core reactivity is further reduced by the highly borated water injected by the Emergency Core Cooling System.

Additional protection against the effects of steam line break is provided by feedwater isolation which occurs upon actuation of the Emergency Core Cooling System. Feedwater line isolation is initiated in order to prevent excessive cooldown of the reactor vessel and thus protect the Reactor Coolant System boundary.

Additional protection against a steamline ~~steam~~ break accident is provided by closure of all steam line isolation valves in order to prevent uncontrolled blowdown of all steam generators. The generation of the protection system signal (about 2.0 seconds) is again short compared to the time to trip the fast acting steam line isolation valves which are designed to close in less than approximately 5 seconds.

0794 PKG

In addition to actuation of the Engineered Safety Features, the effect of a steamline break accident also generates a signal resulting in a reactor trip on overpower or following Emergency Core Cooling System actuation. However, the core reactivity is further reduced by the highly borated water injected by the Emergency Core Cooling System.

The analyses in Chapter 15 of the steam break accidents and an evaluation of the protection system ~~instrumentation and channel~~ design shows that the Engineered Safety Features Actuation Systems are effective in preventing or mitigating the effects of a steam break accident.

REFERENCES

1. Nay, J., 'Process Instrumentation for Westinghouse Nuclear Steam Supply System (4 Loop Plant)' WCAP-7671, May 10, 1971 (Non-Proprietary).

2. Katz, D. N., 'Solid State Logic Protection System Description, WCAP-7488-L, March 3, 1971 (Proprietary) and WCAP-7672 June, 1971 (Non-Proprietary).

3. The Institute of Electrical and Electronics Engineers, Inc., IEEE Standard: 'Criteria for Protection System for Nuclear Power Generating Stations,' IEEE Standard 279-1971.

4. Mesmeringer, J. C., 'Failure Mode and Effects Analysis (FMEA) of the Engineered Safety Features Actuation System, WCAP-8584, Revision 1, February 1980 (Proprietary) and WCAP-8760, February 1980 (Non-Proprietary).

5. Erin, L. E. "Eagle 21 Microprocessor Based Process Protection System," (Westinghouse Topical Report, January 1987). 63

I29

0794 PKG

Insert 29 to Page 7.3-28

5. Erin, L. E., "Topical Report, Eagle 21 Microprocessor-Based Process Protection System," WCAP-12374 Rev. 1 December 1991 (Westinghouse Proprietary Class 2); WCAP-12375 Rev. 1 December 1991 (Westinghouse Proprietary Class 3)

6. Reagan, J. R., "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar Units 1 and 2, Eagle 21 Version," WCAP-12096 Rev. 5 (Westinghouse Proprietary Class 2)

0794 PKG
Replace with Insert 30

TABLE 7.3-1

INSTRUMENTATION OPERATING CONDITION FOR ENGINEERED SAFETY FEATURES

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	SAFETY INJECTION		
	a. Manual	2	1
	b. High Containment Pressure	3	2
	c. High Differential Pressure Between Steam Lines	12 (3/steam line)	2 in any one steam line
	d. Pressurizer Low Pressure*	3	2
	e. High Steam flow in 2/4 Steam Lines Coincident with low-low T_{avg} or low Steam Line Pressure	2/steam line	1/steam line in any two lines
		4 T_{avg} Signals	2
		4 Pressure Signals	2

44

* Permissible bypass if reactor coolant pressure less than 2000 psig 44

Revised by Amendment 44

TABLE 7.3-1

INSTRUMENTATION OPERATING CONDITION FOR ENGINEERED SAFETY FEATURES

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	SAFETY INJECTION		
1a.	Manual	2	1
1b.	High Containment Pressure	3	2
1c.	Pressurizer Low Pressure*	3	2
1d.	Low Steamline Pressure (Lead-Lag compensated)*	12 (3/steamline)	2/3 in any steamline
2.	CONTAINMENT SPRAY		
2a.	Manual**	4	2
2b.	Containment Pressure High-High	4	2

* Interlocked with Permissive P-11; see functional description of P-11 in Table 7.3-3.

** Manual actuation of containment spray is accomplished by actuating either of two sets (two switches per set). Both switches in a set must be actuated to obtain a manually initiated spray signal. The sets will be wired to meet separation and single failure requirements of IEEE Standard 279-1971. Simultaneous operation of two switches is desirable to prevent inadvertent spray actuation.

0794 PKG

Delete — info. included in Insert 30

TABLE 7.3-1 (Continued)

INSTRUMENTATION OPERATING CONDITION FOR ENGINEERED SAFETY FEATURES

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
2.	CONTAINMENT SPRAY		
	a. Manual**	4	2
	b. Containment Pressure High-High	4	2

**Manual actuation of containment spray is accomplished by actuating either of two sets (two switches per set). Both switches in a set must be actuated to obtain a manually initiated spray signal. The sets will be wired to meet separation and single failure requirements of IEEE Standard 279-1971. Simultaneous operation of two switches is desirable to prevent inadvertant spray actuation.

0794 PKG

Replace with Insert 31

TABLE 7.3-2

INSTRUMENT OPERATING CONDITIONS FOR ISOLATION FUNCTIONS

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	CONTAINMENT ISOLATION		
	a. Automatic Safety Injection (Phase A)	See Item No. 1 (b) through (e) of Table 7.3-1	
	b. Containment Pressure (Phase B)	See Item No. 2 (b) of Table 7.3-1	
	c. Manual		
	Phase A	2	1
	Phase B	See Item No. 2 (a) of Table 7.3-1	
2.	STEAM LINE ISOLATION		
	a. High Steam Flow in 2/4 Steam Lines Coincident with low-low T_{avg} or Low Steam Pressure	See Item No. 1 (e) of Table 7.3-1	
	b. Containment Pressure (High-High)	See Item No. 2 (b) of Table 7.3-1	
	c. Manual	1/loop	1/loop
3.	FEEDWATER LINE ISOLATION		
	a. Safety Injection	See Item No. 1 of Table 7.3-1	
	b. Steam Generator High-High Level 2/3 on any Steam Generator	3/loop	2/loop

0794 PKG

Insert 31 to Table 7.3-2

TABLE 7.3-2

INSTRUMENTATION OPERATING CONDITION FOR ISOLATION FUNCTIONS

NO.	FUNCTIONAL UNIT	NO. OF CHANNELS	NO. OF CHANNELS TO TRIP
1.	CONTAINMENT ISOLATION		
1a.	Automatic Safety Injection (Phase A)	See Item No. 1b through 1~~e~~d of Table 7.3-1	
1b.	Containment Pressure High-High (Phase B)	~~See Item No. 2b of Table 7.3-1.~~ 4	2
1c.	Manual Phase A	2	1
	Phase B	See Item No. 2a of Table 7.3-1.	
2.	STEAMLINE ISOLATION		
2a.	Low Steamline Pressure*	~~See Item No. 1d of Table 7.3-1.~~ 12 (3/steamline)	2/3 in any steamline
2b.	High Steamline Pressure Rate (Rate-Lag compensated)*	12 (3/Steamline)	2/3 in any steamline
2c.	Containment Pressure High-High	~~See Item No. 2b of Table 7.3-1.~~ 4	2
3.	FEEDWATER LINE ISOLATION		
3a.	Safety Injection	See Item No. 1 of Table 7.3-1.	
3b.	Steam Generator High-High Level ~~2/3 in any Steam Generator~~	~~3/loop~~ 12 (3/steam Generator)	~~2/loop~~ 2/3 in any Steam Generator

* Interlocked with Permissive P-11; see functional description of P-11 in Table 7.3-3.

0794 PKG

TABLE 7.3-3

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Input	Function Performed
P-4	Reactor trip	Actuates turbine trip
		Closes main feedwater valves on T_{avg} below low setpoint
		Prevents opening of main feedwater valves which were closed by safety injection or High-High steam generator water level
		Allows manual block of the automatic reactuation of safety injection
	Reactor not tripped	Defeats the block preventing automatic reactuation of safety injection
Replace with Insert 33		
~~P-11~~	~~2/3 Pressurizer pressure below setpoint~~	~~Allows manual block of safety injection actuation on low pressurizer pressure signal~~
	~~2/3 Pressurizer pressure above setpoint~~	~~Defeats manual block of safety injection actuation~~ 45
P-12	2/4 T_{avg} below low-low setpoint	Blocks steam dump
		~~This signal in coincidence with high steamline flow actuates safety injection and steamline isolation~~ condenser dump valves
		Allows manual bypass of steam dump block for the cooldown valves only
		~~Allows manual block of safety injection actuation on high steamline flow~~

0794 PKG

Insert 33 to Table 7.3-3

P-11	2/3 Pressurizer pressure below setpoint	Allows manual block of safety injection actuation on low pressurizer pressure signal. Allows manual block of safety injection and steamline isolation on low steamline pressure. Steamline isolation on high negative rate steamline pressure is permitted when this manual block is accomplished.
	2/3 Pressurizer pressure above setpoint	Defeats manual block of safety injection actuation. Defeats manual block of safety injection and steamline isolation on low steamline pressure and defeats steamline isolation on high negative rate steamline pressure.

TABLE 7.3-3 (Continued)

INTERLOCKS FOR ENGINEERED SAFETY FEATURES ACTUATION SYSTEM

Designation	Input	Function Performed
	3/4 T_{avg} above low-low set-point	Defeats the manual bypass of steam dump block
		~~Defeats manual block of S.I. actuation on high steamline flow~~
P-14	2/3 Steam generator water level above set-point on any steam generator	Closes all feedwater control valves and isolation valves
		Trips all main feedwater pumps which closes the pump discharge valves
		Actuates turbine trip

0794 PKG

7.5.3 Design Criteria

7.5.3.1 Scope

The following criteria establish requirements for the functional performance and reliability of the safety-related Post-Accident Monitoring System (PAMS) for nuclear reactors producing steam for electric power generation. For purposes of these criteria, the nuclear power generating station safety-related PAMS encompasses those electric and mechanical devices and circuitry which provide information needed to:

1. Enable the operator to take the correct manual action during the course of a Condition II, III, or IV fault or during recovery from a Condition II, III, or IV fault.

2. Maintain safe shutdown.

7.5.3.2 Definitions

The definitions in this section establish the meanings of words in the context of their use in these criteria.

Channel - An arrangement of components and modules or software as required to generate a single information signal to monitor a generating station condition.

Components - Items from which the system is assembled (for example, resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

Module - Any assembly of interconnected components which constitutes an identifiable device instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Post Accident Monitoring Function - A post accident monitoring function consists of the sensing of one or more variables associated with a particular generating station condition, signal processing, and the presentation of visual information to the operator.

Plasma Display - A display of information on a screen via a dot-matrix plasma. This display may be either alphanumerical, graphical, or both.

Insert A

Insert A to Page 7.5-2 0794 PKG

Software - The entire set of programs, procedures, and related documentation associated with a system, especially a computer system.

Monitoring System - Where not otherwise qualified, the words 'monitoring system' refer to the nuclear power generating station PAMS as defined in Table 7.5-1.

Type Test - Tests made on one or more units to verify adequacy of design.

7.5.3.3 Requirements

7.5.3.3.1 General Functional Requirements

The nuclear power generating station PAMS functions with precision and reliability to continuously display the appropriate monitored variables. This requirement applies for the full range of conditions and performance enumerated.

7.5.3.3.2 Information Readout

One of the channels used to monitor each parameter is recorded to provide a historical record of the behavior of the parameters. In general, the recorders are not redundant and do not meet the single-failure criteria. The recorders for PAM Category I parameters do not have their own isolation amplifiers because the incoming signal has already been isolated from the post-accident monitoring channel. Two-pen recorders are used in most cases permitting two channels to be recorded on one recorder. The essential raw cooling water flow and the auxiliary feedwater flow are recorded by the plant computer with hard copy available on demand by the operator.

The Inadequate Core Cooling Monitoring (ICCM) System, consisting of the Reactor Vessel Level Instrumentation System (RVLIS), Incore Thermocouple (ICTC) System and the Subcooling Margin Monitor, displays the status of each of its systems on a plasma display. In addition, two three-pen recorders for ICTC monitoring, two digital subcooling margin temperature meters, and the plant computer are also available for use.

7.5.3.3.3 Single Failure Criterion

Any single failure within the PAMS will not result in the loss of the monitoring function. ('Single failure' includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a 'single failure' even though several transistor failures result. Mechanical damage to a mode switch would be a 'single failure' although several channels might become involved.)

7.5.3.3.4 Quality of Components, ~~and~~ Modules and Software

Components and modules are of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels were achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

verification and validation

0794 PKG

The Reactor Control System controls the reactor coolant average temperature by regulation of control rod bank position. The reactor coolant loop average temperatures are determined from hot leg and cold leg measurements in each reactor coolant loop. There is an average coolant temperature (T_{avg}) computed for each loop, where:

$$T_{avg} = \frac{T_{hot} + T_{cold}}{2}$$

(See section 7.2.1.1.4 for discussion of Tavg calculation and equations used to derive Tavg.)

The error between the programmed reference temperature (based on turbine inpulse chamber pressure) and the highest of the T_{avg} temperatures (which is processed through a lead-lag compensation unit) from each of the reactor coolant loops constitutes the primary control signal, as shown in general on Figure 7.7-1. The system is capable of restoring coolant average temperature to the programmed value following a change in load. The programmed coolant temperature increases linearly with turbine load from zero power to the full power condition. The T_{avg} also supplies a signal to pressurizer level control, steam dump control and rod insertion limit monitoring.

The temperature channels needed to derive the temperature input signals for the Reactor Control System are fed from protection channels via isolation ~~amplifiers.~~ devices

An additional control input signal is derived from the reactor power versus turbine load mismatch signal. This additional control input signal improves system performance by enhancing response and reducing transient peaks.

7.7.1.2 Rod Control System

7.7.1.2.1 Description

The full length rod control system receives rod speed and direction signals from the T_{avg} control system. The rod speed demand signal varies over the corresponding range of 5.0 to 45 inches per minute (8 to 72 steps/minute) depending on the magnitude of the input signal. The rod direction demand signal is determined by the positive or negative value of the input signal. Manual control is provided to move a control bank in or out at a prescribed fixed speed.

When the turbine load reaches approximately 15 percent of rated load, the operator may select the "AUTOMATIC" mode, and rod motion is then controlled by the reactor control systems. A permissive interlock C-5 (See Table 7.7-1) derived from measu-

0794 PKG

The water inventory in the Reactor Coolant System is maintained by the Chemical and Volume Control System. During normal plant operation, the charging flow varies to produce the flow demanded by the pressurizer water level controller. The pressurizer water level is programmed as a function of coolant average temperature, with the highest average temperature (auctioneered) being used. The pressurizer water level decreases as the load is reduced from full load. This is a result of coolant contraction following programmed coolant temperature reduction from full power to low power. The programmed level is designed to match as nearly as possible the level changes resulting from the coolant temperature changes.

To control pressurizer water level during startup and shutdown operations, the charging flow is manually regulated from the Main Control Room.

A block diagram of the Pressurizer Water Level Control System is shown on Figure 7.7-5.

7.7.1.7 Steam Generator Water Level Control

Each steam generator is equipped with a three element feedwater flow controller which maintains a programmed water level which is a function of nuclear power. The three element feedwater controller regulates the feedwater valve by continuously comparing the feedwater flow signal, the steam generator water level signal, the programmed level and the pressure compensated steam flow signal. ~~The steam generator water level signal origin, although derived from the protection system, is from a different channel than the one which is used on Figure 7.2-1 (Sheet 3) for the low feedwater flow reactor trip.~~ In addition, the feedwater pump speed is varied to maintain a programmed pressure differential between the steam header and the feed pump discharge header. The speed controller continuously compares the actual ΔP with a programmed ΔP_{ref} which is a linear function of steam flow. Continued delivery of feedwater to steam generators is required as a sink for the heat stored and generated in the reactor following a reactor trip and turbine trip. An override signal closes the feedwater valves when the average coolant temperature is below a given temperature and the reactor has tripped. Manual override of the Feedwater Control System is available at all times. 62

I32

~~As noted above, the steam generator water level signal used to control the steam generator water level is derived from the protection system. However, the channel is independant of the level channels used for reactor trip on low steam generator water level coincident with steam flow feedwater flow mismatch, which are protection grade channels.~~ For the evaluation of the compliance of steam generator low water level channels to Section 4 (Control and Protection System Interaction) of IEEE 279-1971, Std.

Refer to Section 7.2.2.3.5.

low-low

0794 PKG

Insert 32 to Page 7.7-15

Three steam generator water level signals are provided to the Feedwater Control System via a control grade Median Signal Selector (MSS). The MSS installed in the control system provides a "median" signal for use by the control system to initiate control system actions based on this signal. Reference [6]

0794 PKG

Standard 279-1971, refer to Section 7.2.2.3.5 and to Section 4.4.5 of Reference[5] listed in Section 7.2. The following conclusions of the evaluation are presented in Reference[5]:

A spurious high water level signal from the protection channel used for control tends to close the feedwater valve. This level channel is independent of the level and flow channels used for reactor trip on low flow coincident with low level.

a) A rapid increase in the level signal completely stops feedwater flow and actuates a reactor trip on low feedwater flow coincident with low level.

b) A slow drift in the level signal may not actuate a low feedwater signal. Since the level decrease is slow, the operator has time to respond to low level alarms. Since only one steam generator is affected, automatic protection is not mandatory and reactor trip on two-out-of-three low-low level is acceptable.

A block diagram of the Steam Generator Water Level Control System is shown in Figures 7.7-6 and 7.7-7.

7.7.1.8 Steam Dump Control

The Steam Dump System is designed to accept a 50% loss of net load without tripping the reactor.

The Automatic Steam Dump System is able to accomodate this abnormal load rejection and to reduce the effects of the transient imposed upon the Reactor Coolant System. By bypassing

0794 PKG

Operating plant experience has demonstrated the adequacy of the incore instrumentation in meeting the design bases stated.

7.7.1.10 Control Board

A control board functional layout is shown on Figure 7.7-10.

The control board layout is based on operator ease in relating the control board devices to the physical plant and in determining at a glance the status of related equipment. This is referred to as providing a functional layout. Within the boundaries of a functional layout, modules are arranged in columns of control functions associated with separation trains defined for the RPS and ESFAS.

Monitor lights are provided in two places on the control board for automatically actuated valves and components for Phase A and B containment isolation and containment vent isolation with the exception of all Sampling and Water Quality system valves as well as those EGTS valves that are not in the containment annulus vacuum fans flowpath. Indicating circuits are paralleled to red (open) and green (closed) lights located next to the control station and to red and green split lens lights on the Containment Isolation Status panel (CISP).

EGTS containment isolation valves not in the containment annulus vacuum fans flowpath have red and green position indication lights located on the control board at the control station.

Position indication for the Sampling and Water Quality system containment isolation valves is provided by paralleling indicating circuits to red and green lights at the local control station in the Auxiliary Building and to red and green split-lens lights on the CISP.

For a description of separation of wiring within the control board refer to Section 7.1.2.2.2.

7.7.1.11 Boron Concentration Measurement System

The boron concentration measurement system is a monitoring system of the boron concentration in the RCS. This system is provided by Combustion Engineering and provides continuous readout in the MCR of boron concentration in the RCS for the reactor operator. This system provides no control function. The boron concentration in the reactor coolant system is measured in the letdown stream of the CVCS. In addition to the continuous readout in the MCR, a strip chart recorder with the boron concentration in the RCS is provided so that trends in the boron concentration can be monitored by the control room operator.

This system is not required for safety because it provides a monitoring function only.

7.7.1.12 Anticipated Transient Without Scram Mitigation System Actuation Circuitry (AMSAC)

To meet the ATWS Final Rule, Watts Bar added equipment diverse from the existing reactor trip system. The existing reactor trip system is composed of the ~~Foxboro~~

0794 PKG

Process Protection System

~~H-Line Process Instrumentation and Control System,~~ Westinghouse Eagle 21 ~~Instrumentation~~, and the Westinghouse Solid State Protection System (SSPS). The AMSAC equipment consists of a freestanding panel which is installed in the Unit 1 auxiliary instrument room of the Control Building. This modification is diverse from sensor output to the final actuation device. The AMSAC is designed to automatically initiate auxiliary feedwater and trip the turbine under conditions indicative of an ATWS event. Steam generator blowdown is isolated as a result of Auxiliary Feedwater Start. An ATWS event will be detected when low-low level in three out of four steam generators is coincidental with the turbine at or above 40% load. An AMSAC actuation will ensure the RCS pressure will remain below the pressure that will satisfy the ASME Boiler and Pressure Vessel Code Level C services limit stress criteria.

A turbine trip and startup of all AFW pumps occurs when steam generator level less than 12% below 80% power or less than 25% above 80% power within present time delays which will allow generation of an AMSAC signal. The AMSAC signal is generated by low-low water level signals in the steam generators. The AMSAC coincidence logic is 3 out of 4 (3/4) low-low level signals with one channel per steam generator and the turbine at or above 40% load. Load is determined by two pressure transmitters measuring 1st stage turbine pressure. When 2 of 2 transmitters sense 40% load, AMSAC is armed. Only one of the three narrow range level channels per steam generator is used for input to AMSAC coincidence logic. AMSAC actuation is required at a setpoint that is less than the existing RPS steam generator low-low level setpoint. The requirement allows the operation of the RPS before AMSAC.

There is no AMSAC interface to the RPS. The four steam generator level signals are from buffers in the Auxiliary Feedwater System. Signals from two turbine impulse chamber dedicated pressure transmitters are used to indicate if the plant is at or above 40% load and then to determine the trip setpoint. The output signals to start the Auxiliary Feedwater pumps and trip the turbine are from interposing relays.

AMSAC is designed so that once actuated, the completion of mitigating action shall be consistent with the plant turbine trip and auxiliary feedwater circuitry. AMSAC auxiliary feedwater initiation and turbine trip goes to completion after actuation. The output relays are energized to actuated in order to prevent spurious trips and false status indication on loss of power or logic.

The AMSAC contains a manual test panel and built in self checks to annunciate faults automatically. On-line testing capability is incorporated in the AMSAC system. The blocking switch prevents inadvertent actuation by inhibiting the output relays before enabling the test function. A test status output shall inform the control room that the AMSAC is in the test mode and actuation is bypassed.

AMSAC is ~~power~~ powered from 120V ac preferred power which is independent from the RPS power supply.

The AMSAC system, including input comparators, logic processing and actuation output to isolation relays, is non-safety. The QA requirements are given in NRC Generic Letter 85-06, "Quality Assurance Guidance of ATWS Equipment that is not Safety-Related." The AMSAC cabinet is qualified seismic Category I(L).

of the plant control systems are postulated in the analysis of off-design operational transients and accidents covered in Chapter 15, such as, the following:

1. Uncontrolled rod cluster control assembly withdrawal from a subcritical condition.

2. Uncontrolled rod cluster control assembly withdrawal at power.

3. Rod cluster control assembly misalignment

4. Loss of external electrical load and/or turbine trip

5. Loss of all AC power to the station auxiliaries (Station Blackout)

6. Excessive heat removal due to feedwater system malfunctions

7. Excessive load increase incident

8. Accidental depressurization of the Reactor Coolant System.

These analyses will show that a reactor trip setpoint is reached in time to protect the health and safety of the public under those postulated incidents and that the resulting coolant temperatures produce a DNBR well above the limiting value of 1.30. Thus, there will be no cladding damage and no release of fission products to the Reactor Coolant System under the assumption of these postulated worst case failure modes of the Plant Control System.

7.7.2.1 Separation of Protection and Control System

In some cases, it is advantageous to employ control signals derived from individual protection channels through isolation devices ~~amplifiers~~ contained in the protection channel. As such, a failure in the control circuitry does not adversely affect the protection channel. Test results have demonstrated the adequacy for fault voltages up to 580 volts ac and 250 volts dc. Cable trays carrying isolation ~~amplifier~~ device outputs will contain no cables in excess of these voltages. 39

Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition,

0794 PKG

The steam dump and Feedwater Control Systems are designed to prevent the average coolant temperature from falling below the programmed no load temperature following the trip to ensure adequate reactivity shutdown margin.

7.7.3 Suppliers

All control systems not required for safety discussed in Section 7.7, including the Reactor Control System, the Rod Control System, the Plant Control System Interlocks, the Pressurizer Pressure Control, the Pressurizer Water Level Control, the Steam Generator Water Level Control, the Steam Dump Control, and the Incore Instrumentation are provided by Westinghouse. 6.

REFERENCES

1. Blanchard, A. E. and Katz, D. N., 'Solid State Rod Control System, Full Length,' WCAP-9012-L, March, 1970 (Proprietary) and WCAP-7778, December, 1971 (Non-Proprietary).

2. Lipchak, J. B. and Stokes, R. A., 'Nuclear Instrumentation System,' WCAP-8255, January, 1974.

3. Blanchard, A. E., 'Rod Position Monitoring,' WCAP-7571, March, 1971.

4. Loving, J. J., 'Incore Instrumentation (Flux-Mapping System and Thermocouples,' WCAP-7607, July, 1971.

5. Shopsky, W. E., 'Failure Mode and Effects Analysis (FMEA) of the Solid State Full Length Rod Control System,' WCAP-8976, August 1977.

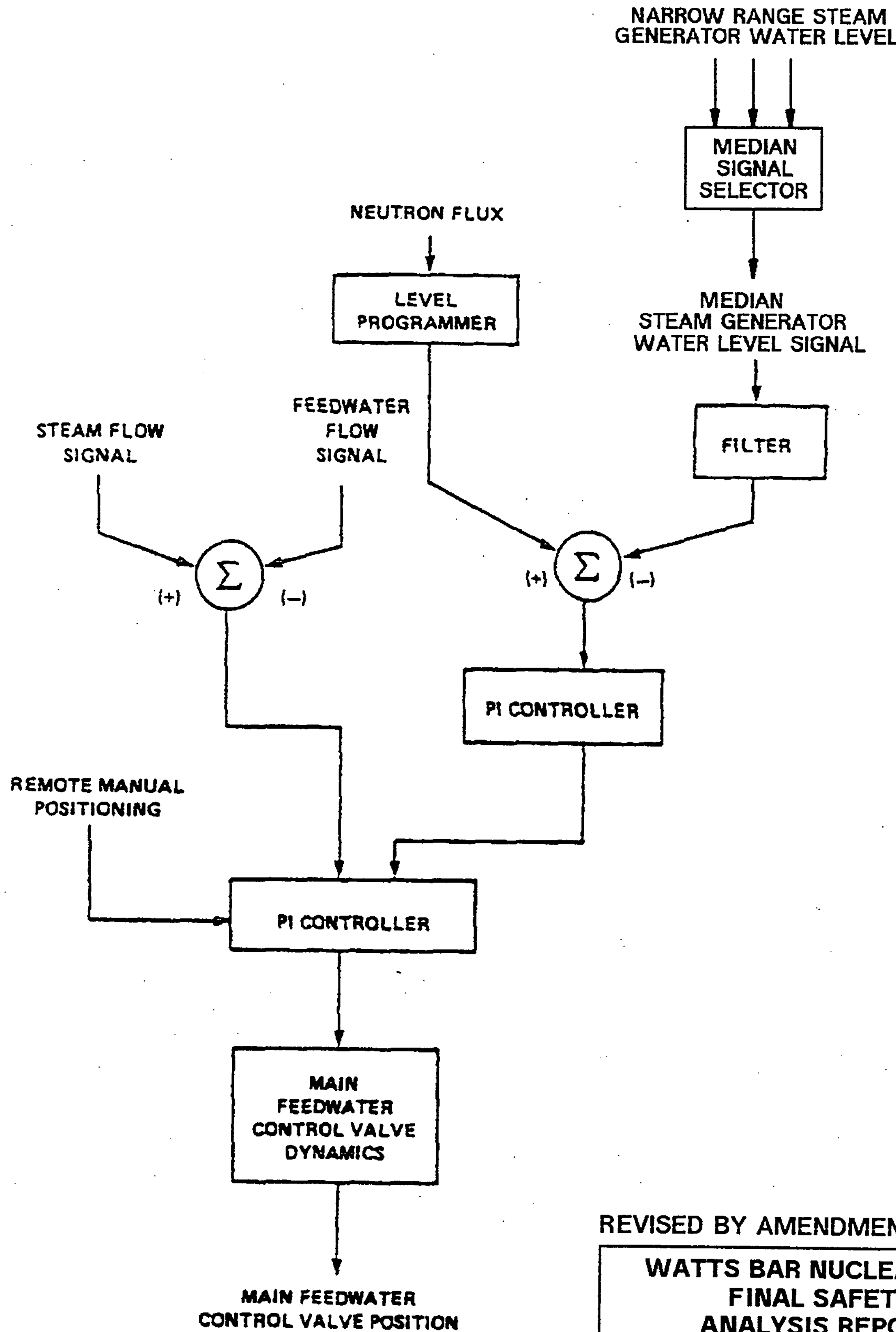
36

0794 PKG

Insert 36 to Page 7.7-28

6. Mermigos, J. F., "Median Signal Selector for Foxboro Series Process Instrumentation Application to Deletion of Low Feedwater Flow Reactor Trip," WCAP-12417 October 1989 (Westinghouse Proprietary Class 2); WCAP-12418 October 1989 (Westinghouse Proprietary Class 3)

0794 PKG



REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

BLOCK DIAGRAM OF
STEAM GENERATOR
WATER LEVEL CONTROL SYSTEM
FIGURE 7.7-6

TABLE 8.1-1 (cont)

SAFETY LOADS AND FUNCTIONS

I39

Safety Loads	Function	Power
Solid-State Protection System	Prevents reactor from operating in unsafe condition	120V a.c.
Nuclear Instrument System	Monitors reactor power level for reactor control and trip logic	120V a.c.
Auxiliary Relay Racks	Auxiliary relays for process control	120V a.c. & 125V d.c.
Power Switchgear	Control power for power switchgear	125V d.c.
Vital Inverter	Supplies power to the vital instrument buses	125V d.c.
Reactor Trip Switchgear Control	Trips reactor	125V d.c.
Diesel Generator Control	Remote control of diesel generators	125V d.c.
Auxiliary Feed Pump Turbine	Automatic start of auxiliary feed pump turbine	125V d.c.
Emergency Lighting Cabinet	Provides power to emergency lighting panel	125V d.c.
Solenoid Valves	Controls flow through safety related valves (pneumatic valves with solenoid pilots)	125V d.c.

0794 PKG

Insert 39 to Table 8.1-1

Process Protection System	Monitors process parameters which initiate actuation of reactor trip and engineering safeguards systems	120 VAC

0794 PKG

The safety valves provide 100 percent relieving capacity to protect the system from overpressure. The capacity provided by the atmospheric relief valves is over and above the safety valve capacity. The atmospheric relief valves, which have a set pressure slightly lower than the safety valves, prevent unnecessary opening of the safety valves.

Four atmospheric relief valves have been provided per unit (one per steam generator).

Bidirectional steam line isolation valves are installed to protect the plant during the following accident situations:

1. Break in the steam line piping either inside or outside the containment.

2. Break in the feedwater piping downstream of the last check valve before the steam generator.

3. Steam generator tube rupture.

The main steam line isolation valves are 32-inch wye type bidirectional globe, straight through flow, air to open, spring to close. These valves are capable of closing within 5 seconds after receipt of a closure signal on a 'high-high' containment pressure signal, ~~or high steam flow coincident with low steam generator pressure or low reactor coolant T_{avg}~~ low steamline pressure, or high steamline pressure rate as shown in Figures 10.3-8 and 10.3-5. 42

For accident situation No. 1, inside containment, the steam generator associated with the damaged line discharges completely into the Containment. The other steam generators would act to feed steam through the interconnecting header to reverse flow into the damaged line and then release into the Containment. The 5-second closing time for the isolation valves in the other three lines will limit containment pressure rise below design pressure. If any of these three valves fail to close, protection is provided by closure of the valve in the broken line. Hence, redundancy is provided to allow for a single failure of any one isolation valve.

0794 PKG

15.1 CONDITION I - NORMAL OPERATION AND OPERATIONAL TRANSIENTS

Condition I occurrences are those which are expected frequently or regularly in the course of power operation, refueling, maintenance, or maneuvering of the plant. As such, Condition I occurrences are accommodated with margin between any plant parameter and the value of that parameter which would require either automatic or manual protective action. Inasmuch as Con- In as much dition I occurrences occur frequently or regularly, they must be considered from the point of view of affecting the consequences of fault conditions (Conditions II, III and IV). In this regard, analysis of each fault condition described is generally based on a conservative set of initial conditions corresponding to adverse conditions which can occur during Condition I operation. the most adverse set of

A typical list of Condition I events is listed below:

1. Steady state and shutdown operations

   a. Power operation (≈ 15 to 100 percent of full power)

   b. Start up (or standby) (critical, 0 to 15 percent of full power)

   c. Hot shutdown (subcritical, Residual Heat Removal System isolated)

   d. Cold shutdown (subcritical, Residual Heat Removal System in operation)

   e. Refueling

2. Operation with permissible deviations

   Various deviations which may occur during continued operation as permitted by the plant Technical Specifications must be considered in conjunction with other operational modes. These include:

   a. Operation with components or systems out of service (such as power operation with a reactor coolant pump out of service)

   b. Leakage from fuel with cladding ~~clad~~ defects

   c. Radioactivity in the reactor coolant
      i. Fission products
      ii. Corrosion products
      iii. Tritium

0794 PKG

d. Operation with steam generator leaks up to the maximum allowed by the Technical Specifications

e. Testing as allowed by the Technical Specifications

3. Operational transients

a. Plant heatup and cooldown (up to 100°F/hour for the Reactor Coolant System; 200°F/hour for the pressurizer)

b. Step load changes (up to ± 10 percent)

c. Ramp load changes (up to 5 percent/minute)

d. Load rejection up to and including design load rejection transient

15.1.1 Optimization of Control Systems

A ~~control system~~ setpoint study WAS ~~has been~~ performed ~~(WCAP 9159)~~ in order to simulate performance of the reactor control and protection systems. In this study, emphasis ~~is~~ WAS placed on the development of a control system which will automatically maintain prescribed conditions in the plant even under ~~a~~ the most conservative set of reactivity parameters with respect to both system stability and transient performance. 53

For each mode of plant operation, a group of optimum controller setpoints ~~is~~ WAS determined. In areas where the resultant setpoints ~~are~~ were different, compromises based on the optimum overall performance, ~~are~~ were made and verified. A consistent set of control system parameters ~~is~~ WAS derived, satisfying plant operational requirements throughout the core life and for power levels between 15 and 100 percent.

The study ~~will comprise~~ comprised an analysis of the following control systems: rod cluster control assembly, steam dump, steam generator level, pressurizer pressure and pressurizer level.

15.1.2 Initial Power Conditions Assumed In Accident Analyses

15.1.2.1 Power Rating

Table 15.1-1 lists the principle power rating values which are assumed in analyses performed in this section. Two ratings are given:

1. The guaranteed Nuclear Steam Supply System thermal power output. This power output includes the thermal power generated by the reactor coolant pumps.

0794 PKG

2. The Engineered Safety Features design rating. The Westinghouse supplied Engineered Safety Features are designed for a thermal power higher than the guaranteed value in order not to preclude realization of future potential power capability. This higher thermal power value is designated as the Engineered Safety Features design rating. This power output includes the thermal power generated by the reactor coolant pumps.

Where initial power operating conditions are assumed in accident analyses, the "guaranteed Nuclear Steam Supply System thermal power output" plus allowance for errors in steady state power determination is assumed. Where demonstration of adequacy of the containment and Engineered Safety Features are concerned, the "Engineered Safety Features design rating" plus allowance for error is assumed. The thermal power values used for each transient analyzed are given in Table 15.1-2. ~~In all cases where the 3579 MWt rating is used in an analysis, the resulting transients and consequences are conservative compared to using the 3425 MWt rating.~~

15.1.2.2 Initial Conditions

For accident evaluation, the initial conditions are obtained by adding the maximum steady state errors to rated values. The following steady state errors are considered:

1.	Core power	± 2 percent allowance for calorimetric error
2.	Average Reactor Coolant System Temperature	± 6.5°F allowance for controller deadband and measurement error
3.	Pressurizer pressure	± 30 psi allowance for steady state fluctuations and measurement error

Initial values for core power, average Reactor Coolant System temperature and pressurizer pressure are selected to minimize the initial DNBR unless otherwise stated in the sections describing specific accidents.

replace with Insert A

15.1.2.3 Power Distribution

The transient response of the reactor system is dependent on the initial power distribution. The nuclear design of the reactor core minimizes adverse power distribution through the placement of control rods and operation instructions. The power distribution may be characterized by the radial factor $F_{\Delta H}$ and the total peaking factor F_q. The peaking factor limits are given in the Technical Specifications.

INSERT A to Page 15.1-5

0794 PKG

15.1.2.2 Initial Conditions

For accident evaluation, the initial conditions are obtained by adding maximum steady state errors to rated values. The following steady state errors are considered:

1.	Core power	± 2 percent allowance calorimetric error
2.	Average Reactor Coolant System temperature	± 5.5 °F allowance for deadband and and measurement error
3.	Pressurizer pressure	± 46 psi allowance for steady state fluctuations and measurememt error

For some accident evaluations, an additional 1.0 °F is added to the average Reactor Coolant System temperature to account for steam generator fouling.

Initial values for core power, average Reactor Coolant System temperature and pressurizer pressure are selected to minimize the initial DNBR unless otherwise stated in the sections describing specific accidents.

0794 PKG

For transients which may be DNB limited the radial peaking factor is of importance. The radial peaking factor increases with decreasing power level due to rod insertion. This increase in $F_{\Delta H}$ is included in the core limits illustrated in Figure 15.1-1. All transients that may be DNB limited are assumed to begin with a value of $F_{\Delta H}$ consistent with the initial power level defined in the Technical Specifications.

The axial power shape used in the DNB calculation is the 1.55 chopped cosine as discussed in Section 4.4.3.2.2.

For transients which may be overpower limited the total peaking factor F_q is of importance. The value of F_q may increase with decreasing power level such that full power hot spot heat ~~flux~~ is not exceeded (i.e. F_q x Power = design hot spot heat flux). All transients that may be overpower limited are assumed to begin with a value of F_q consistent with the initial power level as defined in the Technical Specifications.

The value of peak KW/ft can be directly related to fuel temperature as illustrated on Figures 4.4-1 and 4.4-2. For transients which are slow with respect to the fuel rod thermal time constant the fuel temperatures are illustrated on Figures 4.4-1 and 4.4-2. For transients which are fast with respect to the fuel rod thermal time constant, for example, rod ejection, a detailed heat transfer calculation is made.

15.1.3 Trip Points And Time Delays To Trip Assumed In Accident Analyses

A reactor trip signal acts to open two trip breakers connected in series feeding power to the control rod drive mechanisms. The loss of power to the mechanism coils causes the mechanisms to release the rod cluster control assemblies which then fall by gravity into the core. There are various instrumentation delays associated with each trip function, including delays in signal actuation, in opening the trip breakers, and in the release of the rods by the mechanisms. The total delay to trip is defined as the time delay from the time that trip conditions are reached to the time the rods are free and begin to fall. Limiting trip setpoints assumed in accident analyses and the time delay assumed for each trip function are given in Table 15.1-3. Reference is made in that table to overtemperature and overpower ΔT trip shown in Figure 15.1-1.

Insert B

The difference between the limiting trip point assumed for the analysis and the nominal trip point represents an allowance for instrumentation channel error and setpoint error. During ~~plant~~ preoperational start-up tests, it is demonstrated that actual instrument errors and time delays are equal to or less than the assumed values. Additionally, protection system channels are calibrated and instrument response times determined periodically in accordance with the plant Technical Specifications.

at-15.1/1

0794 PKG

INSERT ~~A~~ B to Page 15.1-6

Accident analyses which assume the S/G Low-Low Water Level trip signal to initiate protection functions may be affected by the Trip Time Delay (TTD) (Reference 21) system, which was developed to reduce the incidence of unnecessary feedwater related reactor trips.

The TTD imposes a system of pre-determined delays upon the S/G Low-Low level reactor trip and auxiliary feedwater initiation. The values of these delays are based upon (1) the prevailing power level at the time the Low-Low level trip setpoint is reached, and by (2) the number of steam generators in which the Low-Low level trip setpoint is reached. The TTD delays the reactor trip and auxiliary feedwater actuation in order to provide time for corrective action by the operator or for natural stabilization of shrink/swell water level transients. The TTD is primarily designed for low power or startup operations.

15.1.4 Instrumentation Drift And Calorimetric Errors - Power Range Neutron Flux

The instrumentation drift and calorimetric errors used in establishing the power range high neutron flux setpoint are presented in Reference 22.

The calorimetric error is the error assumed in the determination of core thermal power as obtained from secondary plant measurements. The total ion chamber current (sum of the top and bottom sections) is calibrated (set equal) to this measured power on a periodic basis.

The secondary power is obtained from measurement of feedwater flow, feedwater inlet temperature to the steam generators and steam pressure. High accuracy instrumentation is provided for these measurements with accuracy tolerances much tighter than those which would be required to control feedwater flow.

15.1.5 Rod Cluster Control Assembly Insertion Characteristic

The negative reactivity insertion following a reactor trip is a function of the acceleration of the rod cluster control assemblies and the variation in rod worth as a function of rod position. With respect to accident analyses, the critical parameter is the time of insertion up to the dashpot entry or approximately 85 percent of the rod cluster travel. ~~For accident analyses the insertion time to dashpot entry is conservatively taken as 2.7 seconds at thermal design flow and 3.65 seconds at mechanical design flow, based on D-Loop test results described in Reference 1.~~ The most limiting insertion time to dashpot entry used for accident analyses is 2.7 seconds. For the dropped rod cluster control assembly analysis (Section 15.2.3), a rod insertion time of 3.3 seconds is assumed (consistent with reference 21. The normalized rod cluster control assembly position versus time curve assumed in accident analyses is shown in Figure 15.1-2.

Figure 15.1-3 shows the fraction of total negative reactivity insertion for a core where the axial distribution is skewed to the lower region of the core. An axial distribution which is skewed to the lower region of the core can arise from an unbalanced xenon distribution. This curve is used as input to all point kinetics core models used in transient analyses.

There is inherent conservatism in the use of this curve in that it is based on a skewed flux distribution which would exist relatively infrequently. For cases other than those associated with unbalanced xenon distributions, significant negative reactivity would have been inserted due to the more favorable axial distribution existing prior to trip.

The normalized rod cluster control assembly negative reactivity insertion versus time curve corresponding to an insertion time to dashpot entry of 2.7 seconds is shown in Figure~~s~~ 15.1-4. The curve~~s~~ shown in ~~these~~ this figure~~s~~ ~~were~~ was obtained from Figures 15.1-2 and

0794 PKG

15.1-3. ~~Unless otherwise specified in the individual accident description, the reactivity versus time function corresponding to mechanical design flow was assumed.~~ A total negative reactivity insertion following a trip of 4 percent $\Delta k/k$ is assumed in the transient analyses except where

0794 PKG

specifically noted otherwise. This assumption is conservative with respect to the calculated trip reactivity worth available as shown in Table 4.3-3.

The normalized rod cluster control assembly the most limiting negative reactivity insertion versus time curve for an axial power distribution skewed to the bottom (Figure 15.1-4) is used in ~~those~~ transient analyses~~, for which a point kinetics core model is used~~. Where special analyses require use of three dimensional or axial one dimensional core models, the negative reactivity insertion resulting from the reactor trip is calculated directly by the reactor kinetics code and is not separable from the other reactivity feedback effects. In this case, the rod cluster control assembly position versus time of Figure 15.1-2 is used as code input. Unless the accident descriptions specify otherwise, the trip reactivity or position versus time curve corresponding to mechanical design flow was assumed in the analysis [20]. 63

15.1.6 <u>Reactivity Coefficients</u>

The transient response of the reactor system is dependent on reactivity feedback effects, in particular the moderator temperature coefficient and the Doppler power coefficient. These reactivity coefficients and their values are discussed in detail in Chapter 4.

In the analysis of certain events, conservatism requires the use of large reactivity coefficient values whereas in the analysis of other events, conservatism requires the use of small reactivity coefficient values. Some analyses such as loss of reactor coolant from cracks or ruptures in the Reactor Coolant System do not depend on reactivity feedback effects. The values used are given in Table 15.1-2; reference is made in that table to Figure 15.1-5 which shows the upper and lower bound Doppler power coefficients as a function of power, used in the transient analysis. The justification for use of conservatively large versus small reactivity coefficient values are treated on an event by event basis. To facilitate comparison, individual sections in which justification for the use of large or small reactivity coefficient values is to be found are referenced below:

Condition II Events		<u>Section</u>
1.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal From a Subcritical Condition	15.2.1
2.	Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	15.2.2
3.	Rod Cluster Control Assembly Misalignment	15.2.3
4.	Uncontrolled Boron Dilution	15.2.4

0794 PKG

the expense of adjacent colder rods. A conservative estimate of this effect is a reduction of 10 percent of the gamma-ray contribution or 3 percent of the total. Since the water density is considerably reduced at this time, an average of 98 percent of the available heat is deposited in the fuel rods, the remaining 2 percent being absorbed by water, thimbles, sleeves and grids. The net effect is a factor of 0.95 rather than 0.974, to be applied to the heat production in the hot rod.

15.1.9 Computer Codes Utilized

or referenced

are

Summaries of some of the principal computer codes used in transient analyses are given below. Other codes, in particular, very specialized codes in which the modeling has been developed to simulate one given accident, such as those used in the analysis of the Reactor Coolant System pipe rupture (Section 15.4), are summarized in their respective accident analyses sections. The codes used in the analyses of each transient have been listed in Table 15.1-2.

and which consequently have a direct bearing on the accident itself

15.1.9.1 ~~Factran~~ FACTRAN

FACTRAN calculates the transient temperature distribution in a cross section of a metal clad UO_2 fuel rod and the transient heat flux at the surface of the clad using as input the nuclear power and the time-dependent coolant parameters (pressure, flow, temperature, and density). The code uses a fuel model which exhibits the following features simultaneously:

1. A sufficiently large number of radial space increments to handle fast transients such as rod ejection accidents.

2. Material properties which are functions of temperature and a sophisticated fuel-to-clad gap heat transfer calculation.

3. The necessary calculations to handle post DNB transients: film boiling heat transfer correlations, Zircaloy-water reaction and partial melting of the materials.

FACTRAN is further discussed in Reference [12].

15.1.9.2 ~~BLKOUT~~ Deleted by Amendment 72

~~The BLKOUT Code is used to analyze specifically the long term (slow) transient behavior of the Reactor Coolant System process variables. The "two loop" analytical model employed permits studying effects caused by anomalous conditions in one loop using lumped parameters to describe the conditions of all remaining loops. The plant components simulated are the entire~~

0794 PKG

~~Reactor Coolant System including the pressurizer and the associated pressurizer control systems, the steam generator, Chemical and Volume Control System and the steam dump system.~~

~~The code is generally applicable for studying transients following flow or enthalpy, steam flow and charging or letdown flow.~~

~~BLKOUT is further discussed in Reference [13].~~

15.1.9.3 MARVEL

The MARVEL code is used to determine the detailed transient behavior of multi-loop pressurized water reactor systems caused by prescribed initial perturbations in process parameters. The code is useful in predicting plant behavior when different conditions are present in the loops. For analytical purposes, the physical, thermal and hydraulic characteristics of a multi-loop plant are represented by two "equivalent" loops. The perturbation is considered to occur in one or more physical loops. The other equivalent loop thus represents in lumped form, the remaining loops in the plant.

The code simulates the coolant flow through the reactor vessel, hot leg, cold leg, steam generator plus the pressurizer surge line. Neutron kinetics, fuel-clad heat transfer and the rod control system characteristics are modeled. Simulation of the Reactor Trip System, Engineered Safety Features (safety injection) and Chemical and Volume Control System is provided.

MARVEL determines plant behavior following perturbations in any of the following parameters:

1. Reactor Coolant System loop isolation
2. Reactor Coolant System loop flows
3. Core power
4. Reactivity
5. Feedwater enthalpies
6. Feedwater flow
7. Steamline isolation valves
8. Steam flow
9. Pressurizer auxiliary spray
10. Reactor trip
11. Steamline break
12. Feedwater line break
13. Reactor Coolant System leak
14. Safety Injection System
15. Steam dump

0794 PKG

MARVEL also has the capability of calculating the transient value of DNB ratio on the input from the core limits illustrated on Figure 15.1-1. The core limits represent the minimum value of DNBR as calculated for a typical or thimble cell.

MARVEL is further discussed in Reference [14].

15.1.9.4 LOFTRAN

The LOFTRAN program is used for studies of transient response of a pressurized water reactor system to specified perturbations in process parameters. LOFTRAN simulates a multi-loop system by a lumped parameter single loop model containing reactor vessel, hot and cold leg piping, steam generator (tube and shell sides) and the pressurizer. The pressurizer heaters, spray, relief and safety valves are also considered in the program. Point model neutron kinetics, and reactivity effects of the moderator, fuel, boron and rods are included. The secondary side of the steam generator utilizes a homogeneous, saturated mixture for the thermal transients and a water level correlation for indication and control. The reactor protection system is simulated to include reactor trips on neutron flux, overpower and overtemperature reactor coolant delta-T, high and low pressure, low flow, and high pressurizer level. Control systems are also simulated including rod control, steam dump, feedwater control and pressurizer pressure control. The Safety Injection System including the accumulators are also modeled.

LOFTRAN is a versatile program which is suited to both accident evaluation and control studies as well as parameter sizing.

LOFTRAN also has the capability of calculating the transient value of DNB ratio based on the input from the core limits illustrated on Figure 15.1-1. The core limits repr~~s~~esent the minimum value of DNBR as calculated for typical or thimble cell.

LOFTRAN is further discussed in Reference [15].

15.1.9.5 LEOPARD

The LEOPARD computer program determines fast and thermal neutron spectra, using only basic geometry and temperature data. The code optionally computes fuel depletion effects for a dimensionless reactor and recomputes the spectra before each discrete burnup step. 53

LEOPARD is further described in Reference [16].

0794 PKG

15.1.9.6 TURTLE

TURTLE is a two-group, two-dimensional neutron diffusion code featuring a direct treatment of the nonlinear effects of xenon, enthalpy, and Doppler. Fuel depletion is allowed.

TURTLE was written for the study of azimuthal xenon oscillations, but the code is useful for general analysis. The input is simple, fuel management is handled directly, and a boron criticality search is allowed.

TURTLE is further described in Reference 17.

15.1.9.7 TWINKLE

The TWINKLE program is a multi-dimensional spatial neutron kinetics code, which was patterned after steady state codes presently used for reactor core design. The code uses an implicit finite-difference method to solve the two-group transient neutron diffusion equations in one, two and three dimensions. The code uses six delayed neutron groups and contains a detailed multi-region fuel-clad-coolant heat transfer model for calculating pointwise Doppler and moderator feedback effects. The code handles up to 2000 spatial points, and performs its own steady state initialization. Aside from basic cross-section data and thermal-hydraulic parameters, the code accepts as input basic driving functions such as inlet temperature, pressure, flow, boron concentration, control rod motion, and others. Various edits ~~are provided~~, ~~e.g.~~ channelwise power, axial offset, enthalpy, volumetric surge, pointwise power, and fuel temperatures.

The TWINKLE code is used to predict the kinetic behavior of a reactor for transients which cause a major perturbation in the spatial neutron flux distribution.

TWINKLE is further described in Reference 18.

0794 PKG

10. Stehn, J.R. and Clancy, E. F., "Fission-Product Radioactivity and Heat Generation" and "Proceedings of the Second United Nations International Conference on the Peaceful Uses of Atomic Energy, Geneva, 1958," Volume 13, pp. 49-54, United Nations, Geneva, 1958.

11. Obershain, F. E. and Foderaro, A. H., "Energy from Fission Product Decay," WAPD-P-652, 1955.

12. Hunin, C., "FACTRAN, ~~A~~ a Fortran IV Code for Thermal Transients in a UO Fuel Rod," WCAP-7908, July 1972.

Deleted by Amendment 72

13. Geets, J. M. and Salvatori, R., "Long Term Transient Analysis Program for PWRs (BLKOUT Code)," WCAP-7898, June 1972

14. Geets, J. M., "MARVEL - A Digital Computer Code for Transient Analysis of a Multiloop PWR System," WCAP-7909, ~~October~~ June 1972.

15. Burnett, T. W. T., et al., "LOFTRAN Code Description," WCAP-7907-P-A (Proprietary), WCAP-7907-A (Non-Proprietary) April 1984

16. Barry, R. F., "LEOPARD, A Spectrum Dependent Non-Spatial Depletion Code for the IBM-7094," WCAP-3269-26, September 1963.

17. Barry, R. F. and Altomare, S., "The TURTLE 24.0 Diffusion Depletion Code," WCAP-7213-P-A (Proprietary) and WCAP-7758-A (Non-Proprietary), January 1975.

18. Risher, D. H., Jr. and Barry, R. F., "TWINKLE - A Multi-Dimensional Nueutron Kinetics Computer Code," WCAP-7979-P-A (Proprietary) and WCAP-8028-A (Non-Proprietary), January 1975.

19. Bordelon, F. M., "Calculation of Flow Coastdown After Loss of Reactor Coolant Pump (PHOENIX Code)," WCAP-7973, August 1970.

20. Skaritka, J. (Ed.), "Hybrid B C Absorber Control Rod Evaluation Report," WCAP-8846, Rev. 1, February 1977.

21. Morita, T., et. al., "Dropped Rod Methodology for Negative Flux Rate Trip Plants," WCAP-10297-P-A (Proprietary) and WCAP-10298-A (Non-Proprietary), June 1983.

22. Reagan, J.R. ~~Tuley, C. R., Zawalick, S.S.~~, "Westinghouse Setpoint Methodology for Protection Systems, Watts Bar 1 and 2, EAGLE 21 Version," WCAP-12096, Rev. ~~4~~ 5, ~~November 1990 (proprietary)~~ (Westinghouse Proprietary Class 2).

23. Miranda, S., et.al., "Steam Generator Low Water Level Protection System Modifications to Reduce Feedwater Related Trips," WCAP-11325-P-A, Revision 1, February 1988.

TABLE 15.1-2

SUMMARY OF INITIAL CONDITIONS AND COMPUTER CODES USED

FAULTS	COMPUTER CODES UTILIZED	REACTIVITY COEFFICIENTS ASSUMED MODERATOR TEMPERATURE (Δ k/°F)	MODERATOR DENSITY (Δ k/gm/cc)	DOPPLER	INITIAL NSSS THERMAL POWER OUTPUT ASSUMED* (MWt)
CONDITION II					
Uncontrolled RCC Assembly Bank Withdrawal from Subcritical Condition	TWINKLE, FACTRAN THINC	Refer to Section 15.2.1.2 (Part 2)	--	Least negative Doppler power coefficient-Doppler defect = -0.9% Δk/k	0
Uncontrolled RCC Assembly Bank Withdrawal at Power	LOFTRAN, FACTRAN THINC	---	Figure 15.1-7 and 0.43	lower and upper (1)	3425
RCC Assembly Misalignment	THINC, ~~TURTLE~~ LOFTRAN	---	Figure 15.1-7	upper (1)	3425
Uncontrolled Boron Dilution	NA	NA	NA	NA	0 and 3425
Partial Loss of Forced Reactor Coolant Flow	~~PHOENIX~~, LOFTRAN THINC, FACTRAN	---	Figure 15.1-7	upper ~~lower~~ (1)	~~2397 and~~ 3425
Startup of an Inactive Reactor Coolant Loop	MARVEL, THINC FACTRAN	---	0.43	lower (1)	2397
Loss of External Electrical Load and/or Turbine Trip	LOFTRAN	---	Figure 15.1-7 and 0.43	lower and upper (1)	3425
combine Loss of Normal Feedwater/	LOFTRAN	---	Figure 15.1-7	upper (1)	~~3579~~ 3425
Loss of Off-Site Power to the Station Auxiliaries (Station Blackout)	~~BLKOUT~~		~~NA~~	~~NA~~	~~3425~~

0794 PKG

TABLE 15.1-2 (Continued)

SUMMARY OF INITIAL CONDITIONS AND COMPUTER CODES USED

FAULTS	COMPUTER CODES UTILIZED	ASSUMED REACTIVITY COEFFICIENTS: MODERATOR TEMPERATURE (Δ k/°F)	MODERATOR DENSITY (Δ k/gm/cc)	DOPPLER	ASSUMED INITIAL NSSS THERMAL POWER OUTPUT[1] (MWt)
CONDITION II (Cont'd)					
Excessive Heat Removal Due to Feedwater System Malfunctions[3]	MARVEL, LOFTRAN	---	0.43	lower[2]	0 and 3425
Excessive Load Increase Incident	LOFTRAN	---	Figure 15.1-7 and 0.43	lower[2]	3425
Accidental Depressurization of the Reactor Coolant System	LOFTRAN	---	Figure 15.1-7	upper[2]	3425
Accidental Depressurization of the Main Steam System	LOFTRAN	---	Function of Moderator Density See Section 15.2.13 (Figure 15.2-40)	Note 4	0 (subcritical)
Inadvertent Operation of ECCS During Power Operation	LOFTRAN	---	~~Minimum[2]~~ Figure 15.1-7 and 0.43	lower ~~[2]~~ and upper[2]	3425
CONDITION III					
Loss of Reactor Coolant from Small Ruptured Pipes or from Cracks in Large Pipes which Actuates Emergency Core Cooling	NO TRUMP, LOCTA-IV				3479

0794 PKG

TABLE 15.1-2 (Continued)

SUMMARY OF INITIAL CONDITIONS AND COMPUTER CODES USED

FAULTS	COMPUTER CODES UTILIZED	ASSUMED REACTIVITY COEFFICIENTS: MODERATOR TEMPERATURE (Δ k/°F)	ASSUMED REACTIVITY COEFFICIENTS: MODERATOR DENSITY (Δ k/gm/cc)	DOPPLER	ASSUMED INITIAL NSSS THERMAL POWER OUTPUT[1] (MWt)
CONDITION III (Cont'd)					
Inadvertent Loading of a Fuel Assembly into an Improper Position	LEOPARD, TURTLE	---	Minimum	NA	3425
Complete Loss of Forced Reactor Coolant Flow	~~PHOENIX~~ THINC, FACTRAN	---	Figure 15.1-7	lower[2]	~~2397~~ ~~and~~ 3425
Waste Gas Decay Tank	NA	---	NA	NA	3579
Single RCC Assembly Withdrawal at Full Power	TURTLE, THINC LEOPARD	---	NA	NA	3425
CONDITION IV					
Major rupture of pipes containing reactor coolant up to and including double-ended rupture of the largest pipe in the Reactor Coolant System (Loss of Coolant Accident)	SATAN-VI, WREFLOOD, LOTIC 2, BASH, LOCBART	See Section 15.4.1, References		See Section 15.4.1, References	3479

0794 PKG

TABLE 15.1-2 (Continued)

SUMMARY OF INITIAL CONDITIONS AND COMPUTER CO~~R~~DES USED

FAULTS	COMPUTER CODES UTILIZED	ASSUMED REACTIVITY COEFFICIENTS: MODERATOR TEMPERATURE (Δ k/°F)	MODERATOR DENSITY (Δ k/gm/cc)	DOPPLER	ASSUMED INITIAL NSSS THERMAL POWER OUTPUT[1] (MWt)
CONDITION IV (Cont'd)					
Major ~~secondary system pipe rupture up to and including double ended rupture (~~Rupture of a Steam Pipe~~)~~	LOFTRAN, ~~THING~~	Function of Moderator Density; see Section 15.2.13 (Figure 15.2-40)		Note 4	0 (subcritical)
Major Rupture of a Main Feedwater Pipe	LOFTRAN	---	Figure 15.1-7	upper[2]	3425
Steam Generator Tube Rupture	NA	NA	NA	NA	3579
Single Reactor Coolant Pump Locked Rotor	~~PHOENIX~~, LOFTRAN, FACTRAN	----	Figure 15.1-7	lower[2]	~~2397 and~~ 3425
Fuel Handling Accident	NA	NA	NA		3579
Rupture of a Control Mechanism Housing (RCCA Ejection)	TWINKLE, FACTRAN ~~LEOPARD~~	Refer to Section 15.4.6	---	Consistent with lower limit shown on Figure 15.1-5	0 and 3425

[1] A minimum of 2% margin has to be applied.
[2] Reference Figure 15.1-5
[3] Reference Figure 15.1-7
[4] Reference Figure 15.4-9

0794 PKG

0794 PKG

TABLE 15.1-3

TRIP POINTS AND TIME DELAYS TO TRIP ASSUMED IN ACCIDENT ANALYSES

Trip Function	Limiting Trip Point Assumed In Analysis	Time Delays (Seconds)
Low Reactor Coolant Flow (from loop flow detectors)	87% loop flow	~~1.0~~ 1.2
Undervoltage Trip	68%	1.5
Turbine Trip	Not applicable	1.0
Low-Low Steam Generator Level	0% ~~or 9%~~ of narrow range span ~~depending on the particular accident~~	2.0 + TTD *
High-High Steam Generator Level, Turbine Trip and Feedwater Isolation	89.7% of narrow range level span	2.5

* Trip Time Delay (TTD) is applicable only below 50% RTP.

0794 PKG

~~2. Reactor trip on low feedwater flow signal in any steam generator. (This signal is actually a steam flow-feedwater flow mismatch in coincidence with low water level.)~~

2 ~~3~~. Two motor driven auxiliary feedwater pumps which are started on:

a. Low-low level both turbine driven in any steam generator
b. Trip of ~~all~~ main feedwater pumps
c. Any safety injection signal
d. Loss of offsite power
e. Manual actuation

3 ~~4~~. One turbine driven auxiliary feedwater pump is started on:

a. Low-low level both turbine driven in any two steam generators.
b. Trip of ~~all~~ main feedwater pumps
c. Any safety injection signal
d. Loss of offsite power
e. Manual actuation

Refer to Chapter 10 for the design of the Auxiliary Feedwater System.

The motor driven auxiliary feedwater pumps are supplied by the diesels if a loss of offsite power occurs and the turbine-driven pump utilizes steam from the secondary system. Both type pumps are designed to start within one minute even if a loss of all AC power occurs simultaneously with loss of normal feedwater. The turbine exhausts the secondary steam to the atmosphere. The auxiliary pumps take suction from the condensate storage tank for delivery to the steam generators.

The analysis shows that following a loss of normal feedwater, the Auxiliary Feedwater System is capable of removing the stored and residual heat thus preventing either overpressurization of the RCS or loss of water from the reactor core.

15.2.8.2 Analysis of Effects and Consequences

Method of Analysis

A detailed analysis using the LOFTRAN [5] Code is performed in order to obtain the plant transient following a loss of normal feedwater. The simulation describes the plant thermal kinetics, RCS including the natural circulation, pressurizer, steam generators and feedwater system. The digital program computes pertinent variables including the steam generator level, pressurizer water level, and reactor coolant average temperature.

Two cases are examined for a loss of normal feedwater event. The first is the case where offsite ac power is maintained, and the second is the case where offsite ac power is lost, which results in reactor coolant pump coastdown as described in Section 15.2.5.2.

The case where offsite ac power is lost is limiting with respect to overpressurization of the RCS and loss of water from the reactor core due to the decreased capability of the reactor coolant pump to aid in residual core heat removal as a result of the reactor coolant pump coastdown.

0794 PKG

2. The plant is initially operating at 102% of the Nuclear Steam Supply System ~~Engineered Safety Features~~ design rating. The heat added to the RCS by the reactor coolant pumps is assumed.

3. The core residual heat generation is based on the 1979 version of ANS 5.1 [14] based upon long term operation at the initial power level. The decay of U-238 capture products is included as an integral part of this expression.

4. A heat transfer coefficient in the steam generator associated with RCS natural circulation.

5. Two ~~Only one~~ motor driven auxiliary feedwater pumps are ~~is~~ available one minute after the accident.

6. Auxiliary feedwater is delivered to four ~~two~~ steam generators.

7. Secondary system steam relief is achieved through the self-actuated safety valves. Note that steam relief will, in fact, be through the power-operated relief valves or condenser dump valves for most cases of loss of normal feedwater. However, for the sake of analysis these have been assumed unavailable.

8. The initial reactor coolant average temperature is set conservatively higher ~~6.5°F lower~~ than the nominal value for the case where offsite ac power is maintained since this results in a greater expansion of the RCS from pump and decay heat during the transient and, subsequently, a higher water level in the pressurizer. For the case where offsite ac power is lost, the initial reactor coolant average temperature is set conservatively ~~4.0°F~~ lower than the nominal value since this results in a greater density in the RCS and lower natural circulation.

9. The initial pressurizer pressure is 46 psi higher than nominal. This 46 psi allowance is for steady state fluctuations and measurement error.

10. The low-low steam generator level trip setpoint is conservatively assumed to be 0.0% ~~9.0%~~ of narrow range span.

The loss of normal feedwater analysis is performed to demonstrate the adequacy of the reactor protection and engineered safeguards systems (e.g., the auxiliary feedwater system) in removing long term decay heat and preventing excessive heatup of the RCS with possible resultant RCS overpressurization or loss of RCS water.

As such, the assumptions used in this analysis are designed to minimize the energy removal capability of the system and to maximize the possibility of water relief from the coolant system by maximizing the coolant system expansion, as noted in the assumptions listed above.

One such assumption is the loss of external (offsite) ac power. This assumption results in coolant flow decay down to natural circulation conditions reducing the steam generator heat transfer coefficient. Following a loss of offsite ac power, the first few seconds of a loss of normal feedwater transient will be virtually identical to the transient response (including DNBR and neutron flux versus time) presented in Section 15.3.4 for the complete loss of forced reactor coolant flow incident.

0794 PKG

An additional assumption made for the loss of normal feedwater evaluation is that the pressurizer power-operated relief valves are assumed to function normally. If these valves were assumed not to function, the coolant system pressure during the transient would rise to the actuation point of the pressurizer safety valves (2500 psia). The increased RCS pressure, however, results in less expansion of the coolant and hence more margin to the point where water relief from the pressurizer would occur. The balance of plant assumptions used in the analysis are listed in Table 15.2-3.

Results

Figures 15.2-27a through 15.2-27~~i~~h show the significant plant parameter transients following a loss of normal feedwater where offsite power is lost. The calculated sequence of events for this accident are listed in Table 15.2-1.

Following the reactor and turbine trip from full load, the water level in the steam generators will fall due to the reduction of steam generator void fraction and because steam flow through the safety valves continues to dissipate the stored and generated heat. One minute following the initiation of the low-low level trip, ~~one~~ both of the motor-driven auxiliary feedwater pumps are ~~is~~ automatically started and are ~~is~~ at full speed, reducing the rate of water level decrease.

The capacity of the auxiliary feedwater pumps are ~~is~~ such that the water level in the steam generators ~~being fed~~ does not recede below the lowest level at which sufficient heat transfer area is available to dissipate core residual heat without water relief from the RCS relief or safety valves.

From Figure 15.2-27~~g~~f, it can be seen that at no time is there water relief from the pressurizer. If the auxiliary feed delivered is greater than that of two ~~one~~ motor-driven pumps, if the initial reactor power is less than 102% of the NSSS ~~Engineered Safety Features~~ design rating, or if the steam generator water level in one or more steam generators is above the low-low level trip point at the time of trip, then the ~~result will be a higher steam generator minimum water level and margin exists for reactor coolant water relief.~~ results of this transient will be bounded by the analysis presented.

RCS pressure will stabilize following operator action to terminate flow to the inadvertantly opened valve; normal operating procedures may then be followed. The operating procedures would call for operator action to control RCS boron concentration and pressurizer level using the CVCS and to 30 maintain steam generator level through control of the main or auxiliary feedwater system. Any action required of the operator to stabilize the plant will be in a time frame in excess of ten minutes following reactor trip.

15.2.12.3 Conclusions

The pressurizer low pressure and the overtemperature ΔT Reactor Protection System signals provide adequate protection against 53 this accident, and the minimum DNBR remains in excess of 1.30.

15.2.13 ACCIDENTAL DEPRESSURIZATION OF THE MAIN STEAM SYSTEM

15.2.13.1 Identification of Causes and Accident Description

The most severe core conditions resulting from an accidental depressurization of the Main Steam System are associated with an inadvertent opening of a single steam dump, relief or safety valve. The analyses performed assuming a rupture of a main steam line are given in Section 15.4.2.1.

The steam release as a consequence of this accident results in an initial increase in steam flow which decreases during the accident as the steam pressure falls. The energy removal from the Reactor Coolant System causes a reduction of coolant temperature and pressure. In the presence of a negative moderator temperature coefficient, the cooldown results in a reduction of core shutdown margin. 41

The analysis is performed to demonstrate that the following criterion is satisfied: Assuming a stuck rod cluster control assembly, with or without offsite power, and assuming a single failure in the Engineered Safety Features there will be no consequent fuel damage after reactor trip for a steam release equivalent to the spurious opening, with failure to close, of the largest of any single steam dump, relief or safety valve. This 53 criterion is satisfied by verifying the DNB design basis is met.

The following systems provide the necessary protection against an accidental depressurization of the main steam system.

1. Safety Injection System actuation from any of the following: 49
   a. Two out of three ~~signals of low-~~low pressurizer pressure signals.
   b. Two out of three high containment pressure signals. 53

c. Two out of ~~four loops high~~ three low steam line pressure signals in any steamline. ~~flow coincident with either two out of four loops low steam line pressure or two out of four loops low-low T_{avg}.~~ 53

2. The overpower reactor trips (neutron flux and ΔT and the reactor trip occuring ~~in~~ conjunction with receipt of the safety injection signal).

3. Redundant isolation of the main feedwater lines: Sustained high feedwater flow would cause additional cooldown. Therefore, in addition to the normal control action which will close the main feedwater valves following reactor trip, a safety injection signal will rapidly close all feedwater control valves, trip the main feedwater pumps, and close the feedwater pump discharge valves (closure is accomplished by a main feedwater pump trip signal).

4. Trip of the fast-acting steamline stop valves (Main Steam Isolation Valves) (designed to close in less than 5 seconds) on: 55

   a. Two out of four ~~H~~high-high containment pressure signals.

   b. ~~Two out of four loops high steam line flow coincident with either two out of four loops low steam line pressure or two out of four loops low-low T_{avg}.~~ 53

   Two out of three low steamline pressure signals in any steamline.

c. Two out of three high negative ~~steam~~ steamline pressure rate signals in any ~~loop~~ steamline (below Permissive P-11).

15.2.13.2 Analysis of Effects and Consequences

Method of Analysis

The following analyses of a secondary system steam release are performed for this section.

1. A full plant digital computer simulation to determine Reactor Coolant System transient conditions during cooldown, and the effect of safety injection [5]. 53

2. Analyses to determine that there is no consequential fuel damage.

The following conditions are assumed to exist at the time of a secondary steam system release.

1. End-of-life shutdown margin at no load, equilibrium xenon conditions, and with the most reactive rod cluster control assembly stuck in its fully withdrawn position. Operation of rod cluster control assembly banks during core burnup is restricted in such a way that addition of positive reactivity in a secondary system steam release accident will not lead to a more adverse condition than the case analyzed.

2. A negative moderator coefficient corresponding to the end-of-life rodded core with the most reactive rod cluster control assembly in the fully withdrawn position. The variation of the coefficient with temperature and pressure is included. The keff versus temperature at 1000 psi corresponding to the negative moderator temperature coefficient used is shown in Figure 15.2-40.

3. Minimum capability for injection of high concentration boric acid solution corresponding to the most restrictive single failure in the Safety Injection System. This corresponds to the flow delivered by one charging pump delivering its full contents to the cold leg header. The injection curve used is shown in Figure 15.4-10. Low concentration boric acid must be swept from the safety injection lines downstream of the RWST prior to the delivery of high concentration boric acid 53 (1950 ppm) to the reactor coolant loops. This effect has been allowed for in the analysis.

The cooldown for the case shown in Figure 15.2-41 is more rapid than the case of steam release from all steam generators through one steam dump, relief, or safety valve. The transient is conservative with respect to cooldown, since no credit is taken for the energy stored in the system metal other than that of the fuel elements.

Following blowdown of the faulted steam generator, the plant can be brought to a stabilized hot standby condition through control of auxiliary feedwater flow and safety injection flow, as described by plant operating procedures. The operating procedures would call for operator action to limit RCS pressure and pressurizer level by terminating safety injection flow, and to control steam generator level and RCS coolant temperature using the auxiliary feedwater system. Any action required of the operator to maintain the plant in a stabilized condition will be in a time frame in excess of ten minutes following safety injection actuation.

15.2.13.3 Conclusions

The analysis shows that the criteria stated earlier in this section are satisfied since a DNBR less than the limiting value given by the WBN Technical Specifications does not exist.

15.2.14 Inadvertent Operation of Emergency Core Cooling System

This analysis was performed after the boron injection tank and associated 900 gallons of 20,000 ppm boron was deleted from the Watts Bar design basis, and therefore it is not referenced in this section.

15.2.14.1 Identification of Causes and Accident Description

Spurious Emergency Core Cooling System (ECCS) operation at power could be caused by operator error or a false electrical actuating signal. Spurious actuation may be assumed to be caused by any of the following:

1. High containment pressure

2. Low pressurizer pressure

~~3. High steamlinedifferential pressure~~

3 ~~4. Low-Low T_{avg} in conjunction with high steamline flow or l~~ L ow steamline pressure

4 ~~5.~~ Manual actuation

Following the actuation signal, the suction of the centrifugal charging pumps is diverted from the volume control tank to the refueling water storage tank.

0794 PKG

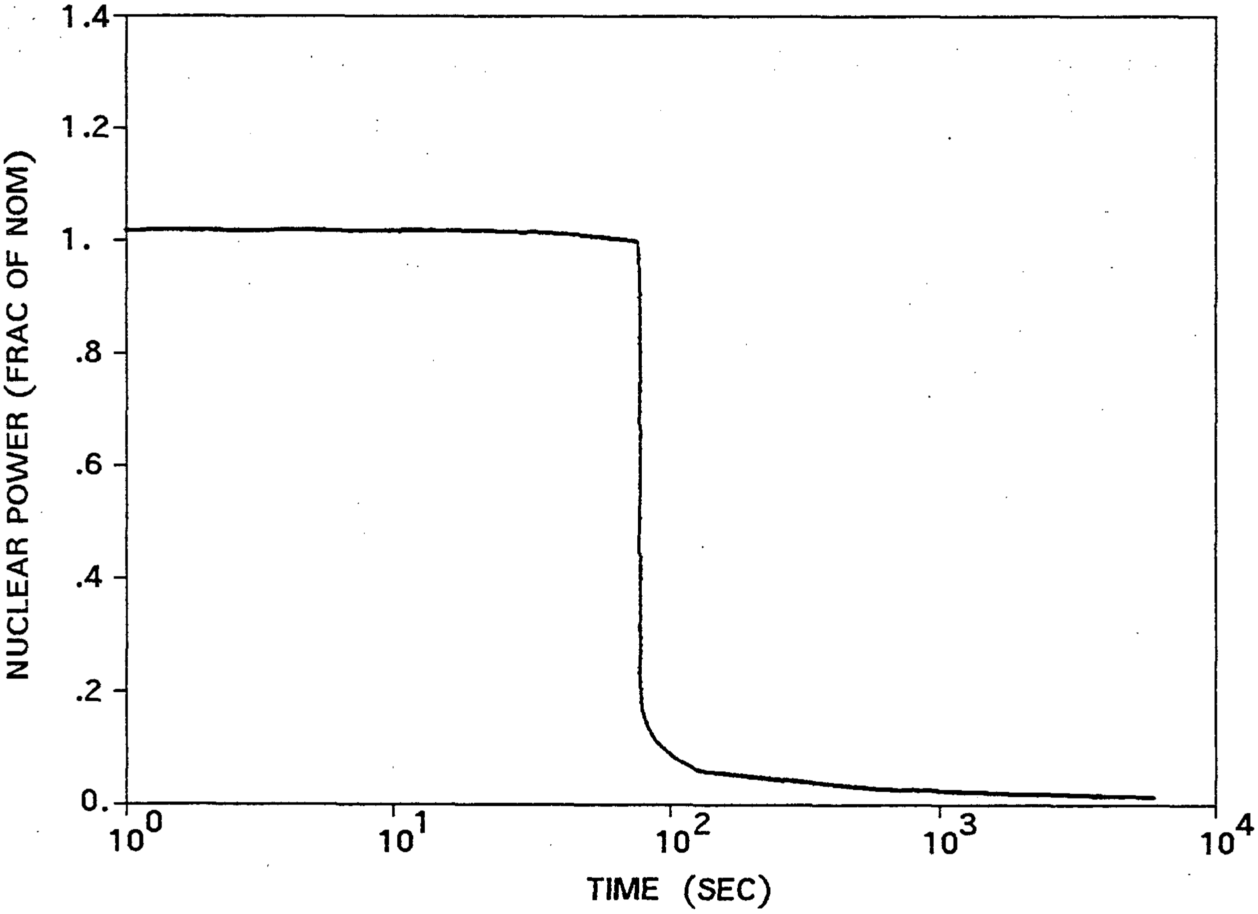
TABLE 15.2-1

TIME SEQUENCE OF EVENTS FOR CONDITION II EVENTS

Accident	Event	Time (sec.)
Loss of Normal Feedwater with Loss of Offsite Power	Main Feedwater Flow Stops	10
	Low-low steam generator water level reactor trip	~~67~~ 68.531
	Rods begin to drop	~~69~~ 70.531
	Reactor coolant pumps begin to coast down	~~71~~ 72.531
	Four ~~Two~~ steam generators begin to receive auxiliary feed from two ~~one~~ motor-driven auxiliary feedwater pumps	~~127~~ 128.531
	Peak water level in pressurizer occurs	~~1406~~ 76
Excessive feedwater at full load	One main feedwater control valve fails fuly open	0
	High Steam Generator Level setpoint reached	29.0
	Minimum DNBR occurs	29.0

63

0794 PKG



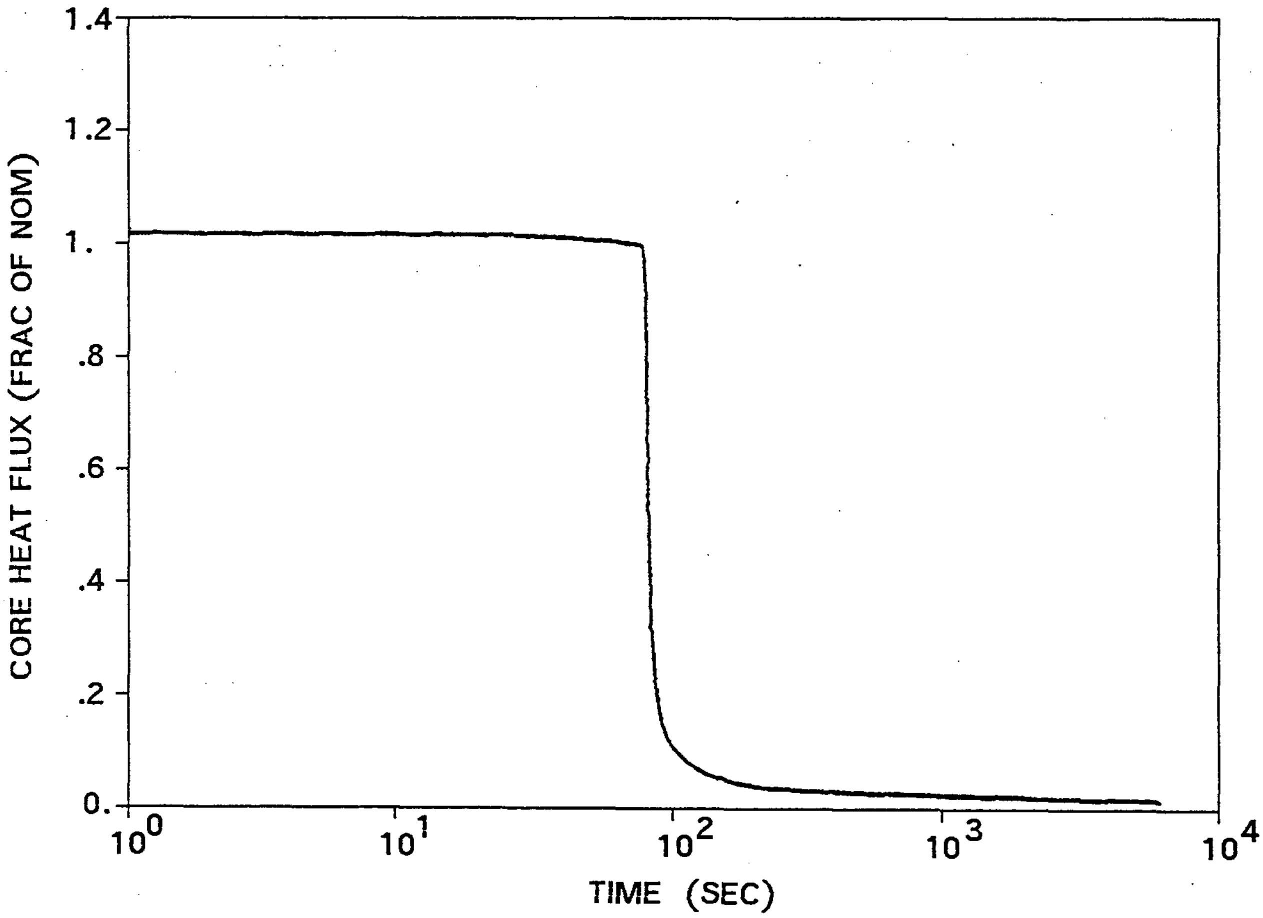
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

NUCLEAR POWER TRANSIENT FOR LOSS OF NORMAL FEEDWATER

FIGURE 15.2-27A

0794 PKG



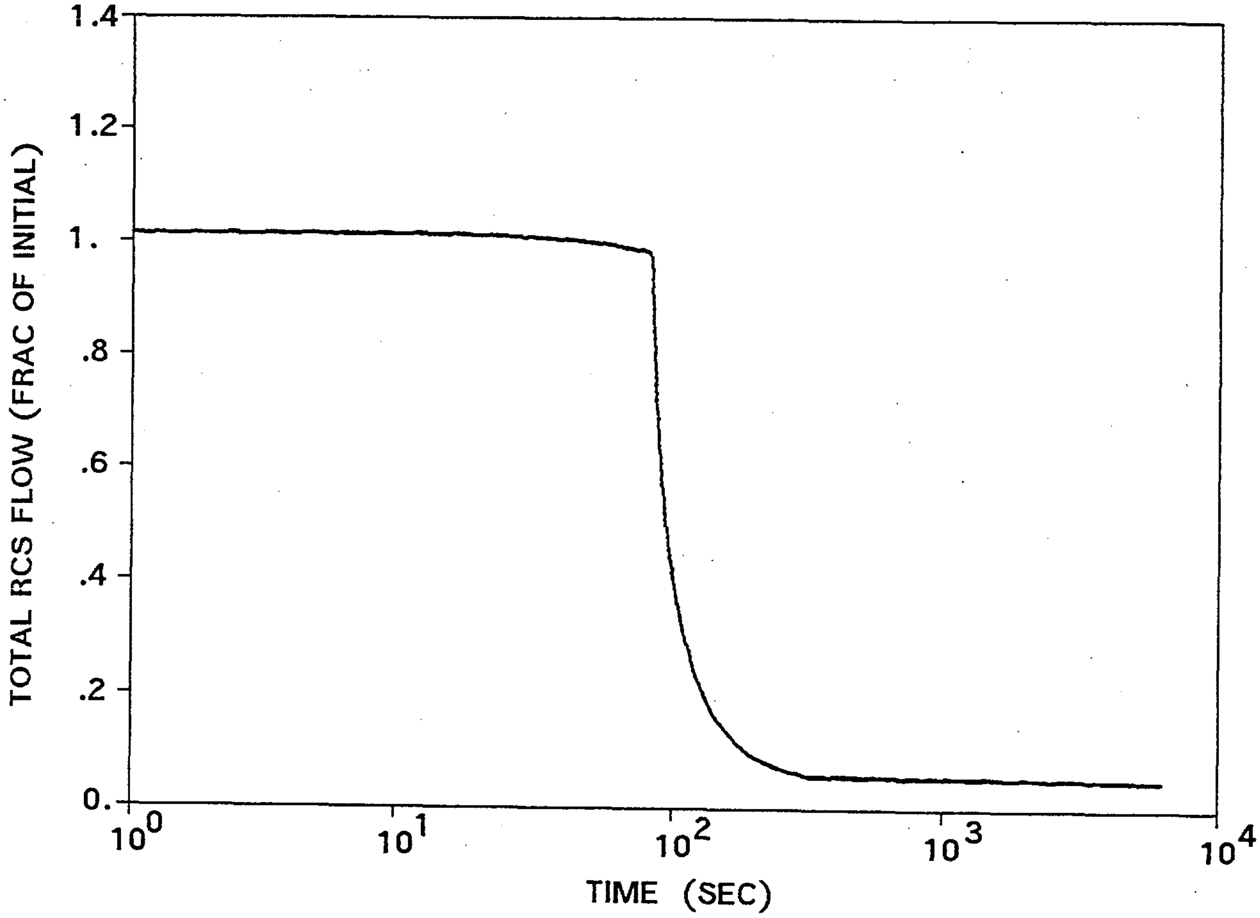
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

CORE HEAT FLUX TRANSIENT FOR LOSS OF NORMAL FEEDWATER

FIGURE 15.2-27B

0794 PKG

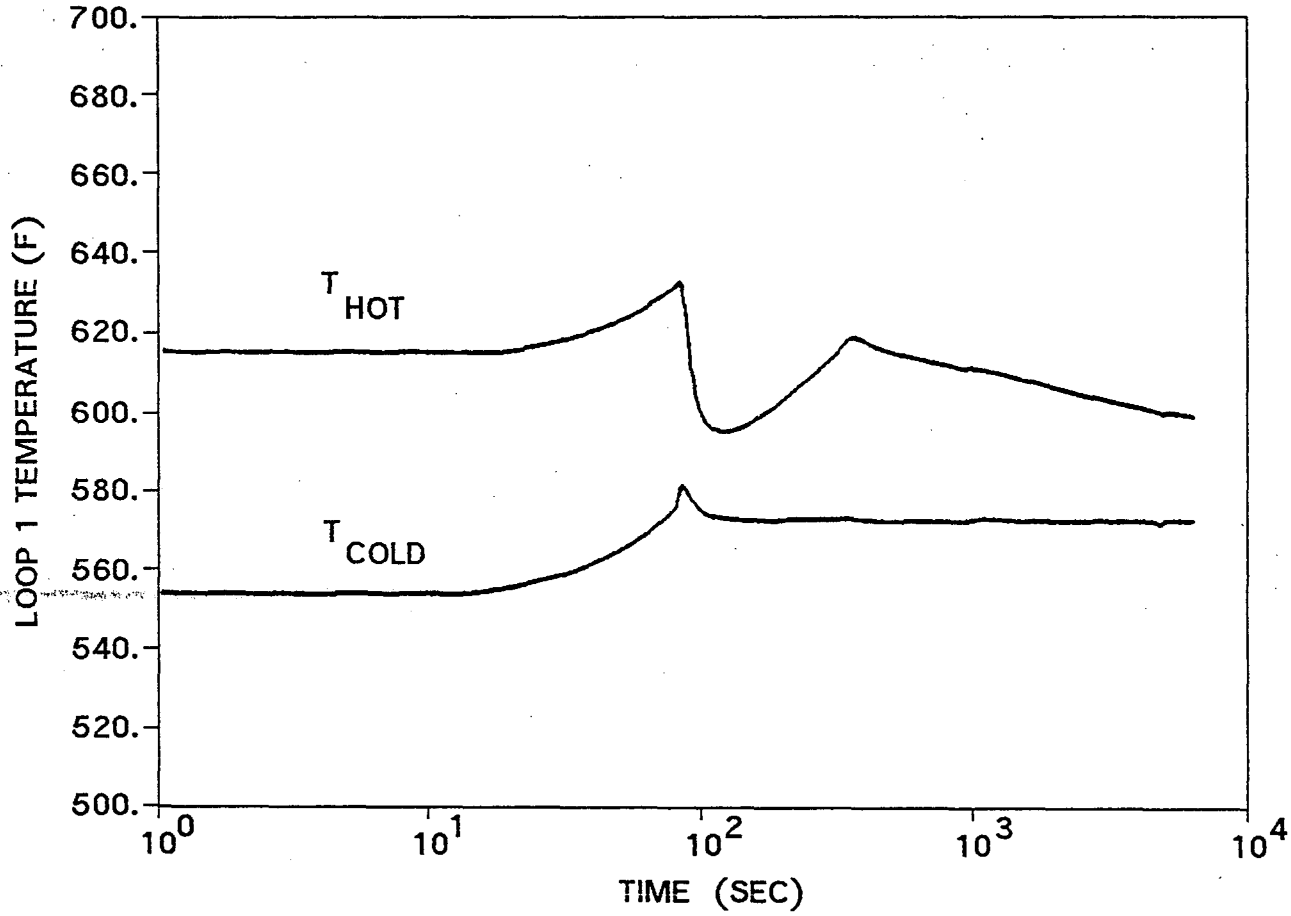


REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

FLOW TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27C

0794 PKG



REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

REACTOR COOLANT SYSTEM
TEMPERATURE TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27D

0794 PKG

FIGURE 15.2-27E

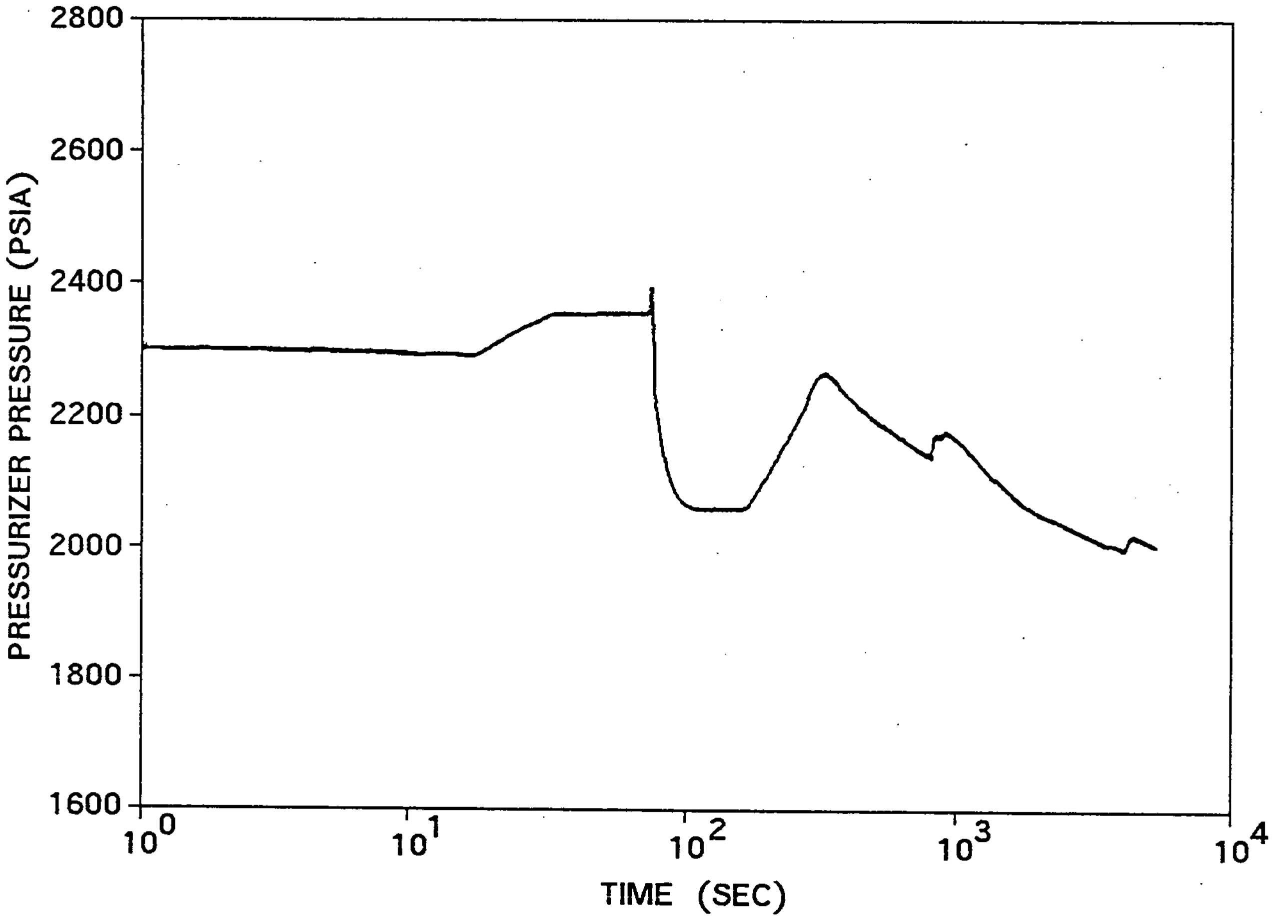
DELETED BY AMENDMENT 72

REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

CORE AVERAGE
TEMPERATURE TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27E

0794 PKG

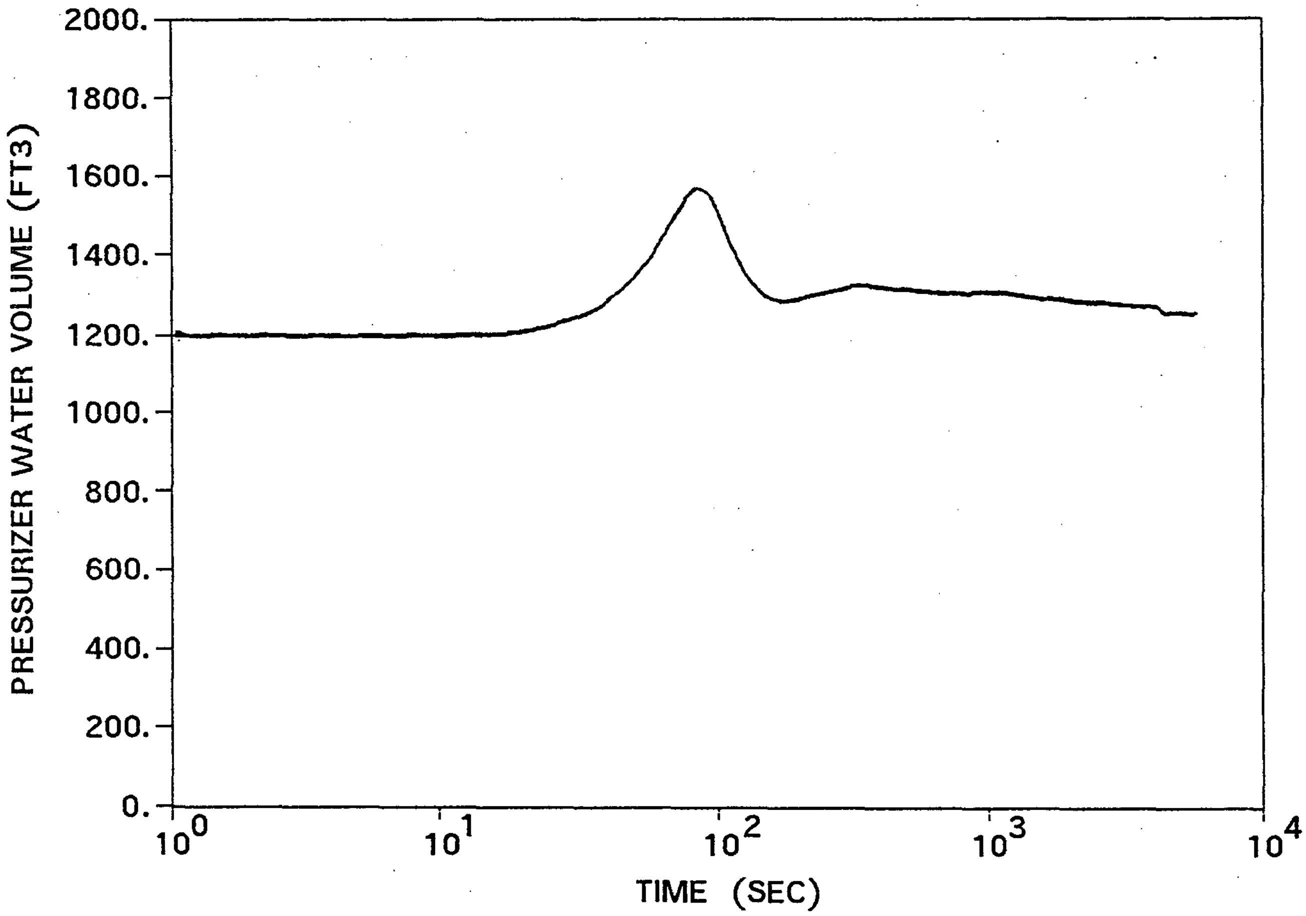


REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

PRESSURIZER PRESSURE TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27F

0794 PKG



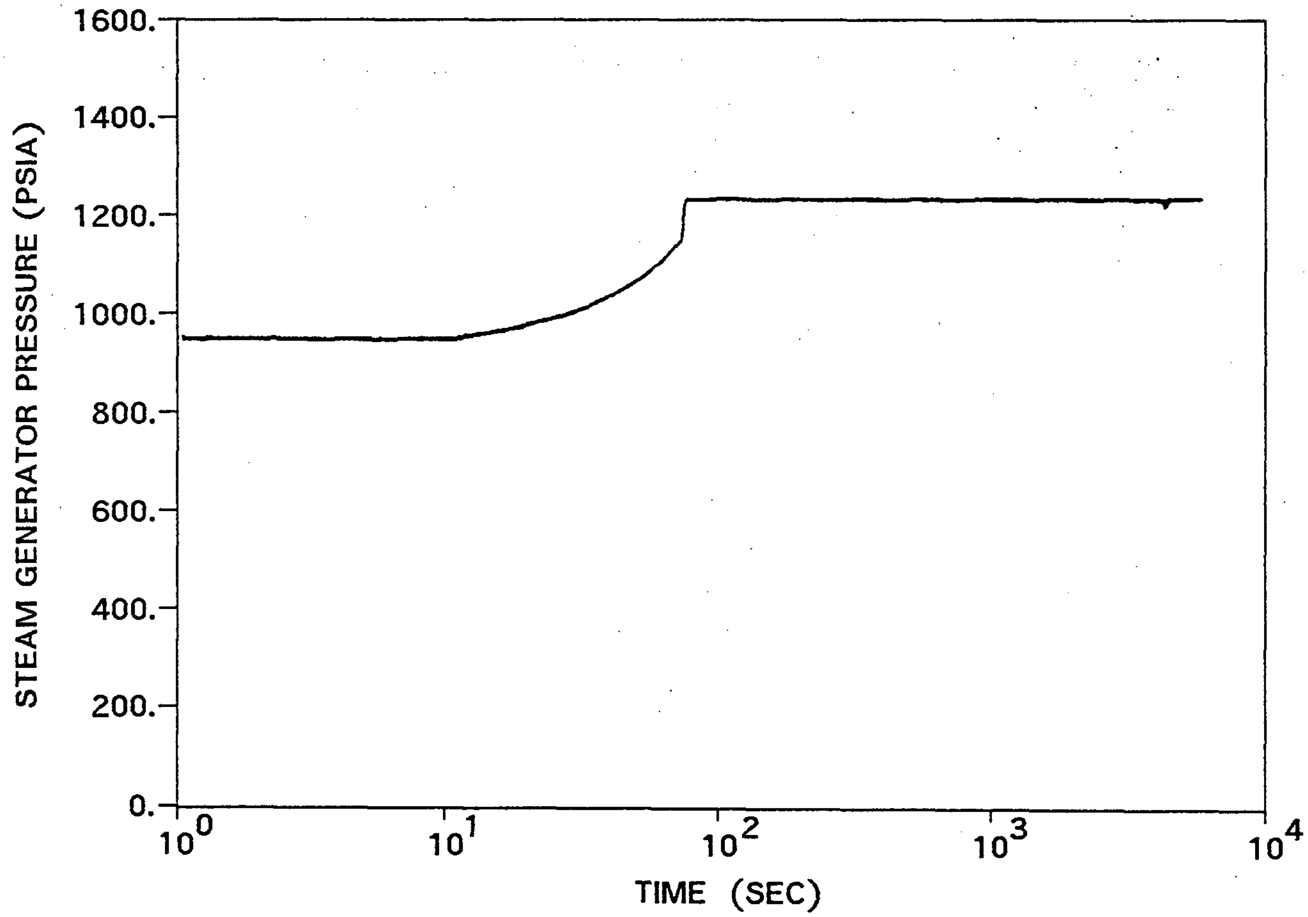
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

PRESSURIZER WATER VOLUME TRANSIENT FOR LOSS OF NORMAL FEEDWATER

FIGURE 15.2-27G

0794 PKG

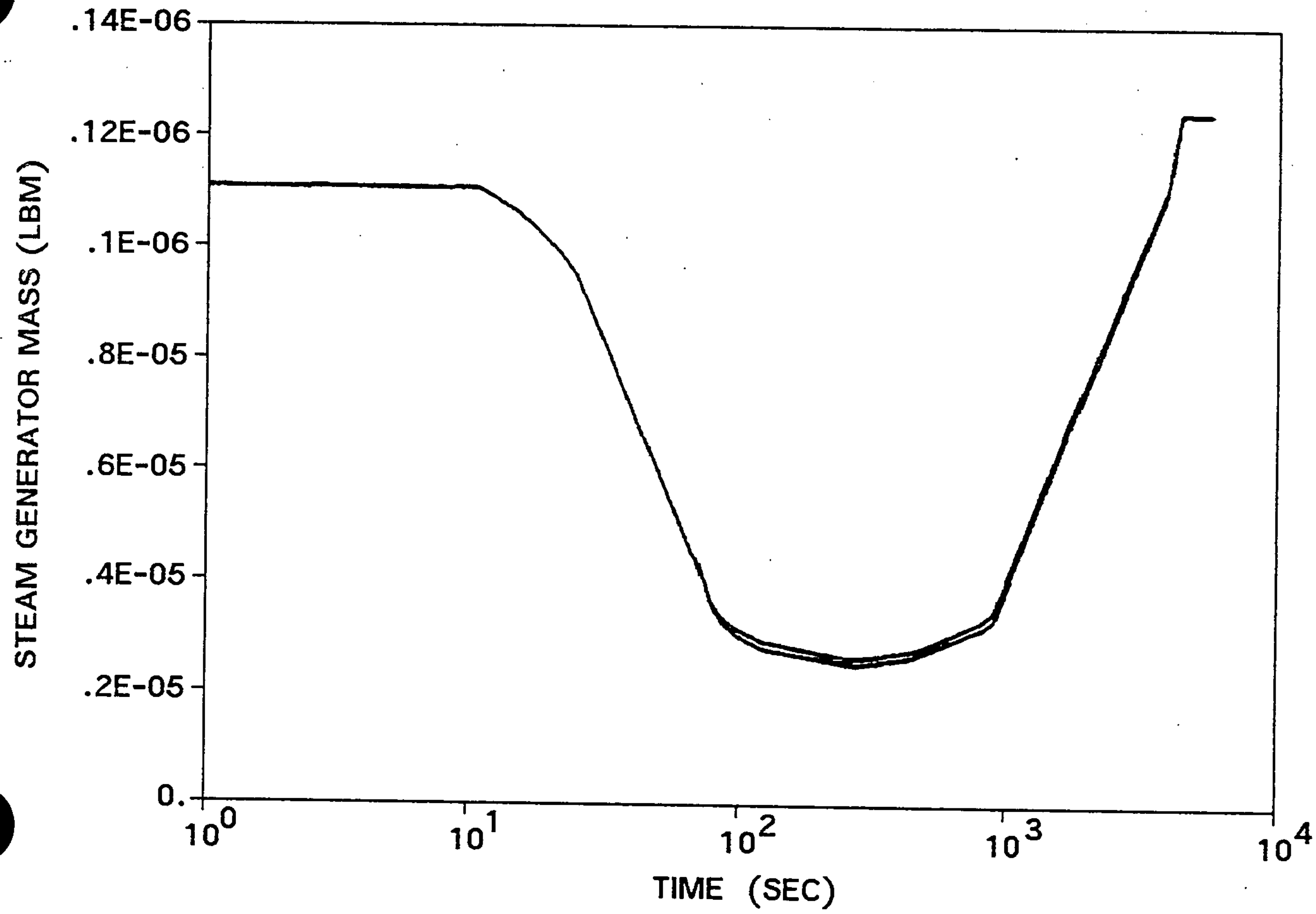


REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

STEAM GENERATOR
PRESSURE TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27H

' 0794 PKG



REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

STEAM GENERATOR
MASS TRANSIENT
FOR LOSS OF
NORMAL FEEDWATER
FIGURE 15.2-27I

and return to power. A return to power following a steam line rupture is a potential problem mainly because of the high power peaking factors which exist assuming the most reactive RCCA to be stuck in its fully withdrawn position. The core is ultimately shut down by the boric acid injection delivered by the Safety Injection System.

The analysis of a main steam line rupture is performed to demonstrate that the following criterion is satisfied:

Assuming a stuck RCCA with or without offsite power, and assuming a single failure in the engineered safeguards the core remains in place and intact. Radiation doses are not expected to exceed the guidelines of 10CFR100.

Although DNB and possible clad perforation following a steam pipe rupture are not necessarily unacceptable, the following analysis, in fact, shows that no DNB occurs for any rupture assuming the most reactive assembly stuck in its fully withdrawn position.

The following functions provide the necessary protection for a steam line rupture:

1. Safety Injection System actuation from any of the following:

    a. Two out of three ~~signals of~~ low pressurizer pressure signals. 53

    b. Two out of three high containment pressure signals.

    c. ~~Low steam line pressure in any one loop relative to two out of three other loops.~~ Two out of three low steamline pressure signals in any steamline.

    d. ~~High steamline flow in two out of four loops coincident with either two out of four loops low steamline pressure or two out of four loops low-low T.~~

2. The overpower reactor trips (neutron flux and ΔT) and the reactor trip occurring in conjunction with receipt of the safety injection signal.

3. Redundant isolation of the main feedwater lines: Sustained high feedwater flow would cause additional cooldown. Therefore, in addition to the normal control action which will close the main feedwater valves, a safety injection signal will rapidly close all feedwater control valves, main feedwater isolation valves, trip the 53

main feedwater pumps, and close feedwater pump discharge valves.

4. Trip of the fast acting steam line stop valves (main steam isolation valves) (designed to close in less than 5 seconds) on: 53

   a. Two out of four ~~H~~high-~~H~~high containment pressure signals.

   ~~b. Two out of four loops high steamline flow coincident with either two out of four loops low steamline pressure or two out of four low-low T_{avg} in the coolant loops.~~

Fast-acting isolation valves are provided in each steam line that will fully close within 7 seconds after a steamline isolation signal setpoint is reached. 53 For breaks downstream of the isolation valves, closure of all valves would completely terminate the blowdown. For any break, in any location, no more than one steam generator would blowdown even if one of the isolation valves fails to close. A description of steam line isolation is included in Chapter 10. 53

Steam flow is measured by monitoring dynamic head in nozzles located in the throat of the steam generator. The effective throat area of the nozzles is 1.4 square feet, which is considerably less than the main steam pipe and thus the nozzles also serve to limit the maximum steam flow for a break at any location.

Table 15.4-6 lists the equipment required in the recovery from a high energy line rupture. Not all equipment is required for any one particular break, since it will vary depending upon postulated break location and details of initial conditions. Design criteria and methods of protection of safety related equipment from the dynamic effects of postulated piping ruptures are provided in Section 3.6. 53

15.4.2.1.2 <u>Analysis of Effects and Consequences</u>

<u>Method of Analysis</u>

The analysis of the steam pipe rupture has been performed to determine:

b. Two out of three low steamline pressure signals in any steamline.

c. Two out of three high negative steamline pressure rate signals in any steamline ~~(below Permissive P-11)~~.

 0794 PKG

energy stored in the fuel. Thus, the additional stored energy is removed via the cooldown caused by the steam line break before the no load conditions of RCS temperature and shutdown margin assumed in the analyses are reached. After the additional stored energy has been removed, the cooldown and reactivity insertions proceed in the same manner as in the analysis which assumes no load condition at time zero.

However, since the initial steam generator water inventory is greatest at no load, the magnitude and duration of the RCS cooldown are greater for steam line breaks occurring from no load conditions.

7. In computing the steam flow during a steam line break, the Moody Curve [9] for fl/D = 0 is used.

8. A steam generator tube plugging level of 10% is assumed.

9. A thermal design flowrate of 372,400 gpm is used which accounts for the 10% steam generator tube plugging level and instrumentation uncertainty.

Results

The results presented are a conservative indication of the events which would occur assuming a steam line rupture since it is postulated that all of the conditions described above occur simultaneously.

Core Power and RCS Transient

Figure 15.4-11 shows the RCS transient and core heat flux following a main steam line rupture (complete severance of a pipe) at initial no load condition (case a). Offsite power is assumed available so that full reactor coolant flow exists. The transient shown assumes an uncontrolled steam release from only one steam generator. Should the core be critical at near zero power when the rupture occurs the initiation of safety injection by low steam line pressure ~~coincident with high steamline flow~~ will trip the reactor. Steam release from more than one steam generator will be prevented by automatic trip of the fast acting isolation valves in the steam lines by high-high containment pressure or ~~signals or high steam line flow coincident with either~~ low steam line pressure signals. ~~or low-low T_{avg}.~~ Even with the failure of one valve, release is limited by isolation valve closure for the other steam generators while the one generator blows down. The main steamline isolation valves are designed to be fully closed in less than 5 seconds from receipt of a closure signal.

0794 PKG

A feedline rupture reduces the ability to remove heat generated by the core from the reactor coolant system because of the following reasons:

1. Feedwater to the steam generators is reduced. Since feedwater is subcooled, its loss may cause reactor coolant temperatures to increase prior to reactor trip;

2. Liquid in the steam generator may be discharged through the break, and would then not be available for decay heat removal after trip;

3. The break may be large enough to prevent the addition of any main feedwater after trip.

An auxiliary feedwater system is provided to assure that adequate feedwater will be available such that:

1. No substantial overpressurization of the reactor coolant system shall occur; and

2. Liquid in the reactor coolant system shall be sufficient to cover the reactor core at all times.

The following provides the necessary protection for a main feedwater rupture:

1. A reactor trip on any of the following conditions:

   a. High pressurizer pressure

   b Overtemperature delta-T~~,~~

   c. Low-low steam generator water level in ~~any~~ one or more steam generators

   ~~d. Low steam generator level plus steam/feed flow mismatch in any steam generator.~~

   d. ~~e.~~ Safety injection signals from any of the following:

      i) ~~High steamline flow coincident with either low steam line pressure or low-low Tavg~~ Low steam line pressure

      iii) High containment pressure 53

      ~~iii) High steam line differential pressure~~

2. An Auxiliary Feedwater System to provide an assured source of feedwater to the steam generators for decay heat removal.

ii.) Low pressurizer pressure

0794 PKG

15.4.2.2.2 Analysis of Effects and Consequences

Method of Analysis

A detailed analysis using the LOFTRAN [15] Code is performed in order to determine the plant transient following a feedline rupture. The code describes the plant thermal kinetics, Reactor Coolant System including natural circulation, pressurizer, steam generators and feedwater system, and computes pertinent variables including the pressurizer pressure, pressurizer water level, and reactor coolant average temperature. 53

The method used conservatively neglects the heat absorbed by thick metal of the reactor coolant system during the heatup following the feedline rupture. Conservatively high core residual heat generation is assumed following trip, based on long-term operation of the initial power level. The liquid relief capacity of the pressurizer safety valves is calculated by the code assuming homogeneous equilibrium flow of saturated water.

DELETE

On the secondary side, no credit is taken for the 470 gpm flow from the motor-driven auxiliary pump connected to the affected steam generator, until it is isolated from that loop by the operator. The turbine-driven auxiliary feed flow provides a maximum of 940 gpm starting one minute after low-low steam-generator level trip, and its flow thereafter is conservatively calculated as a function of steam generator pressure. A conservative upper limit is used for the volume of piping which must be purged of hot main feedwater before the relatively cold (120°F) auxiliary feedwater enters the intact steam generator. A conservative upper limit is used for steam dump flow capacity. The quality assumed for the fluid blowing down from the affected steam generator to the rupture is selected conservatively as a function of time, in order to maximize the delay before the low-low water level trip setpoint is reached, and then to minimize the heat transfer effectiveness of the steam generator. The decrease of heat transfer area with shell-side liquid mass is also calculated. 38

In order to reduce the number of cases analyzed, no credit is taken for pressurizer relief valve or spray operation or for high pressurizer pressure trip. Similarly, no credit is taken for containment pressure initiation of safety injection, auxiliary feedwater, and main steamline isolation. This permits analyzing a singly hypothetical case which bounds breaks inside and outside of the containment with and without pressure control. 53

Major assumptions for the case analyzed are:

Two cases are analyzed. One case assumes that offsite electrical power is maintained throughout the transient. Another case assumes the loss of offsite electrical power at the time of reactor trip, and the RCS flow decreases to natural circulation. Both cases assume a double-ended rupture of the largest feedwater pipe at full power. Major assumptions used in the analysis are as follows:

1. The plant is initially operating at 102 percent of the ~~Engineered Safety Features~~ design rating.

2. Initial reactor coolant average temperature is 6.5°F above the nominal value, and the initial pressurizer pressure is ~~30~~ 46 psi above its nominal value.

~~3. The reactor coolant pumps are assumed to continue to operate until they are turned off by the operator. This assumption increases the heat input and maximizes the peak reactor coolant temperature.~~

~~4. A full double-ended break of the main feedwater pipe between the check valve and the steam generators stops immediately.~~ 38

~~5. The most restrictive single failure in the auxiliary feedwater system was assumed. This is the loss of the motor-driven auxiliary feedwater pump that would otherwise supply feedwater to two intact steam generators within one minute of auxiliary feedwater actuation.~~

~~6. A delay of 10 minutes after reactor trip is assumed before the operator actions are performed.~~

3. The pressurizer power-operated relief valves and the safety relief valves are assumed to function. No credit is taken for pressurizer spray. Initial pressurizer level is at the nominal programmed value plus 5% uncertainty.

4. No credit is taken for the following potential protection logic signals to mitigate the consequences of the accident:
   - High pressurizer pressure
   - Overtemperature ΔT
   - High pressurizer level
   - High containment pressure

5. Main feedwater to all steam generators is assumed to stop at the time the break occurs. (All main feedwater spills out through the break.)

6. Saturated liquid discharge (no steam) is assumed from the affected steam generator through the feedline rupture. This assumption minimizes energy removal from the NSSS during blowdown.

Insert A →

INSERT A to Page 15.4-20 0794 PKG

7. No credit is taken for the low-low water level trip on the affected steam generator until the steam generator level reaches 0% of the narrow range span. This assumption minimizes the steam generator fluid inventory at the time of trip, and thereby maximizes the resultant heatup of the reactor coolant.

8. A double-ended break area of 0.223 ft^2 is assumed.

9. No credit is taken for heat energy deposited in reactor coolant system metal during the RCS heatup.

10. No credit is taken for charging or letdown.

11. Steam generator heat transfer area is assumed to decrease as the shellside liquid inventory decreases.

12. ~~Conservative core residual heat generation is assumed based upon long-term operation at the initial power level preceding the reactor trip.~~

The core residual heat generation is based on the 1979 version of ANS 5.1 [ref. 33] based upon long term operation at the initial power level. The decay of U-238 capture products is included as an integral part of this expression.

13. The auxiliary feedwater is actuated by the low-low steam generator water level signal. The auxiliary feedwater is assumed to supply a total of 410 gpm to two unaffected steam generators, based on the following scenario:

- The turbine driven pump is assumed to fail.
- The motor-driven pump supplying the faulted steam generator is conservatively assumed to lose all its flow out the break. The intact steam generator aligned to that pump is therefore assumed to receive no flow.
- The remaining motor-driven pump supplies flow to two intact steam generators.

A 60 second delay was assumed following the low-low level signal to allow time for startup of the emergency diesel generators and the auxiliary feedwater pumps.

0794 PKG

Results

DELETE

Figures 15.4-13 and 15.4-14 show the calculated plant parameters following a feedline rupture. The assumed auxiliary feedwater flow rate is capable of removing decay heat 1831 seconds after trip. After this time, core decay heat decreases below the auxiliary feedwater heat removal capacity, and reactor coolant temperatures and pressures decrease. Calculated results for plant parameters are listed below. 53

Maximum required relief rate from pressurizer safety valves

1. Steam relief, prior to filling pressurizer — 3.5 ft³/sec
2. Water relief, prior to when primary coolant temperature begins to decrease — 1.1 ft³/sec 38

The results show that, even with the conservative method of calculation, the remaining liquid volume is more than adequate to fill the reactor coolant system. Therefore, the reactor core would remain covered with water.

Also, the calculated required relief rates are well within the relief capacity of the pressurizer safety valves. Therefore, no overpressurization occurs within the reactor coolant system.

The time sequence of events is shown on Table 15.4-9.

Figures 15.4-13 a, b and c ~~(sheets 1,2,3)~~ shows the calculated plant parameters following a feedline rupture for the case with offsite power. Figures 15.4-14 a, b and c ~~(sheets 1,2,3)~~ shows the calculated plant parameters following a feedline rupture with loss of offsite power. The calculated sequence of events for both cases analyzed is presented in Table 15.4-9.

The system response following the feedwater line rupture is similar for both cases analyzed. Results presented in the figures show that pressures in the RCS and main steam system remain below 110% of the respective design pressures. Pressurizer pressure increases until reactor trip occurs on low-low steam generator narrow range level. Pressure then decreases, due to the loss of heat input, until steamline isolation occurs. Coolant expansion occurs due to reduced heat transfer capability in the steam generators. The pressurizer ~~safety~~ relief valves open to maintain primary pressure at an acceptable value. The calculated relief rates are ~~well~~ within the relief capacity of the pressurizer ~~safety~~ relief valves. Addition of the safety injection flow aids in cooling down the primary side and helps to ensure that sufficient fluid exists to keep the core covered with water.

The reactor core remains covered with water throughout the transient, as water relief due to thermal expansion is limited by the heat removal capability of the auxiliary feedwater ~~WBNP-52~~ system and makeup is provided by the safety injection system. Bulk boiling does not occur in the RCS prior to the turnaround of the ~~transient~~.

0794 PKC

15.4.2.2.3 Conclusions

Results of the analysis show that for the postulated feedline rupture, the assumed auxiliary feedwater system capacity is adequate to remove decay heat, to prevent overpressurizing the reactor coolant system, and to prevent the water level in the RCS from dropping to the top of the core.

15.4.3 Steam Generator Tube Rupture

15.4.3.1 Identification of Causes and Accident Description

The accident examined is the complete severance of a single steam generator tube. The accident is assumed to take place at power with the reactor coolant contaminated with fission products corresponding to continuous operation with a limited amount of defective fuel rods. The accident leads to an increase in contamination of the secondary system due to leakage of radioactive coolant from the Reactor Coolant System. In the event of a coincident loss of offsite power, or failure of the condenser dump system, discharge of activity to the atmosphere takes place via the steam generator safety and/or power-operated relief valves.

In view of the fact that the steam generator tube material is inconel-600 and is a highly ductile material, it is considered that the assumption of a complete severance is somewhat conservative. The more probable mode of tube failure would be one or more minor leaks of undetermined origin. Activity in the steam and power conversion system is subject to continual surveillance and an accumulation of minor leaks which exceed the limits established in the Technical Specifications ~~are~~ is not permitted during the unit operation. 53

The operator is expected to determine that a steam generator tube rupture has occurred, and to identify and isolate the faulty steam generator on a restricted time scale in order to minimize contamination of the secondary system and ensure termination of radioactive release to the atmosphere from the faulty unit. The recovery procedure can be carried out on a time scale which ensures that break flow to the secondary system is terminated before water level in the affected steam generator rises into the main steam pipe. Sufficient indications and controls are provided to enable the operator to carry out these functions satisfactorily.

0794 PKG

Consideration of the indications provided at the control board, together with the magnitude of the break flow, leads to the conclusion that the isolation procedure can be completed within 30 minutes of accident initiation.

Assuming normal operation of the various plant control systems, the following sequence of events is initiated by a tube rupture:

1. Pressurizer low pressure and low level alarms are actuated and charging pump flow increases in an attempt to maintain pressurizer level. On the secondary side there is a steam flow/feedwater flow mismatch alarm ~~before trip~~ as feedwater flow to the affected steam generator is reduced due to the additional break flow which is now being supplied to that unit.

2. Continued loss of reactor coolant inventory leads to a reactor trip signal generated by low pressurizer pressure. Resultant plant cooldown following reactor trip leads to a rapid change of pressurizer level, and the safety injection signal, initiated by low-low pressurizer pressure, follows 53 soon after the reactor trip. The safety injection signal automatically terminates normal feedwater supply and initiates auxiliary feedwater addition.

3. The steam generator blowdown liquid monitor and the condenser offgas radiation monitor will alarm, indicating a sharp increase in radioactivity in the secondary system and will automatically terminate steam generator blowdown.

4. The reactor trip automatically trips the turbine and if offsite power is available the steam dump valves open permitting steam dump to the condenser. In the event of a coincident station blackout, the steam dump valves would automatically close to protect the condenser. The steam generator pressure would rapidly increase resulting in steam discharge to the atmosphere through the steam generator safety and/or poweroperated relief valves.

5. Following reactor trip, the continued action of auxiliary feedwater supply and borated safety injection flow (supplied from the refueling water storage tank) provide a heat sink which absorbs some of the decay heat. Thus, steam bypass to the condenser, or in the case of loss of offsite power, steam relief to atmosphere, is attenuated during the 30 minutes in which the recovery procedure leading to isolation is being carried out.

0794 PKG

27. A. O. Allen, "The Radiation Chemistry of Water and Aqueous Solutions," Princeton, N. J., Van Nostrand, 1961.

28. D. A. Powers and R. O. Meyer, "Cladding Swelling and Rupture Models for LOCA Analysis," NRC Report NUREG-0630, April 1980.

29. Letter from T. M. Anderson, Westinghouse Electric Corporation to D. G. Eisenhut, U.S. Nuclear Regulatory Commission, NS-TMA-2174, December 1979.

30. "Westinghouse ECCS Evaluation Model. 1981 Version," WCAP-9220 (Proprietary Version), WCAP-9221 (Non-Proprietary Version), February 1982.

31. "Fuel Densification Experimental Results and Model For Reactor Application," WCAP-8218-A (proprietary).

32. USNRC Regulatory Guide 1.7, Revision 2, November 1978, "Control of Combustible Gas Concentrations in Containment Following a Loss of Coolant Accident".

33. "American National Standard for Decay Heat Power in Light Water Reactors," ANSI/ANS-5.1-1979, August 1979.

0794 PKG

TABLE 15.4-1

TIME SEQUENCE OF EVENTS FOR CONDITION IV EVENTS

Accident	Event	Time (Seconds)
Major Reactor Coolant System Pipe Ruptures, Double-Ended Cold Leg Guillotine*		
Major Secondary System Pipe Rupture		
1. Case A		

Event	Time (Seconds)
Steam Line Ruptures	0.0
~~High Steam Flow~~/Low Steam Pressure Setpoint Reached	0.63
Pressurizer Empties	11.0
Criticality Attained	22.4
Boron Reaches Core	56.8

2. Case B

Event	Time (Seconds)
Steam Line Ruptures	0.0
~~High Steam Flow~~/Low Steam Pressure Setpoint Reached	0.63
Pressurizer Empties	12.0
Criticality Attained	24.8
Boron Reaches Core	73.6

Accident	Event	Time (Seconds)
Single Reactor Coolant Pump Locked Rotor		
1. Four loops in operation, one locked rotor	Rotor on one pump locks	0
	Low flow trip point reached	0.03
	Rods begin to drop	1.03

*See Table 15.4-17

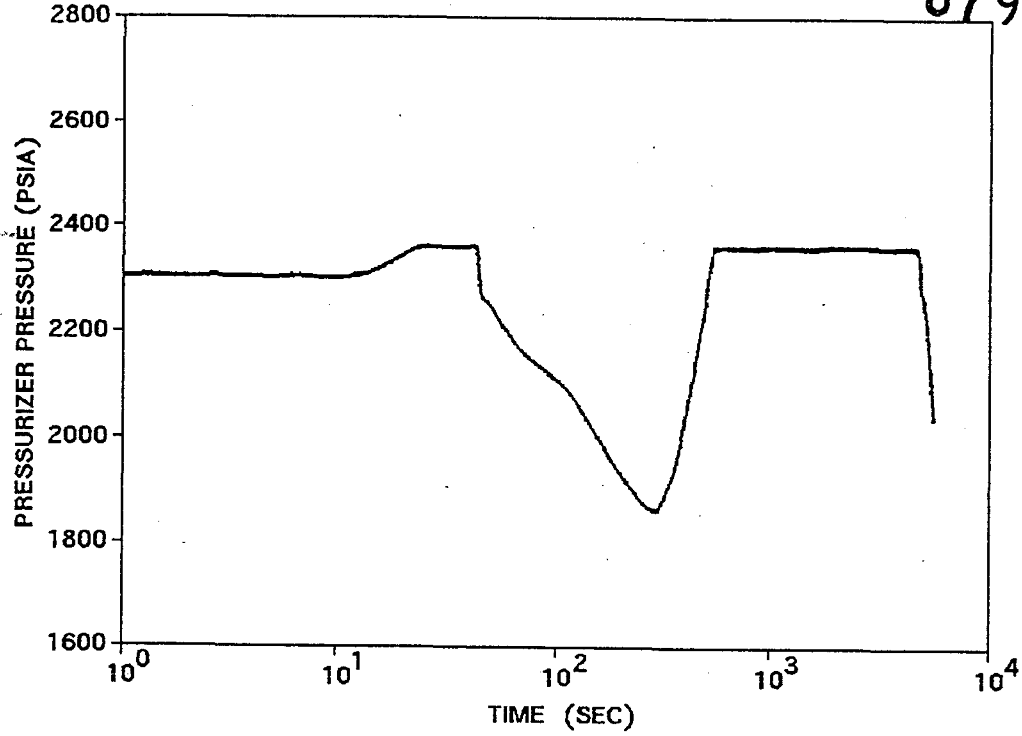
0794 PKG

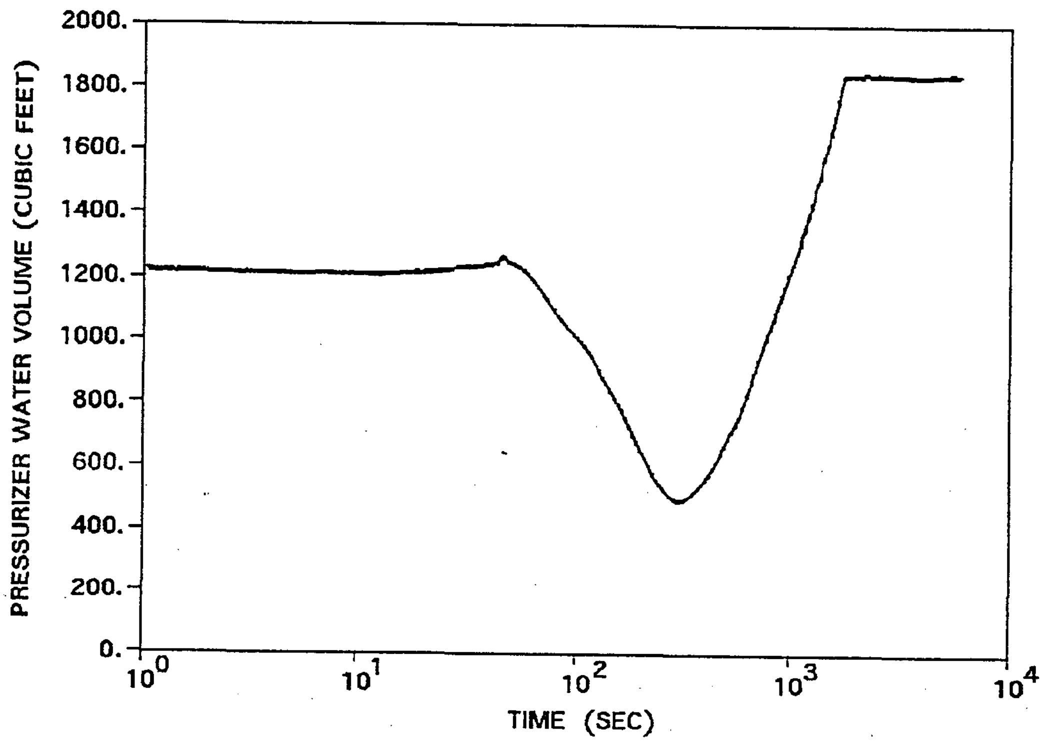
TABLE 15.4-9

TIME SEQUENCE OF EVENTS FOR FEEDLINE BREAK

Event	Time (seconds) With Offsite Power	Without Offsite Power
Feedine Rupture Occurs	10	10
Low-low steam generator level reactor trip and auxiliary feedwater pump start setpoint reached in affected steam generator	~~29~~ 36	36
Rods begin to drop	~~31~~ 38	38
Auxiliary feedwater starts to intact steam generators	~~89~~ 96	96
Cold auxiliary feedwater reaches intact SGs	260	260
~~Steam pressure too low to drive auxiliary feedwater pump~~	~~290~~	
Pressurizer ~~safety~~ relief valve setpoint reached	~~360~~ 545	740
~~Isolation of motor-driven auxiliary feed flow to the break~~	~~630~~	
Low Steamline Pressure Setpoint Reached	363	437
All main steam stop (main steam isolation) valves closed	~~630~~ 370	444
~~All reactor coolant pump power turned off~~	~~630~~	
Pressurizer water relief begins	~~825~~ 1710	4900
Core power decreases to auxiliary feedwater removal capacity	~~1860~~ ~4600	~1800

0794 PKG





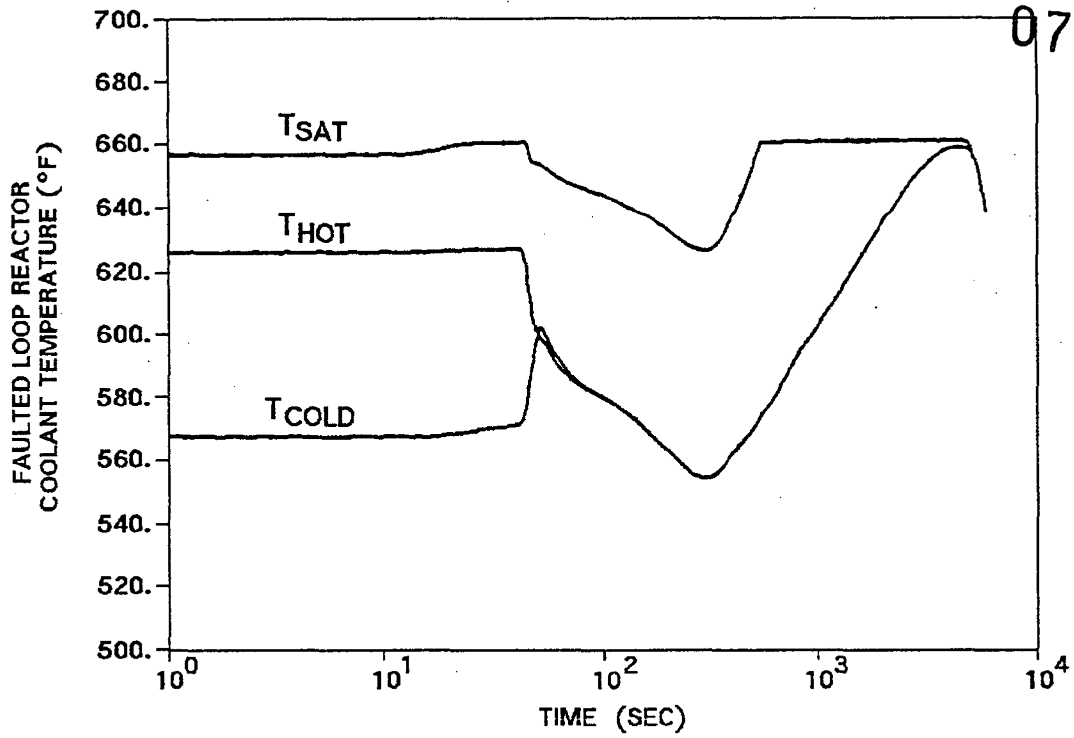
REVISED BY AMENDMENT 72

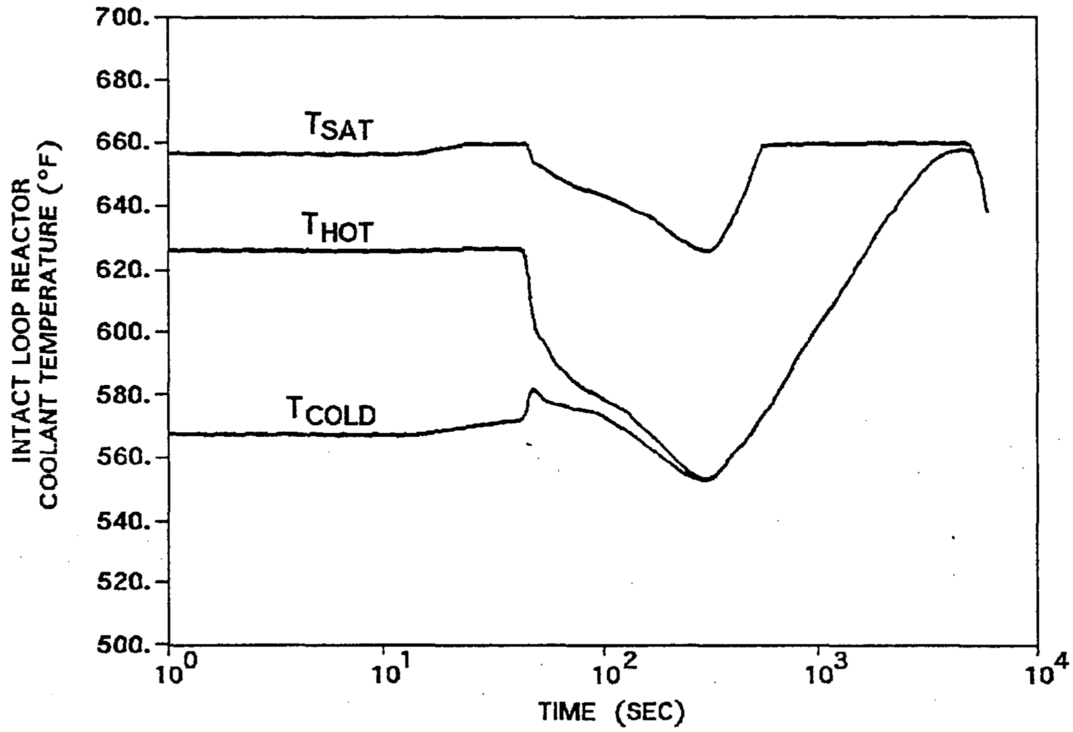
WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

PRESSURIZER PRESSURE AND WATER VOLUME TRANSIENTS FOR MAIN FEEDLINE RUPTURE WITH OFFSITE POWER

FIGURE 15.4-13A

0794 PKG





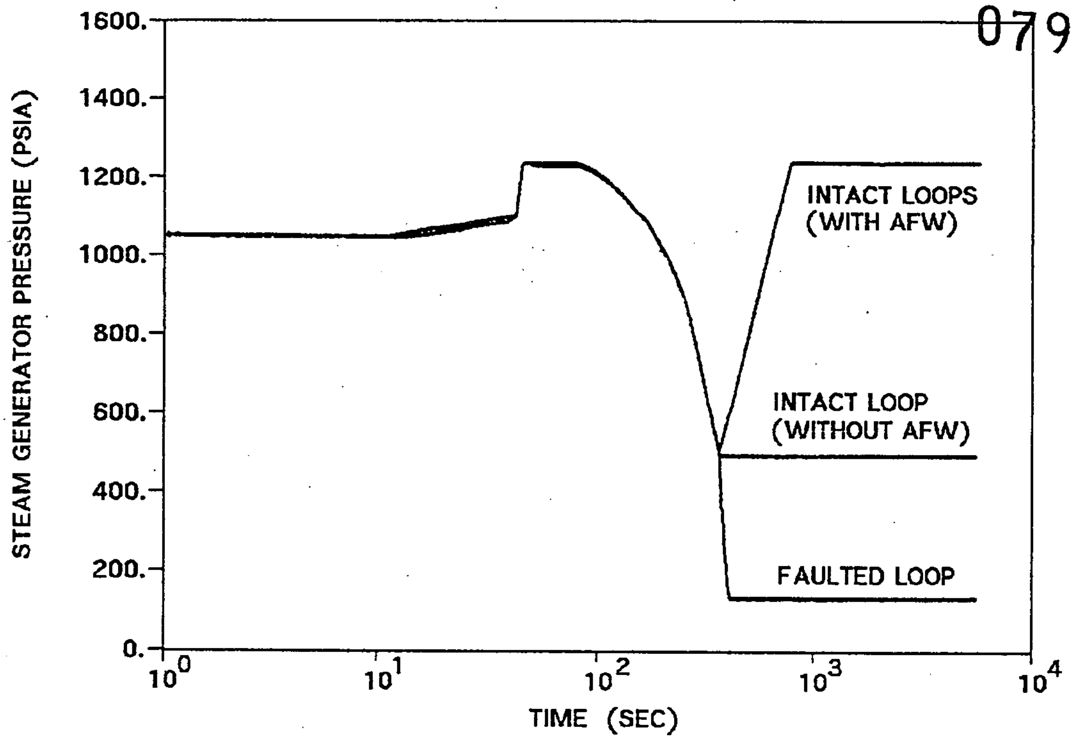
REVISED BY AMENDMENT 72

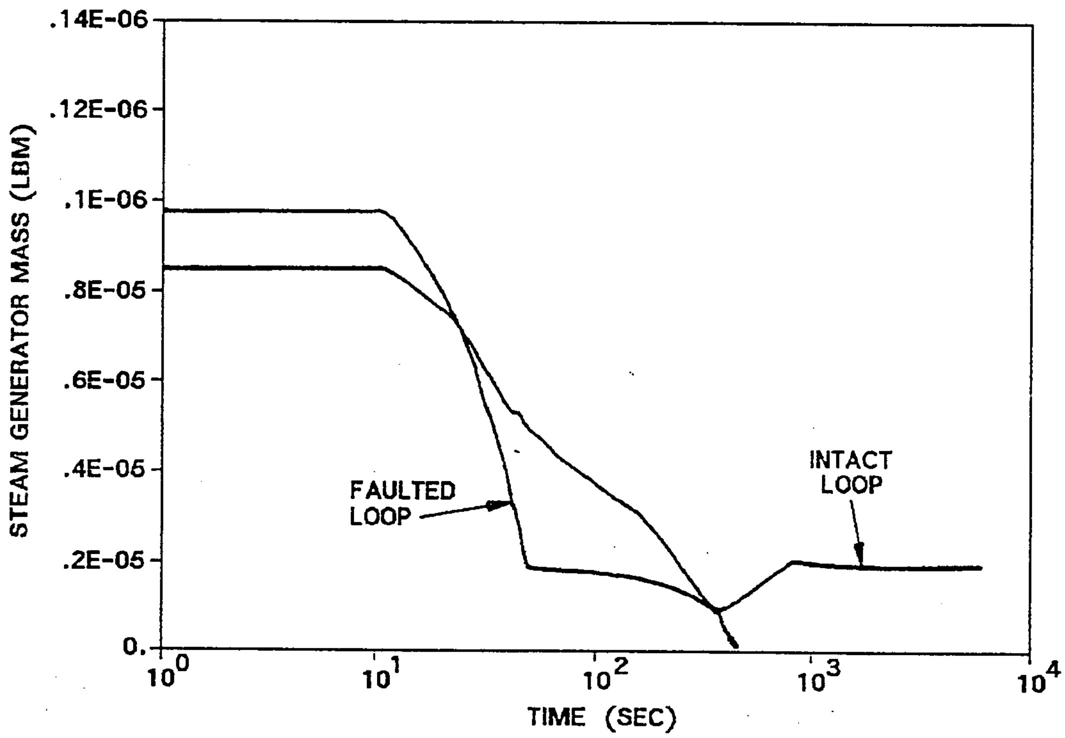
WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

REACTOR COOLANT TEMPERATURE TRANSIENTS FOR THE FAULTED AND INTACT LOOPS FOR MAIN FEEDLINE RUPTURE WITH OFFSITE POWER

FIGURE 15.4-13B

0794 PKG

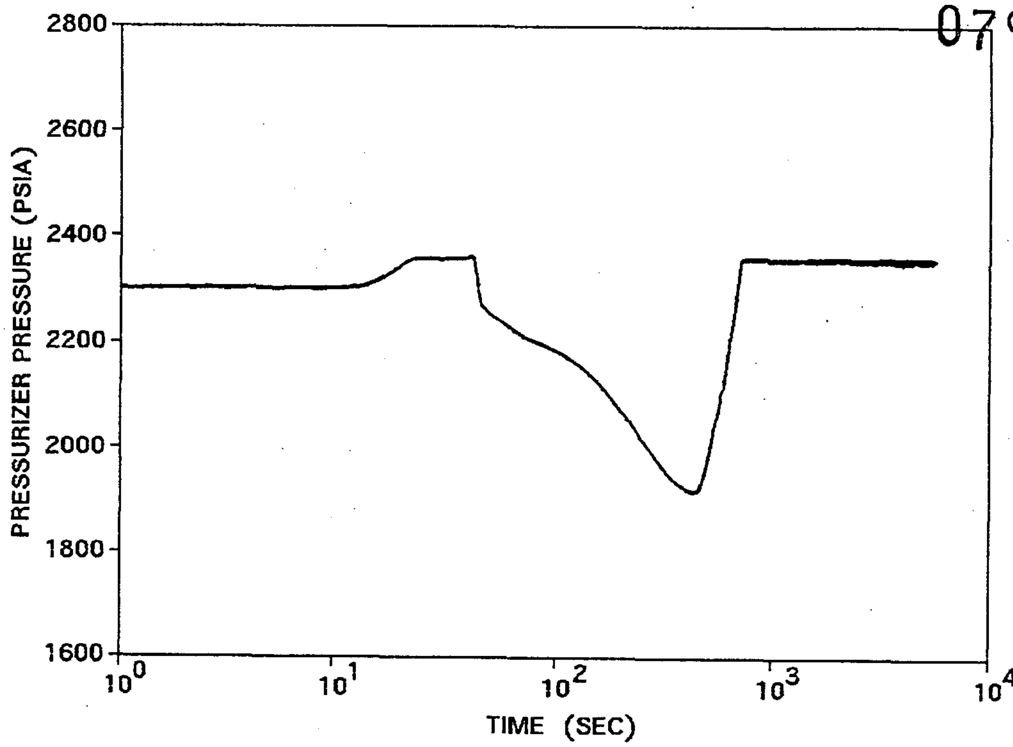


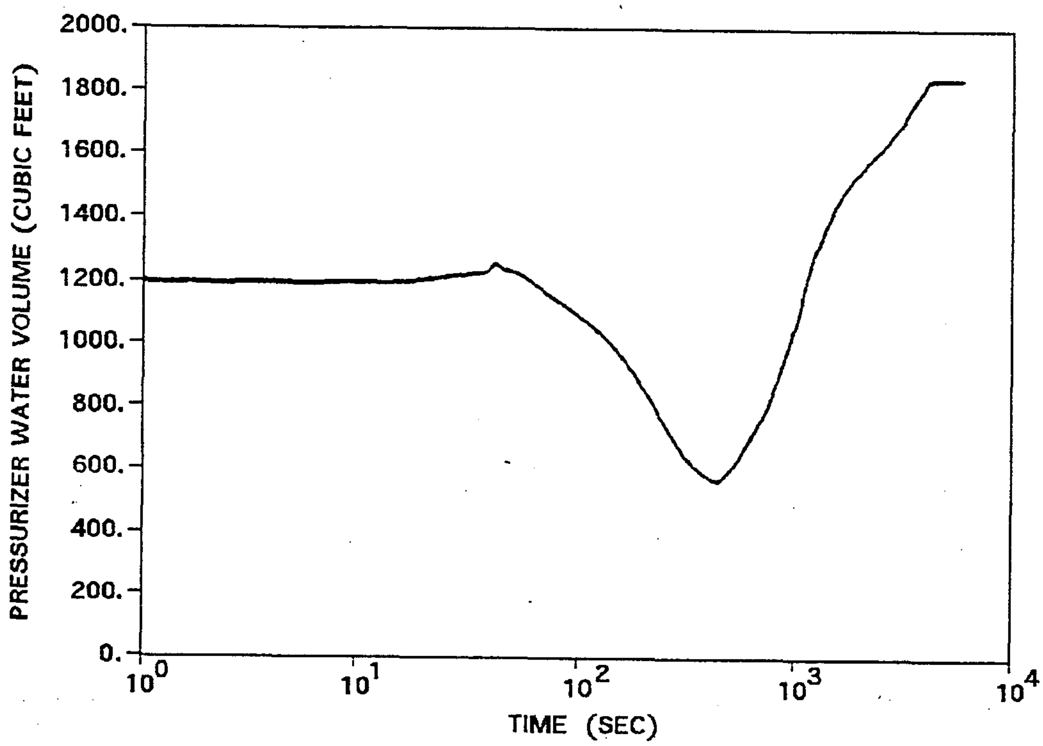


REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

STEAM GENERATOR PRESSURE
AND WATER MASS TRANSIENTS
FOR MAIN FEEDLINE RUPTURE
WITH OFFSITE POWER
FIGURE 15.4-13C



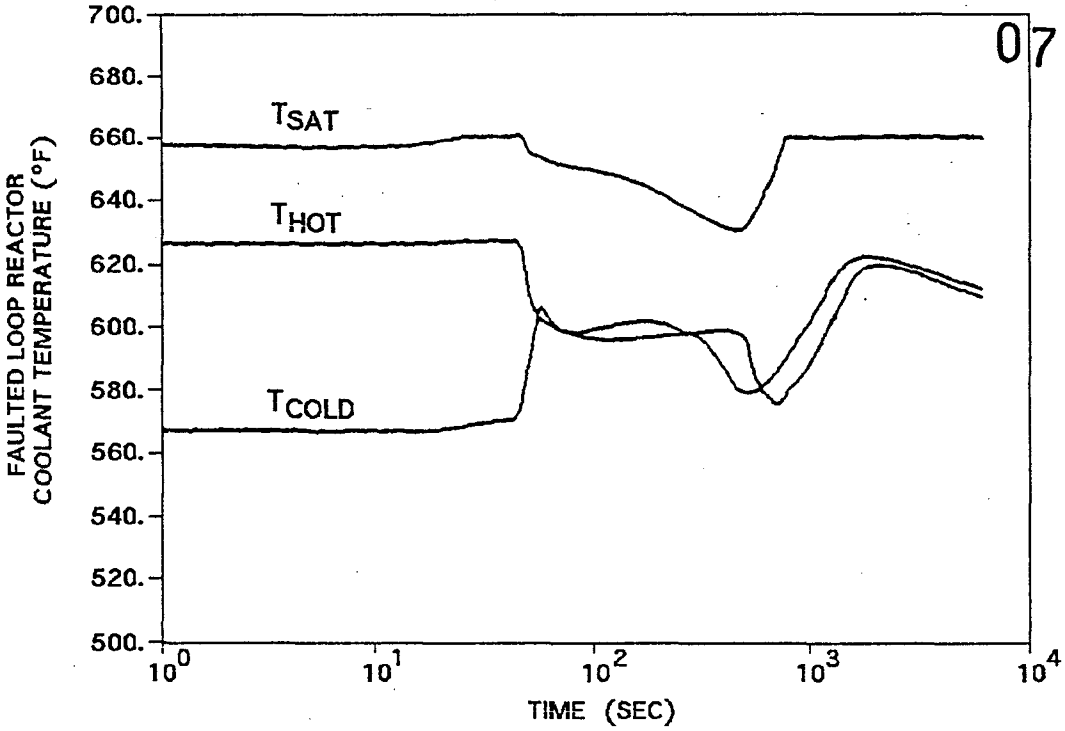


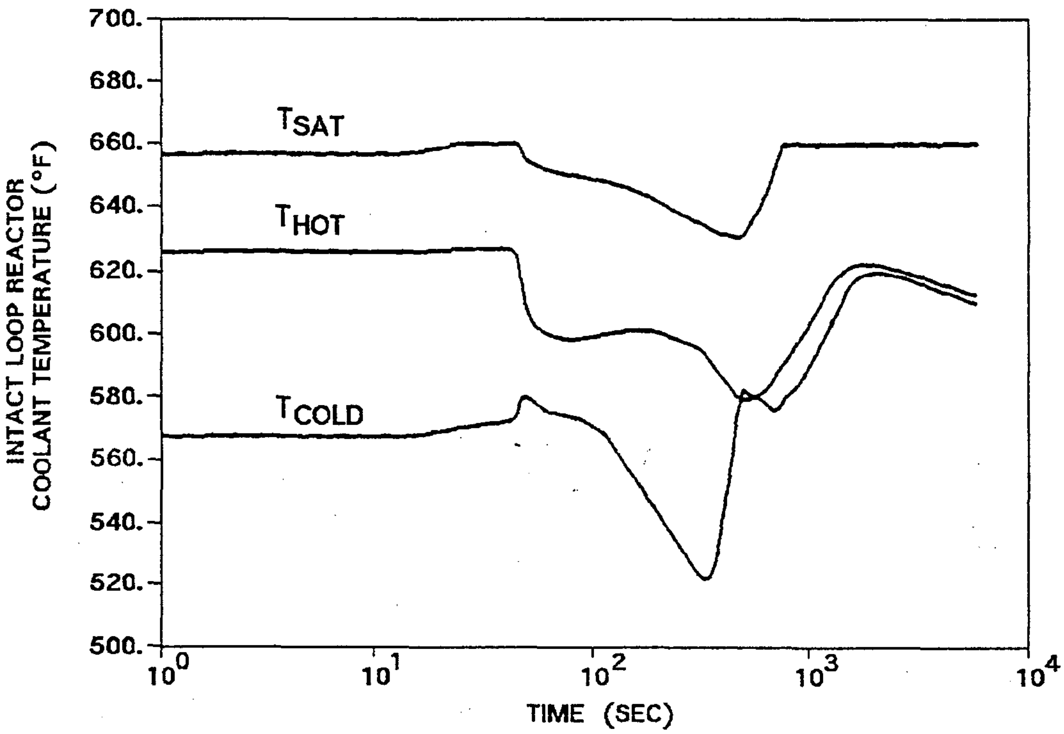
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

PRESSURIZER PRESSURE AND
WATER VOLUME TRANSIENTS
FOR MAIN FEEDLINE RUPTURE
WITH OFFSITE POWER
FIGURE 15.4-14A

0794 PKG





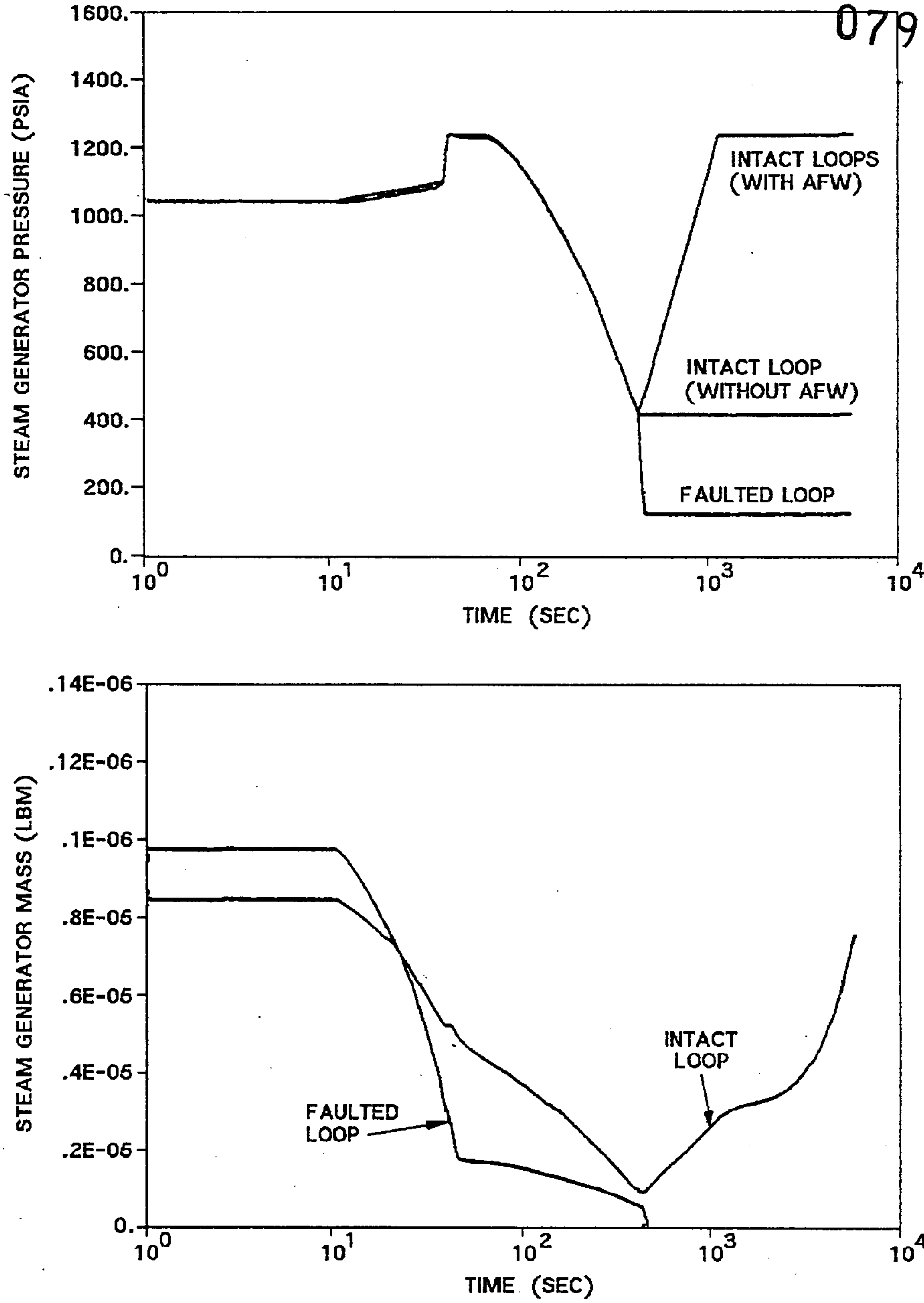
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT FINAL SAFETY ANALYSIS REPORT

REACTOR COOLANT TEMPERATURE TRANSIENTS FOR THE FAULTED AND INTACT LOOPS FOR MAIN FEEDLINE RUPTURE WITH OFFSITE POWER

FIGURE 15.4-14B

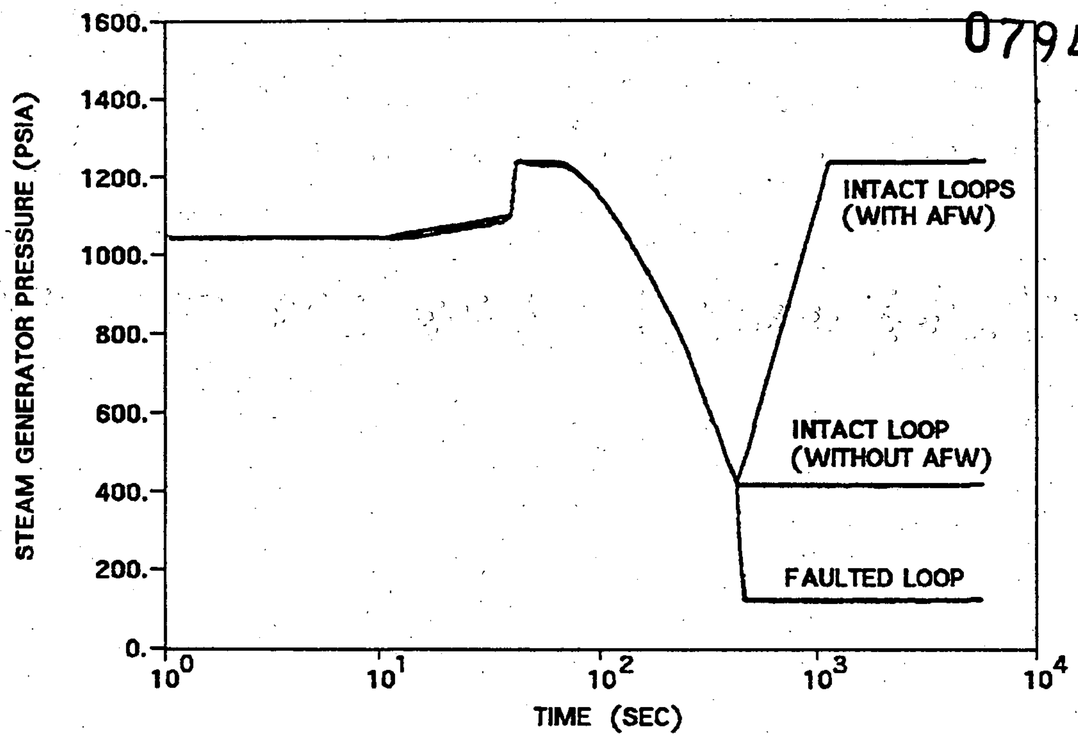
0794 PKG



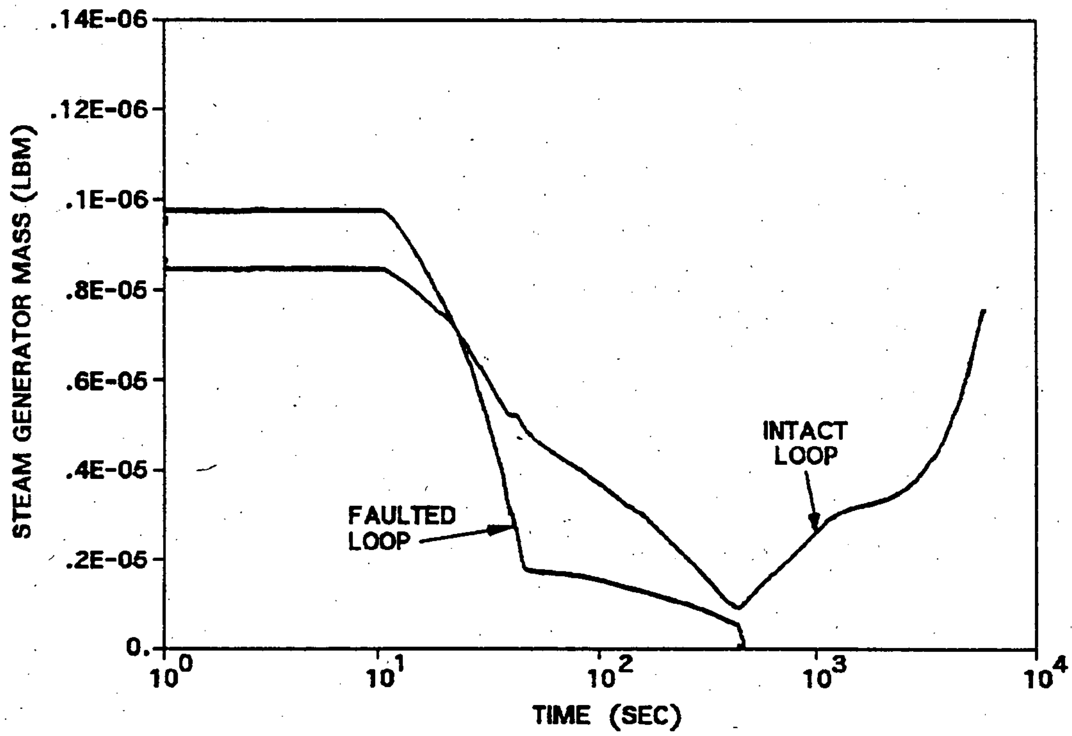
REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY ANALYSIS REPORT

STEAM GENERATOR PRESSURE AND WATER MASS TRANSIENTS FOR MAIN FEEDLINE RUPTURE WITH OFFSITE POWER
FIGURE 15.4-14C



0794 PKG



REVISED BY AMENDMENT 72

WATTS BAR NUCLEAR PLANT
FINAL SAFETY
ANALYSIS REPORT

STEAM GENERATOR PRESSURE AND WATER MASS TRANSIENTS FOR MAIN FEEDLINE RUPTURE WITH OFFSITE POWER
FIGURE 15.4-14C