Tennessee Valley Authority, Post Office Box 2000, Soddy-Daisy, Tennessee 37379-2000

January 31, 1997

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

In the matter of	)	Docket Nos. 50-327
TENNESSEE VALLEY AUTHORITY	)	50-328

SEQUOYAH NUCLEAR PLANT - AUXILIARY FEEDWATER CONTROL LOGIC

As requested at the December 16,1996 Pre-decisional Enforcement Conference, please find enclosed, an evaluation of the acceptability of the auxiliary feedwater control logic for a turbine runback condition.

Should you have any questions, please contact Jim Smith at 423-843-6672.

R. H. Shell

R H. Shell
Site Licensing and Industry Affairs Manager

A001

JDS:EAM
cc: Mr. R. W. Hernan, Project Manager
U.S. Nuclear Regulatory Commission
One White Flint, North
11555 Rockville Pike
Rockville, Maryland 20852-2739

NRC Resident Inspector
Sequoyah Nuclear Plant
2600 Igou Ferry Road
Soddy-Daisy, Tennessee 37379-3624

Mr. Tom Peebles
U.S. Nuclear Regulatory Commission
Region II
101 Marietta Street, NW, Suite 2900
Atlanta, Georgia 30323-0199

Enclosure
Evaluation for SQ963123PER
Auxiliary Feedwater Control Logic -
SEQUOYAH NUCLEAR PLANT (SQN)

Background

On October 11, 1996, Unit 2 was in an "orderly shutdown" condition in accordance with 0-G0-5 to preclude seal damage to Nos. 4 and 2 RCP seal. When the reactor power level was at approximately 45 percent power, the 2B main feedwater pump was manually shut off and an unexpected turbine runback occurred because of a failure of the turbine runback circuitry. The operators took manual control of the control rods, verified turbine load rejection and then returned the rod control system back to automatic. As the turbine load approached zero, the unit was manually tripped (0827 EST) and Emergency Procedure E-0 "Reactor Trip or Safety Injection" was entered, and then ES-0.1, "Reactor Trip Response" was entered. Since a turbine runback was initiated, the Auxiliary Feedwater (AFW) System started, and both motor-driven pumps (MDAFWP) and the turbine-driven pump (TDAFWP) started, their respective level control valves came full-open and flow was delivered to all steam generators (S/Gs) . The operators followed ES-0.1 through step 3 at which time they entered Emergency Abnormal Procedure EA-3-8, "Manual Control of AFW Flow" to control the Reactor Coolant System (RCS) cooldown based on the requirements of the 'RESPONSE NOT OBTAINED' column in ES-0.1 Step 3.

After the operators entered EA-3-8, manual control of the motor-driven level control valves could not be engaged, nor could resetting of the turbine-driven pump speed controller because of the failure of the turbine runback circuitry. Full-flow was still being delivered to all S/Gs and levels dropped to approximately 12 percent power (narrow range) in all generators. RCS temperatures decreased to 538° F. and the operators manually tripped both MDAFWP's, took manual control of the TDAFWP level control valves and maintained S/G levels within the required range of 10 to 50 percent power. These actions were complete by 0835 EST. A subsequent shutdown margin calculation was performed which demonstrated that adequate shutdown margin was available during this event.

Subsequently, a question arose as to the adequacy of the design interface between the non-safety related Balance of Plant (BOP) runback circuit and the safety-related AFW system control circuits. Specifically, the concern was whether the circuit design could preclude a loss of system function with a single failure as stated in the FSAR and as required by GDC 24 and IEEE 279-1971.

References:

Sequoyah FSAR
NUREG-0011 - SER
IEEE 279 - 1971
NUREG-0737 (Item II.E.1.2)
NUREG-0800 - Standard Review Plan
Design Criteria SQN-DC-V-13.9.8
10 CFR 50.55a (h)

Design Basis:

In the event of a loss of the main feedwater supply, the AFW System supplies sufficient feedwater to the S/Gs to remove primary system stored and residual core energy. The AFW system is designed to start automatically in the event of (1) a loss of offsite electrical power, (2) a feedwater line break, (3) safety injection, (4) lo-lo S/G level, (5) a trip of both main feedwater pumps or one main feedwater pump > 80 percent power, or (6) AMSAC, any of which will result in, may be

coincident with, or may be caused by a reactor trip. The AFW System is designed to supply sufficient feedwater to prevent the relief of primary coolant through the pressurizer safety valves and the uncovering of the core. The AFW System has adequate capacity to maintain the reactor at hot standby and then cool the RCS to the temperature at which the Residual Heat Removal System may be placed in operation.

Engineered Safety Feature (ESF) standards, including seismic conditions and single failure requirements are met for the AFW System. The required flow to two or more S/Gs will be provided regardless of any single failure in the short-term or any single active failure or credible passive failure in the long-term.

The AFW System serves as a backup system for supplying feedwater to the secondary side of the S/Gs at times when the feedwater system is not available, thereby maintaining the heat sink capabilities of the S/G. As an ESF System, the AFW System is directly relied upon to prevent core damage and system over-pressurization in the event of transients such as a loss of normal feedwater or a secondary system pipe rupture, and to provide a measure for plant cooldown following any plant transient.

The plant events which impose safety-related performance requirements on the design of the AFW System are (1) loss of main feedwater with or without offsite power available, (2) secondary system pipe ruptures (feedline or steamline), (3) loss of AC power, (4) LOCA and (5) cooldown.

Circuit Design

The design function of the BOP loss of feedpump runback circuit is an anticipation circuit for ensuring that an adequate heat sink for the RCS exists above 80 percent power turbine load. One operating main feed pump, with full condensate flow available, can only supply approximately 85 percent power of the required flow to maintain S/G levels on program. Therefore, the turbine is instructed to runback to 75 percent load, the running main feed pump speeds up to its high speed stop, the tripped main feed pumps turbine condenser isolation valves close to force full-flow to the operating main feed pump, and the AFW pumps start to guarantee that an adequate heat sink exists to preclude a reactor trip on lo-lo S/G level. This circuit is electrically isolated from the train A & B interface circuits for the above actions through interposing relays. The circuit also works from a two out of two logic sequence which makes it immune to a spurious action due to single failure in the arming circuit.

This circuit exists to ensure that secondary side transients do not result in a challenge to the primary systems. Since this circuit is not safety-related, its failure must not impair the ability of the safety-related reactor protection system from performing its function of protecting the fission product barriers. Therefore, if the turbine runback circuit failed to operate above 80 percent power turbine load, then the safety-related reactor trip function of lo-lo SG level would trip the reactor prior to loss of the heat sink and automatically initiate AFW for heat sink recovery. If a turbine runback circuit failure occurred below 80 percent power (as it did for this event), then the consequential automatic start of AFW would not be harmful for RCS overpressurization protection, however, some limited RCS overcooling and potential loss of shutdown margin would be a concern. However, redundant boration systems are provided in the design to respond to an overcooling event. As evidenced by this event, the emergency procedures provided the necessary guidance to the operator to diagnose the event and successfully mitigate the overcooling event. This scenario involved the failure of multiple components.

Operations Procedure Evaluation

Emergency Procedure E-0 is a recovery/restoration guideline utilized after a reactor trip or safety injection to assist the operator in assessing plant conditions and to identify the appropriate

recovery guidance. It is a procedure which is written to be a "blind" reaction to whatever transient or event has occurred which resulted in the entry condition. The first requirement of the procedure is to ensure that all automatic actions have occurred which protect the reactor. E-0 directs the operator to transition to ES-0.1 when the main control room (MCR) operators have identified that the safety injection is not actuated or required. ES-0.1 is utilized to verify that the plant stabilizes at no-load conditions. These actions include verification of RCS temperature and adequate shutdown margin. EA-3-8 is utilized by ES-0.1 to stabilize and control RCS overcooling by manual operation of AFW. These procedures are adequate not only for this specific event, but are written to cover the many unknown possibilities associated with transients and accidents. The RCS post-reactor trip temperature transient due to automatic AFW control is limited to approximately 520° F. based on past experience) and does not present any other safety concerns beyond the shutdown margin concern. ES-0.1 requires boration in response to overcooling to maintain shutdown margin. Redundant safety grade boration flowpaths are available.

For analyzed events such as steam line break scenarios and steam generator tube rupture event, the guidance of the Emergency Procedures E-2 and E-3 provide instructions for the operator to isolate auxiliary feedwater to the faulted S/G. Diverse methods are available to the operator to isolate AFW (close LCVs, stop and pull to lock pumps, isolate manual valves or isolate the steam supply).

Design Basis Evaluation

A. Design Basis Event Mitigation

As demonstrated in the October 11 reactor trip, multiple failures of the pressure switches in the BOP runback circuit can result in the inability to take manual control of the MDAFW LCVs and the inability to take manual control of the TDAFW speed control circuit. This condition was reviewed in this evaluation to determine if compliance with the design/licensing bases is maintained. Failure of the pressure switches in the BOP runback circuit have **no impact** on *automatic initiation* of AFW, **no impact** on *automatic control* of AFW, and **no impact** on the *manual initiation* of AFW. Consequently, there are no adverse impacts in the design basis ability of the AFW system to provide an adequate heat sink for the RCS heat-up events; only design basis events which require manual control of AFW (primarily to limit RCS cooldown to maintain adequate shutdown margin and to isolate a faulted or ruptured S/G will be addressed.

As defined in FSAR 10.4.7.2 and 15.4, two design basis events require MCR operators to take action to manually control AFW; (1) steam line break (inside or outside of containment) and (2) steam generator tube rupture. To assess the impact of the unavailable manual control circuits, the most limiting single failures are considered:

- Consider a failure of the TDAFW pump speed control to transfer to manual, in conjunction with a faulted or ruptured SG requiring isolation and a single failure that prevents an LCV to close. The flow from the TDAFW pump to the faulted S/G can be isolated via a) trip of the TDAFW pump, b) isolation of steam supply to the TDAFW pump, and/or c) local isolation of the individual AFW line by manual isolation valves. Once the manual isolation valves are closed, the TDAFW pump can be restarted if needed to supply the intact SGs.

- Consider a failure of the capability to take manual control of the MDAFW LCVs, in conjunction with a faulted or ruptured SG requiring isolation and a single failure of an emergency power train or vital battery. The flow from the

MDAFW pumps can be isolated via a) its Auxiliary Control Room LCV controller in manual, b) pull-to-lock of the MDAFW pump, or c) local isolation of the individual AFW line by manual isolation valves. Once the manual isolation valves are closed, the MDAFW pump can be restarted if needed to supply the intact S/Gs.

The AFW control system failure that prohibits taking manual control of the 1) TDAFW pump speed and 2) MDAFW LCVs does not introduce a new failure not previously analyzed. The failure of an LCV to close was previously considered in FSAR section 10.4. This failure, in conjunction with a design basis event and credible single failure, can be mitigated using the existing AFW System design, emergency procedures and operator capability.

B. Compliance with the FSAR, NRC Design Criteria and Industry Standards

1. NRC General Design Criteria GDC 24 Evaluation (FSAR 3.1)

"Separation of protection and control systems. The protection system shall be separated from control systems to the extent that failure 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 systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety in not significantly impaired."

The SQN commitment to GDC 24 relative to the AFW System is defined in FSAR Section 7.3, Engineered Safety Features (ESF) Actuation System. The ESF Actuation System, as defined in Chapter 7 applies to the process portion which monitors various plant parameters and the digital portion which receives input from the process portion and performs the logic necessary to actuate the ESFs. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment vessel penetrations and process protection racks, terminating in the slave relays. As stated in FSAR 7.3.1.1.4, the actuation circuitry requirements (for the AFW System) are defined in FSAR Chapter 6 (which refers to Section 10. 4.7.2), which contain the requirements for design of the AFW control System. Chapters 6 and 10 (AFW actuation circuits) do not state that compliance with GDC 24 is required. Therefore, GDC 24 is applicable to the ESFAS from the plant parameter input to the slave relays. GDC 24 requirements are not applicable to the AFW actuation circuits downstream of the slave relays. From a historical perspective, FSAR Chapter 7.3 information on ESFAS was prepared by the NSSS vendor and addressed their scope of supply on the protection system. TVA's scope of supply was addressed in Chapter 10. The TVA portion of the scope of supply was reviewed extensively by NRC as part of NUREG-0737 Item II.E.1.2. The review was performed to SRP 10.4.9 and documented in FSAR Chapter 10.4.7 (Table 10.4.7-10). GDC 24 is not a requirement specified in the SRP. Effectively, GDC 24 requirements apply at the system actuation level for ESFAS and not at the individual component level for AFW.

Although GDC 24 does not apply to the AFW actuation circuits, the design of the system at SQN meets the intent of the requirements. The actuation of the control system cascades through the protective system to position specific pumps and valves to the required positions in response to a potential undercooling event.

Automatic actuation and control is not impaired. In the event of an undesired actuation of the control system and the potential for an overcooling event, the MCRoperators have the ability to (1) mitigate the potential loss of shutdown margin due to overcooling using redundant ESF boration systems and to (2) manually override the protective system by closing the TDAFW injection valves and/or stopping the TDAFW pump by tripping the trip/throttle valve or by closing the steam supply valves. The MDAFW pump can also be tripped by the control room operators to stop the unwanted flow of AFW from this system. In the event of a faulted S/G, the MCR operators have the ability to limit, or terminate flow to the faulted S/G by tripping one or both of the AFW pumps feeding the faulted S/G until the LCVs or other valve(s) in the line is (are) manually closed. Single failures are addressed in item A above.

2. IEEE 279-1971 Evaluation

The referenced segment of IEEE 279-1971 is 4.17 which states;

"*Manual Initiation. The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation., safety injection, core spray, etc). No single failure, as defined by the note following Section 4.2, within the manual, automatic, of common portions of the protection system shall prevent initiation of protective action by manual or automatic means. Manual initiation should depend upon the operation of a minimum of equipment.*

Section 4.2 reads as follows;

"*Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required. NOTE: "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.*

Manual initiation of the protective system is accomplished without consideration to the control system. The control system will not prevent any actuation of the protective system but will only influence what controlling actions the protective system will take. In other words, with the runback signal from the control system, the protective system (AFW) will operate in an automatic (for MDAFW) or full-flow (for TDAFW) mode. As noted in design basis event evaluation, other manual actions are available to mitigate and to terminate the overcooling event should it occur.

The original design did not consider multiple pressure switch failures (e.g., water intrusion from a spurious fire system actuation) as a credible event. Subsequently, the fire detection system has been modified to replace the fire detectors with a weatherproof design, making it less vulnerable to spurious actuation. The pressure switch conduits/junction box system has been sealed to prevent water intrusion. As a result, TVA considers a repeat of this event to not be credible.

3. FSAR Evaluation

Section 7.1.2.1.2 and 7.3.1.2.2 These sections state that the ESFAS has provisions for manually initiating (actuating) from the control room all of the functions of the ESF system. Manual actuation serves as a backup to automatic initiation.

The AFW System is automatically initiated and controlled by an ESFAS actuation. If a failure in the BOP runback circuit results in a non-functional MDAFW pump LCV manual control circuit and a non-functional TDAFW pump manual speed control circuit, AFW can still be manually initiated with the MDAFW pump switches and opening the steam supply to the TDAFW pump. Once initiated, MDAFW flow is automatically controlled and can be manually controlled, if needed, as described above in accordance with Emergency Procedures. Similarly, the TDAFW pump operates at full speed and its LCV can be manually controlled, if needed.

Section 7.7.2.1 - This section of the FSAR basically states that a failure in control circuitry will not adversely effect a protective function. A failure in the BOP runback circuit will not adversely effect the protective function of AFW, as described within this report.

Section 10.4.7.2.1 and 15.4 - In the "Secondary System Pipe Ruptures" subparagraph, the FSAR states that the AFW system design must allow for terminating, limiting, or minimizing that fraction of AFW which is delivered to a faulted loop or spilled through a break in order to ensure that sufficient flow will be delivered to the remaining effective steam generator(s) and to prevent containment over-pressurization following a steamline break inside containment. The FSAR considers the isolation of AFW flow to a faulted SG as a manual action to be accomplished within 10 minutes. As described above and per Emergency Procedures, manual actions can be performed to terminate or limit the flow of AFW to a faulted loop in the event of the most critical single failure coincident with a failure in the BOP runback circuit which disables the manual control circuits of the MDAFW LCVs and the TDAFW pump speed control.

In the "Station Blackout" subparagraph, the FSAR states that SG level can be maintained by controlling TDAFW pump speed and by closing the TDAFW pump LCVs using available air from accumulator tank and high pressure air cylinder. If the postulated failure of the BOP runback circuit occurs coincident with station blackout, the interposing relay in the BOP runback circuit cannot be energized (because of the blackout), removing the consequences of the failure of the pressure switches and any impact on the AFW control circuits.

Section 10.4.7.2.3 and Section 15.4 - In the "Steamline Break" subparagraph, the FSAR states that AFW flow is assumed to exist to the faulted S/G until AFW flow is manually realigned by the MCR operator 10 minutes after a fault initiation. A failure in the BOP runback circuit will not prevent the MCR operator from full-filling this action as previously described. It is also noted that the FSAR states that if a remotely controlled AFW LCV should fail to close for unspecified reasons, the operator can trip one or both of the MAFW pumps feeding the faulted SG to isolate AFW until the failed LCV or other(s) in the line is (are) manually closed.

In the subparagraph defining SQN compliance with NUREG-0578, the FSAR states that each AFW pump has manual initiation capability independent of automatic initiation. If a failure in the BOP runback circuit results in a non-functional MDAFW pump LCV manual control circuit and a non-functional TDAFW pump manual speed control circuit, AFW can still be manually initiated with the MDAFW pump switches and opening the steam supply to the TDAFW pump. Once initiated, AFW flow can be manually controlled, if needed, as previously described.

Section 10.4.7.2.5 and Section 15.4 - The FSAR states that the MCR operator can take manual control of the MDAFW pump LCVs by blocking the accident signal. **Although the operator cannot take manual control of the LCVs by blocking the accident signal if a failure of the BOP circuit has occurred coincident with the accident, the LCV can be manually controlled in the auxiliary control room. Other means (as stated previously) are also available to isolate flow to a faulted SG.**

In the subparagraph defining SQN compliance with Regulatory Guide 1.62, the FSAR states the all AFW pumps can be started either remote-manually or locally. As noted previously, the failure of the pressure switches in the BOP runback circuit does not impair the ability to manually (remotely or locally) start the AFW pumps.

C. Containment Isolation - AFW LCVs

AFW penetrations, X-40A and X-40B are considered a "closed system" inside containment with an isolation valve outside containment (the level control valves). The closed system requirements of Standard Review Plan 6.2.4 are satisfied by this configuration and meet the requirements of GDC 57 based on an NRC approved exemption in NUREG-0011, Supplement 5, Section 6.2.4 for use of a TVA Class C (ASME Code Class 3) valve and piping outside of containment as the outer boundary. The original design of the plant utilized a check valve outside of containment (ASME Code Class 2) as the outer boundary per the requirements of the 1967 AEC criterion 53 bases. The designation of a "containment isolation" valve outside of containment for the closed system was done to attempt to meet the 10CFR50 Appendix A GDC 57. The level control valves do not receive a containment isolation signal since these lines will be in use post-event and are not required to close for containment isolation reasons. It is also noted that if the AFW is not inservice, the level control valves close automatically even with the BOP runback circuit failure.

The Class B (ASME Code Class 2) portion of the S/G, tube sheet and the piping inside containment up to the containment vessel is the "containment boundary" for Appendix J and accident analysis purposes. In addition, 10CFR50 Appendix J local leakrate testing (Type C) of these penetrations and valves are not required based on Section 3.5 of ANSI/ANS-56.2-1984 and the definition of Type C tests in 10CFR50 Appendix J Section II Part H. In accordance with ANS-56.2 document, the Type A integrated leakrate testing satisfies the leakrate requirements for secondary side penetrations. A Single Failure of the LCV to close if required for steam generator isolation for a faulted steam generator is acceptable since this is a non-radioactive event and ultimately does not require containment isolation. Failure of an LCV to close during a S/G tube rupture event is bounded by the radiological consequences previously evaluated for the SGTR event (i.e., S/G tube ruptures do not lead to core damage, 10CFR100 limits are based on 125,000 lbm of steam released to the atmosphere through the S/G safeties). Failure of an LCV to isolate during a LOCA event is not evaluated since the

S/Gs are intact and the piping and vessel inside containment are the containment isolation boundary. These conditions bound the assumed failure of the LCV itself and a concurrent failure of the BOP runback circuit.

Original Design Considerations

The original design of the BOP runback circuit intended to provide single failure protection by requiring two of two pressure switch logic in combination with a trip of either main feedpump to activate the circuit, start the BOP runback and automatically initiate AFW. As was identified in the October reactor trip, an unanticipated common failure mode existed which could (and did) cause concurrent failures of both pressure switches. With sealing of the junction boxes and replacement of the existing fire detector with a sealed detector, the identified common mode failure has been eliminated. It is also noted that other postulated plant events (such as fires and earthquakes) which could cause concurrent failure of the pressure switches are bounded by the above analysis.

The original design of the BOP runback circuit and the interface with the AFW control circuits were evaluated extensively post-TMI by the NRC in NUREG-0737. This design feature was described in the FSAR text and on the drawings.

Conclusion

The AFW System (including the control circuitry) complies with the SQN design and licensing basis. However, TVA intends to improve the design of the AFW control circuits to either (1) enable the runback signal to be reset, permitting manual control of the MDAFW pump LCVs and the TDAFW pump speed or (2) add a local indicator of the "armed" status of the circuit.

I:license:wordoc:afwlogicr1