Docket No. 50-245
B15692

Attachment 3

Millstone Nuclear Power Station, Unit No. 1

Proposed Technical Specifications Revision
Safety Relief Valves

Marked-up Version of Current Technical Specification

July 1996

~~December 29, 1995~~

LIMITING CONDITION FOR OPERATION

3.6 PRIMARY SYSTEM BOUNDARY

D. Coolant Leakage

Whenever irradiated fuel is in the reactor vessel, reactor coolant leakage into the primary containment from unidentified sources shall not exceed 2.5 gpm. In addition, the total reactor coolant system leakage into the primary containment shall not exceed 25 gpm. If these conditions cannot be met, or if leak rate cannot be determined, initiate an orderly shutdown and have the reactor in the COLD SHUTDOWN or REFUEL CONDITION within 24 hours.

E. Safety and Relief Valves

1. ~~During power operation or~~ Whenever the reactor coolant pressure is greater than 90 psig with irradiated fuel in the reactor vessel, the safety valve function of at least five safety/relief valves shall be operable, except as specified in 3.6.B.1.b. (The solenoid activated relief function of the safety/relief valves shall be operable as required by Specification 3.5.D.). (1)e

automatic Pressure relief (APR)

SURVEILLANCE REQUIREMENTS

4.6 PRIMARY SYSTEM BOUNDARY

D. Coolant Leakage

Reactor coolant system leakage into the primary containment shall be checked and recorded at least once every 8 hours, unless the reactor is in the COLD SHUTDOWN or REFUEL CONDITION.

E. Safety and Relief Valves

1. All six of the safety/relief valves top works shall be bench checked or replaced with a bench checked top works each refueling outage.

   a. Prior to startup from each refueling outage, all lift settings for all 6 safety/relief valves shall be within ± 1% of the nominal setpoint(s) as shown below:

No. of Valves	Nominal Setpoint (psig)
1	1095 ± 1%
1	1110 ± 1%
4	1125 ± 1%

~~May 21, 1995~~

SURVEILLANCE REQUIREMENTS (continued)

4.6 PRIMARY SYSTEM BOUNDARY

E. Safety and Relief Valves

1. b. During each refueling outage, determine the as-found lift setpoints of all 6 safety/relief valves. Verify at least 5 of the 6 safety/relief valves are as follows:

No. of Valves	Nominal Setpoint (psig)
1	1095 ± 3%
1	1110 ± 3%
4	1125 ± 3%

2. OPERABILITY of the electrical lift system shall be demonstrated as follows:

a. Whenever the reactor coolant pressure is greater than 90 psig with irradiated fuel in the reactor vessel, an INSTRUMENT CHECK of both electrical lift systems shall be performed daily.

b. During each refueling outage, a SIMULATED AUTOMATIC ACTUATION of both electrical lift systems shall be performed throughout its operating sequence, but excluding actual valve opening.

c. During each refueling outage, an INSTRUMENT CALIBRATION of both electrical lift systems shall be performed.

new

new

new

LIMITING CONDITION FOR OPERATION (continued)

3.6. PRIMARY SYSTEM BOUNDARY

E. Safety and Relief Valves

2. When the safety/relief valves are required to be operable per Specification 3.6.E.1, both electrical lift systems for the safety/relief valves shall be OPERABLE except as specified in 3.6.E.3 below.

3. With one electrical lift system inoperable, restore the system to OPERABLE status within 7 days; otherwise, reduce reactor coolant pressure to less than 90 psig within the subsequent 24 hours.

new

LIMITING CONDITION FOR OPERATION (continued)

3.6 PRIMARY SYSTEM BOUNDARY

E. 4. If Specification 3.6.E.1 or 3.6.E.2 is not met, initiate an orderly shutdown and have the reactor coolant pressure below 90 psig within 24 hours.

5. When the safety/relief valves are required to be operable per Specification 3.6.E.1, the Valve Position Indication shall be operable. Two of the six channels may be out of service provided backup indication for the affected valves is provided by the Valve Discharge Temperature Monitor.

6. If Specification 3.6.E.5 is not met, reactor operation with reactor coolant pressure greater than 90 psig is permissible only for the succeeding 30 days unless the Valve Position Indication System is made operable sooner.

F. Structural Integrity

The structural integrity of the primary boundary shall be maintained as specified in Technical Specification 3.13.

SURVEILLANCE REQUIREMENTS

4.6 PRIMARY SYSTEM BOUNDARY

E. 3. At least one of the safety/relief valves shall be disassembled and inspected each refueling outage.

4. During the initial startup from each refuel outage, within 24 hours of the mode switch being placed in the RUN position, and with reactor power less than 25% of rated; each safety/relief valve shall be manually opened until valve operability has been verified by torus water level instrumentation or by an audible discharge detected by an individual located outside the torus in the vicinity of each discharge line.

5. The Valve Position Indication System shall be functionally tested once every three months and calibrated once per operating cycle. Due to the inaccessability of the pressure switches (in the drywell), the functional test shall consist of a simulated signal into the monitoring channel rather than the instrument.

6. The valve discharge temperature monitor shall be calibrated at least once per operating cycle.

F. Structural Integrity

Inservice Inspection and Testing of primary system boundary components shall be performed as specified in Surveillance Requirement 4.13.

E. Safety and Relief Valves

Place Insert here

Experience with the safety/relief valves indicates that testing of all safety valves per refueling outage is appropriate to detect failures or deterioration until more experience is gained. A tolerance of 1% in the lift setpoint is specified for all valves at restart from a refueling outage. This ensures that all valves have been adjusted to the optimal conditions at the beginning of the cycle.

The safety/relief valves have two functions: i.e., power relief or self-actuated by high pressure. The solenoid actuated function (automatic pressure relief) is that in which external instrumentation signals of coincident high drywell pressure and low-low water level initiate the valves to open. This function is discussed in Specification 3.5.D. In addition, the valves can be operated manually.

The safety function is performed by the same safety/relief valve with a pilot valve causing main valve operation.

It is understood that portions of the Valve Position Indication System cannot be repaired or replaced during operation, therefore, the plant must be shutdown to accomplish such repairs. The 30-day period to do this allows the operator the flexibility to choose his time for shutdown; meanwhile, because of the redundancy provided by the valve discharge temperature monitor and the continued monitoring of the remaining valves by both methods, the ability to detect the opening of a safety/relief valve would not be compromised. The valve operability is not affected by failure of the Valve Position Indication System.

When the setpoint is being bench checked, it is prudent to disassemble one of the safety/relief valves to examine for crud buildup, bending of certain actuator members or other signs of possible deterioration.

move

A manual actuation of each SRV is performed to verify the valve and solenoid are functioning properly and no blockage exists in the SRV discharge lines. It has been demonstrated that the blowdown of an SRV to the torus causes a wave action that is detectable on the torus water level instrumentation. The discharge of a relief line is audible to an individual located outside the torus in the vicinity of the line, as experienced at other BWRs.

mode

Adequate reactor steam dome pressure must be available to perform this test to avoid damaging the valve. This test is performed no more than 24 hours after the switch being placed in the RUN position. This requirement, which is sufficient to allow testing at high enough pressure while limiting reactor power to less than 25 percent power, ensures that the remaining SRVs are adequate to handle any transient in the unlikely event that one SRV discharge line is found blocked. Reactor start-up is allowed prior to performing this test because valve operability and the set points for overpressure protection are verified, per ASME requirements, prior to valve installation.

INSERT to BASES 3.6.E (Page B 3/4 6-4a)

The safety/relief valves have two functions: i.e., power relief and safety. The power relief function is the automatic pressure relief (APR) mode. Power relief actuation is initiated by high drywell pressure coincident with low-low water level. This function is discussed in the Bases for Specification 3.5.D. The safety function is to limit system pressure to less than 110% of the design pressure. The safety function is initiated when steamline pressure increases to the valves's setpoint. There are two methods to ensure the valves open at the appropriate pressure: high pressure actuation via a pilot valve (mechanical lift) and pressure sensor actuation that will open the pilot valve via a solenoid actuator (electrical lift). The mechanical and electric lift functions are necessary to support OPERABILITY of the SRV safety function.

The electrical lift function is a backup, and does not replace the mechanical actuation on high pressure. The electrical lift feature employs two separate systems. The logic is configured in a two-out-of-two-taken-once format in each system. Each system is powered from a separate power source. One system is powered by VAC and the other by IAC. Since the IAC is interruptible upon loss of normal power, 125V DC battery backup power is provided. Upon loss of IAC, power supply to the logic will automatically switch to the battery backup to maintain an uninterruptible supply. Continuity of DC power supply to the SRV pilot solenoid is ensured by use of power-seeking relays in the circuitry.

During reactor power operation, the mechanical lift function cannot be verified, therefore, no in service surveillances are specified. For the electrical lift, an INSTRUMENT CHECK will detect any significant drift in the analog sensor input. This check is performed daily.

At the end of each cycle (during the refueling outage) verification that both the mechanical lift and the electrical lift would function is performed. For the mechanical lift, the as-found lift point is determined by bench testing. Confirmation is made that at least five of the six valves would open within ±3 %. Experience with the safety/relief valves indicates that testing of all safety valves each refueling outage is appropriate to detect failure or deterioration until more experience is gained. A tolerance of 1 % in the lift setpoint is specified for all valves at restart from a refueling outage. This ensures all valves have been adjusted to the optimal conditions at the beginning of each cycle. For electrical lift, verification that the system would function is accomplished by performing a SIMULATED AUTOMATIC ACTUATION and an INSTRUMENT CALIBRATION.

The simulated automatic actuation test demonstrates the operability of the required trip logic. The refuel frequency is based upon the increased potential for an unplanned transient if the surveillance were performed with the reactor at power, and operating experience with similar equipment already in use at the plant.

The instrument calibration ensures that each channel is set consistent with the measurement and setpoint error historical determinations. The refuel frequency is supported by a 30 month interval (24 month + 25%)used for the determination of the magnitude of equipment drift in the setpoint analysis.

Docket No. 50-245
B15692

Attachment 4

Millstone Nuclear Power Station, Unit No. 1

Proposed Technical Specifications Revision
Safety Relief Valves

Retyped Technical Specification

July 1996

LIMITING CONDITION FOR OPERATION

3.6 PRIMARY SYSTE I BOUNDARY

D. Coolant Leakage

Whenever irradiated fuel is in the reactor vessel, reactor coolant leakage into the primary containment from unidentified sources shall not exceed 2.5 gpm. In addition, the total reactor coolant system leakage into the primary containment shall not exceed 25 gpm. If these conditions cannot be met, or if leak rate cannot be determined, initiate an orderly shutdown and have the reactor in the COLD SHUTDOWN or REFUEL CONDITION within 24 hours.

E. Safety and Relief Valves

1. Whenever the reactor coolant pressure is greater than 90 psig with irradiated fuel in the reactor vessel, the safety valve function of at least five safety/relief valves shall be operable, except as specified in 3.6.B.1.b. (The solenoid activated automatic pressure relief (APR) function of the safety/relief valves shall be operable as required by Specification 3.5.D.).

SURVEILLANCE REQUIREMENTS

4.6 PRIMARY SYSTEM BOUNDARY

D. Coolant Leakage

Reactor coolant system leakage into the primary containment shall be checked and recorded at least once every 8 hours, unless the reactor is in the COLD SHUTDOWN or REFUEL CONDITION.

E. Safety and Relief Valves

1. All six of the safety/relief valves top works shall be bench checked or replaced with a bench checked top works each refueling outage.

   a. Prior to startup from each refueling outage, all lift settings for all 6 safety/relief valves shall be within ± 1% of the nominal setpoint(s) as shown below:

No. of Valves	Nominal Setpoint (psig)
1	1095 ± 1%
1	1110 ± 1%
4	1125 ± 1%

LIMITING CONDITION FOR OPERATION (continued)

3.6. PRIMARY SYSTEM BOUNDARY

E. Safety and Relief Valves

2. When the safety/relief valves are required to be operable per Specification 3.6.E.1, both electrical lift systems for the safety/relief valves shall be OPERABLE except as specified in 3.6.E.3 below.

3. With one electrical lift system inoperable, restore the system to OPERABLE status within 7 days; otherwise, reduce reactor coolant pressure to less than 90 psig within the subsequent 24 hours.

SURVEILLANCE REQUIREMENTS

4.6. PRIMARY SYSTEM BOUNDARY

E. Safety and Relief Valves

1. b. During each refueling outage, determine the as-found lift setpoints of all 6 safety/relief valves. Verify at least 5 of the 6 safety/relief valves are as follows:

No. of Valves	Nominal Setpoint (psig)
1	1095 ± 3 %
1	1110 ± 3 %
4	1125 ± 3 %

2. OPERABILITY of the electrical lift system shall be demonstrated as follows:

a. Whenever the reactor coolant pressure is greater than 90 psig with irradiated fuel in the reactor vessel, an INSTRUMENT CHECK of both electrical lift systems shall be performed daily.

b. During each refueling outage, a SIMULATED AUTOMATIC ACTUATION of both electrical lift systems shall be performed throughout its operating sequence, but excluding actual valve opening.

c. During each refueling outage, an INSTRUMENT CALIBRATION of both electrical lift systems shall be performed.

3. At least one of the safety/relief valves shall be disassembled and inspected each refueling outage.

LIMITING CONDITION FOR OPERATION (continued)

3.6 PRIMARY SYSTEM BOUNDARY

E. 4. If Specification 3.6.E.1 or 3.6.E.2 is not met, initiate an orderly shutdown and have the reactor coolant pressure below 90 psig within 24 hours.

5. When the safety/relief valves are required to be operable per Specification 3.6.E.1, the Valve Position Indication shall be operable. Two of the six channels may be out of service provided backup indication for the affected valves is provided by the Valve Discharge Temperature Monitor.

6. If Specification 3.6.E.5 is not met, operation with reactor coolant pressure greater than 90 psig is permissible only for the succeeding 30 days unless the Valve Position Indication System is made operable sooner.

F. Structural Integrity

The structural integrity of the primary boundary shall be maintained as specified in Technical Specification 3.13.

SURVEILLANCE REQUIREMENTS

4.6 PRIMARY SYSTEM BOUNDARY

E. 4. During the initial startup from each refuel outage, within 24 hours of the mode switch being placed in the RUN position, and with reactor power less than 25% of rated; each safety/relief valve shall be manually opened until valve operability has been verified by torus water level instrumentation or by an audible discharge detected by an individual located outside the torus in the vicinity of each discharge line.

5. The Valve Position Indication System shall be functionally tested once every three months and calibrated once per operating cycle. Due to the inaccessability of the pressure switches (in the drywell), the functional test shall consist of a simulated signal into the monitoring channel rather than the instrument.

6. The valve discharge temperature monitor shall be calibrated at least once per operating cycle.

F. Structural Integrity

Inservice Inspection and Testing of primary system boundary components shall be performed as specified in Surveillance Requirement 4.13.

E. Safety and Relief Valves

The safety/relief valves have two functions: i.e., power relief and safety. The power relief function is the automatic pressure relief (APR) mode. Power relief actuation is initiated by high drywell pressure coincident with low-low water level. This function is discussed in the Bases for Specification 3.5.D. The safety function is to limit system pressure to less than 110% of the design pressure. The safety function is initiated when steamline pressure increases to the valves's setpoint. There are two methods to ensure the valves open at the appropriate pressure: high pressure actuation via a pilot valve (mechanical lift) and pressure sensor actuation that will open the pilot valve via a solenoid actuator (electrical lift). The mechanical and electric lift functions are necessary to support OPERABILITY of the SRV safety function.

The electrical lift function is a backup, and does not replace the mechanical actuation on high pressure. The electrical lift feature employs two separate systems. The logic is configured in a two-out-of-two-taken-once format in each system. Each system is powered from a separate power source. One system is powered by VAC and the other by IAC. Since the IAC is interruptible upon loss of normal power, 125V DC battery backup power is provided. Upon loss of IAC, power supply to the logic will automatically switch to the battery backup to maintain an uninterruptible supply. Continuity of DC power supply to the SRV pilot solenoid is ensured by use of power-seeking relays in the circuitry.

During reactor power operation, the mechanical lift function cannot be verified, therefore, no in service surveillances are specified. For the electrical lift, an INSTRUMENT CHECK will detect any significant drift in the analog sensor input. This check is performed daily.

At the end of each cycle (during the refueling outage) verification that both the mechanical lift and the electrical lift would function is performed. For the mechanical lift, the as-found lift point is determined by bench testing. Confirmation is made that at least five of the six valves would open within ±3 %. Experience with the safety/relief valves indicates that testing of all safety valves each refueling outage is appropriate to detect failure or deterioration until more experience is gained. A tolerance of 1 % in the lift setpoint is specified for all valves at restart from a refueling outage. This ensures all valves have been adjusted to the optimal conditions at the beginning of each cycle. For electrical lift, verification that the system would function is accomplished by performing a SIMULATED AUTOMATIC ACTUATION and an INSTRUMENT CALIBRATION.

The simulated automatic actuation test demonstrates the operability of the required trip logic. The refuel frequency is based upon the increased potential for an unplanned transient if the surveillance were performed with the reactor at power, and operating experience with similar equipment already in use at the plant.

The instrument calibration ensures that each channel is set consistent with the measurement and setpoint error historical determinations. The refuel frequency is supported by a 30 month interval (24 month + 25%)used for the determination of the magnitude of equipment drift in the setpoint analysis.

When the setpoint is being bench checked, it is prudent to disassemble one of the safety/relief valves to examine for crud buildup, bending of certain actuator members or other signs of possible deterioration.

A manual actuation of each SRV is performed to verify the valve and solenoid are functioning properly and no blockage exists in the SRV discharge lines. It has been demonstrated that the blowdown of an SRV to the torus causes a wave action that is detectable on the torus water level instrumentation. The discharge of a relief line is audible to an individual located outside the torus in the vicinity of the line, as experienced at other BWRs.

Adequate reactor steam dome pressure must be available to perform this test to avoid damaging the valve. This test is performed no more than 24 hours after the MODE switch being placed in the RUN position. This requirement, which is sufficient to allow testing at high enough pressure while limiting reactor power to less than 25 percent power, ensures that the remaining SRVs are adequate to handle any transient in the unlikely event that one SRV discharge line is found blocked. Reactor start-up is allowed prior to performing this test because valve operability and the set points for overpressure protection are verified, per ASME requirements, prior to valve installation.

It is understood that portions of the Valve Position Indication System cannot be repaired or replaced during operation, therefore, the plant must be shutdown to accomplish such repairs. The 30-day period to do this allows the operator the flexibility to choose his time for shutdown; meanwhile, because of the redundancy provided by the valve discharge temperature monitor and the continued monitoring of the remaining valves by both methods, the ability to detect the opening of a safety/relief valve would not be compromised. The valve operability is not affected by failure of the Valve Position Indication System.

Docket No. 50-245
B15692

Attachment 5

Millstone Nuclear Power Station, Unit No. 1

Proposed Technical Specifications Revision
Safety Relief Valves

Design Change Safety Evaluation
(Provided for Information Only)

July 1996

INTEGRATED SAFETY EVALUATION NUMBER: MP1-95-060 REVISION 4

PLANT CHANGE NUMBER: **PDCR 1-34-95** REVISION: 0

PLANT CHANGE TITLE: **Main Steam Safety Relief Valve Electric Lift**

INFORMATION ONLY

1. *Summary Information*

1.1 *Safety Evaluation Conclusions*

The Design Change (Ref. 1) installs two independent circuits to provide Safety Relief Valve(SRV) Electric Lift actuation. Each circuit logic is configured in a two out of two taken once format. This configuration was selected to ensure an inadvertent signal in any one sensor loop of a circuit will not cause an inadvertent SRV lift. Components utilized in implementing this Design Change are all classified QA Category 1E safety related. This design is consistent with the GE recommended trip logic (Ref.2) which the NRC has reviewed and accepted. Therefore, the proposed Design Change is not an Unreviewed Safety Question and is safe to implement.

1.2 *Description of the Change*

The design utilizes a combination of new and existing Reactor Pressure Vessel (RPV) pressure transmitters configured to provide two independent circuits, S1 and S2. Each circuit is processed within the Post Accident Monitoring (PAM) cabinets, PAM103 and PAM104, in a two out of two taken once format. Each train of SRV electric lift actuation logic utilizes a new and an existing transmitter. This configuration was selected to ensure that no single transmitter failure, either high or low, will result in an inadvertent SRV lift. The existing transmitters are wide-range devices; the new transmitters are narrow-range devices. This diversity within the pressure sensing portion of the logic minimizes any common mode failure potential.

Once an overpressure condition is sensed, the logic will cause the Main Steam SRV pilot solenoid operated valves to open. The pilot solenoid repositioning will port nitrogen to the pilot stage assembly thus enabling the SRV pilot assembly to nitrogen assist opening of the main disc of the SRV. Upon decrease of Reactor Vessel Pressure below the setpoint, the logic will remove the open signal and the SRV pilot solenoid will be de-energized and reposition. This removes the nitrogen from the pilot assembly of the SRV and will reset against spring/steam pressure as currently designed. Bypass switches will be provided to allow operators to bypass either train of SRV electric lift circuitry either for maintenance or in response to specific system annunciators.

PAM 103 is currently supplied by Vital AC, which is uninterruptible upon loss of power. PAM 104 is supplied by Instrument AC, which is not uninterruptible upon loss of power. Therefore, a new power supply was installed in the PAM 104 with 125VDC battery backup capabilities. Upon loss of Instrument AC, the PAM 104 power supply will automatically switch to battery backup to maintain an uninterruptible system.

INFORMATION ONLY

This design is consistent with the design recommended by GE (Ref.2). The NRC has reviewed the GE design and found it to be acceptable (Ref.7). Specifically, Reference 2 states the following design requirements:

The design shall not degrade the ability of the SRVs to open in the safety mode of valve operation.

The design shall not significantly increase the probability of inadvertent SRV actuation or SRV sticking open due to a malfunction in the logic added.

The design modification shall satisfy separation and single failure criteria applicable to Millstone Unit One.

No single failure in a component or logic should disable the relief function of more than one SRV.

The electric power for operating the solenoid actuated pilot valves shall remain available following a loss of normal power (LNP).

The relief mode opening setpoints shall be between 1070 and 1250 psig.

The relief mode closing setpoints shall be at an appropriate setpoint value below the opening setpoint.

All components used to implement the modification shall be safety related and seismic.

The modification shall be considered a backup to SRV spring actuation.

The design implemented at Millstone Unit One meets these requirements. The setpoints for the electric lift logic are the same as the mechanical (spring-actuated) setpoints. Because the electric lift logic experiences a time delay from sensor response and signal processing, it is only a backup to mechanical actuation. Two out of two taken once logic ensures the system can still function given any single active or passive failure in electric lift equipment or logic. Both trains of electric lift logic are available following an LNP, and all equipment added in the design is safety related and seismic.

The GE proposed design does not specify the kind of equipment to be used. The design used at Millstone Unit One is based on Foxboro SPEC 200 Microprocessor control cards. These control cards have been previously utilized for safety-related applications at all three Millstone Units and at Connecticut Yankee. The application at Connecticut Yankee (Replacement of the Reactor Protection System) has been reviewed, audited, and found acceptable by the NRC. The design for electric lift at Millstone Unit One is enveloped by the scope of the Connecticut Yankee design.

1.3 *Aspects of the Change Evaluated*

This safety evaluation addresses the installation and operation of the Main Steam SRV Electric Lift logic including inadvertent actuation potential and component failures. This safety evaluation also addresses the effects of the design change in the Automatic Pressure Relief (APR) system.

1.4 *Malfunctions Evaluated*

This safety evaluation will consider the following malfunctions:

- Failure of a pressure transmitter
- Failure of a microprocessor control card
- Short circuit in the logic scheme
- Inadvertent energizing of a single relay
- Inadvertent lift of one or more SRVs due to Radio Frequency Interference (RFI)

1.5 *References*

1) PDCR 1-034-95, "Main Steam Safety Relief Valve Electric Lift"

2) GE/BWROG OG94-415-11, dated 8/23/95, NEDC-32121P, "Pressure Switch/Transmitter for Two Stage Target Rock Safety/Relief Valve"

3) Uncertainty Calculation; 95-ENG-1281E1 Rev. 1, "Millstone Unit 1 - Main Steam Safety Relief Valve Electric Lift Loop Uncertainties for Reactor Pressure Transmitters PT-263-114, PT-263-115, PT-287-112, and PT-287-113"

4) Setpoint Calculation; 95-ENG-1335E1 Rev.0, "Millstone Unit 1 - Main Steam Safety Relief Valve Electric Lift

5)EPRI TR-102348 "Guideline on Licensing Digital Upgrades"

6)CHAR services Report CSR026B "Evaluation of Electromagnetic Compatibility of the Connecticut Yankee Digital Feedwater Control System"

7)Letter from Bruce A. Boger (Director Division of Reactor Controls and Human Factors) to R.A. Pinelli (Chairman Boiling Water Reactor Owners Group) dated October 24, 1995, "Safety Evaluation Report for General Electric Topical Report NEDC-32121P".

8)GE Report # GE-NE-B13-01805-43, All S/RV's Open at High Power Event for MP1, May 1996.

2. *Unreviewed Safety Question Determination*

2.1 *Impact on Previously Evaluated Accidents*

This Design Change addresses the installation of the Main Steam Safety Relief Valve Electric Lift circuitry. The main purpose of the SRVs, to provide overpressure protection of the Reactor Pressure vessel, does not change under this design modification. However, the new logic and associated circuitry requires evaluating any potential increase in an inadvertent safety/relief valve opening.

INFORMATION ONLY

2.1.1 *List of Accidents Evaluated*

- Inadvertent SRV opening is evaluated under this safety evaluation.
- MSIV closure with flux scram and other overpressure transients.
- Stuck open Relief Valve.

2.1.2 *Effect on the probability of Occurrence of Previously Evaluated Accidents (A.4.1)*

Reference 2 documents a reliability analysis of an Inadvertent Opening of a Relief Valve (IORV). A malfunction in the lift logic could inadvertently open an SRV. The likelihood of such an occurrence is minimized by the redundancy of the electric lift logic design. GE, based on generic analysis, has calculated an increase in the likelihood of an IORV as less than 2.3 times. This evaluation has been reviewed by the NRC and found to be acceptable (Ref.7). Although not quantified, it is concluded that this increase in the likelihood of an IORV bounds the Millstone Unit One design. The probability classification assumed for the IORV in the licensing basis is infrequent i.e. the event can occur occasionally during the life of a particular plant, spanning once in 20 years to once in 100 years. Even though new analytical methodologies can calculate an increase in the probability by a factor of 2.3, the event can still be classified as an infrequent event. Thus it can be concluded that the design change does not alter the original licensing basis classification of the IORV.

Reference 2 concludes that addition of the electric lift logic has no impact on the likelihood of a Stuck Open Relief Valve (SORV). The basis for this conclusion is that the dominant reason for a SORV is a malfunction of the existing electrical circuitry interfacing with a safety relief valve. The redundancy of the lift logic design (two out of two, taken once) and utilization of a pulse type "turn on to trip" actuation signal minimizes the likelihood that the new logic would fail to "turn off" and cause a SORV. It is therefore concluded that an increase in the probability of occurrence of a SORV due to the design change is negligible. Moreover, the benefits of the design change in assuring timely actuation of the SRVs in overpressure transients far outweigh any negative effects associated with the impact on the probability of occurrence of a SORV.

Failure of both pressure transmitters in the same logic train would open all 6 SRVs if the failure was to the high limit of the transmitters. To eliminate the likelihood of such an event, the logic utilizes diverse Rosemount and Gould-Stathem instruments. Neither transmitter fails high on a loss of power. Sensor calibration range diversity gives different signal levels for the circuits to trip. This design attribute minimizes the likelihood that a random noise transient from outside the cabinet will simultaneously satisfy trip logic for both inputs of a train. As detailed in section 2.2.2, no common mode failure exists by which a single active or passive failure of hardware or software could cause multiple SRVs to open.

SRV Electric Lift bypass switches are installed on the benchboard of CRP 903. In accordance with approved plant procedures, the switches give operators the ability to respond to specific system annunciators by bypassing the control logic for either circuit. With a switch in bypass the electric lift signals for the associated circuit will not actuate that circuit's

trip relays. This ensures that operators have control during Off Normal and Surveillance type procedures. The bypass switches do not affect SRV mechanical lift setpoints. The bypass switches will not isolate either Automatic Pressure Relief or Remote Manual actuation of the SRV pilot solenoid circuits. Those circuits remain operational with the SRV electric lift logic bypassed. Front-panel annunciation is provided whenever a circuit of SRV electric lift logic is in bypass, to ensure that a switch is not inadvertently left in bypass after completion of corrective maintenance or channel surveillances. The bypass switches minimize the probability of an inadvertent SRV lift during surveillance testing of the SRV Electric Lift logic.

The proposed design change has no effect on the frequency of MSIV closure or other overpressure transients.

2.1.3 *Effect on the Probability of Occurrence of a Previously Evaluated Malfunction of Equipment Important to Safety (A.4.2)*

The proposed modification utilizes a combination of new and existing transmitters. This necessitates a review of failures that may impact the operation of the current use of the transmitter and the new electric lift logic simultaneously.

Existing Rosemount transmitters provide post-accident wide range accident monitoring and RPV level correction input. The transmitters can potentially fail as-is, fail high, or fail low. The proposed logic of the SRV electric lift is two out of two taken once. The single failure (high) of a transmitter will not inadvertently open an SRV. The dual purpose of the existing Wide Range transmitters would not be adversely impacted by failure. Additionally, failure of a transmitter either low or high would be front-panel annunciated. Therefore, failure of an existing transmitter does not increase the probability of occurrence of a previously evaluated malfunction of equipment important to safety.

The new Gould-Stathem transmitters are strain gauge type sensors which sense RPV narrow range pressure. A failure of a single transmitter will cause the loss of only one train in the electric lift logic and will not cause inadvertent SRV lift. Like the existing transmitters, failure of a new transmitter either low or high is front-panel annunciated. Both wide range and narrow range transmitters are located on environmentally enclosed instrument racks on the 42'-6" elevation of the Reactor Building. Control Rod Drive (CRD) injection flow is provided in instrument racks located on both the 14'-6" elevation and the 42'-6" elevation of the Reactor Building. The sensing lines for both the existing and the new transmitters do not share any connections with CRD injection flow to reference leg fill for reactor vessel level indication. Therefore, a malfunction in the CRD Injection system cannot create a high pressure condition to the SRV electric lift logic sensors that could cause an inadvertent lift of SRVs. The diversity of sensors, taken together with the system configuration in a two train, two out of two taken once scheme, causes no increase in the probability of occurrence of a malfunction previously evaluated.

Other functions of the SRVs, including Safety Relief, Automatic Pressure Relief, and Manual Actuation, remain unaffected by the proposed change. The pressure at which the SRVs

reseat remains unaffected since the electric lift signal is removed when the sensed Reactor Vessel pressure drops more than 0.5% below the lift setpoint: nominal reseat pressure of SRVs is 3-11% below the lift setpoint. No other equipment is affected by this proposed design change.

2.1.4 *Effect on the Consequences of the Previously Evaluated Accidents (A.4.3)* The most limiting transient for the overpressure condition is the MSIV closure with a high flux scram. This transient is reanalyzed every fuel cycle to confirm acceptability of results. The addition of SRV electric lift logic as described in this design change increases the reliability of SRV response within the limits of accident analysis assumptions.

The design change will not degrade the performance of safety systems or prevent actions assumed in the accident analysis, does not alter any of the assumptions made in the analyses, and does not degrade any fission product boundaries. Therefore, there is no effect on the consequences of previously evaluated accidents

2.1.5 *Effect on* the *Consequences of a Previously Evaluated Malfunction of Equipment (A.4.4)*

The proposed modifications as described, will pose no adverse effect on the consequences of a previously evaluated malfunction of equipment important to safety as stated in Section 2.1.3.

2.2 *Potential for a New Unanalyzed Accident*

2.2.1 *Possibility of an Accident of a Different Type Than Previously Evaluated (A.4.5)*

The design uses new Gould-Stathem transmitters rather than existing Gould transmitters which interface with Feedwater control, thus eliminating the possibility of a loss of Feedwater control driving an inadvertent SRV Electric Lift. Additionally, as discussed in Sections 2.1.2, 2.1.3, and 2.2.2 the design change precludes the possibility of inadvertent actuation of the Electric Lift circuitry due to single failures or common mode failures. Notwithstanding the arguments provided in these sections to show that simultaneous lift of all 6 SRVs is not credible, an analysis was performed to evaluate the impact of such an event(Ref 8). The results show that the consequences of simultaneous lift of 6 SRVs remain bounded by chapter 15 events. The transient is fairly mild. The maximum heat flux calculated is just over 101 %. There is no critical heat flux concern from such a small increase in the heat flux. No scram is predicted. The four highest set point SRVs re-close within a couple seconds as the reactor pressure drops below their reseat pressure. The remaining two SRVs may continue to discharge steam to the torus until a corrective action is taken by the operator.

2.2.2 *Possibility of a Malfunction of a Different Type Than Previously Evaluated (A.4.6)*

The design utilizes digital controls to sense an overpressure condition and provide contact closure logic to energize SRV pilot solenoids through trip relays. The logic for each trip circuit requires two separate microprocessor control cards to energize two separate trip relays

before the affected SRV pilot solenoid is energized. Use of this two out of two taken once logic with normally deenergized trip relays minimizes the probability of inadvertent SRV actuation from either loss of power or a single control card malfunction. Inadvertent energizing or bumping of a de-energized relay in CRP 932 could cause that relay to change state. As discussed above, energizing of a single relay will not cause inadvertent SRV actuation. Front panel annunciation indicates to operators that a single relay is in the trip condition. This ensures that system corrective maintenance or surveillance activities do not leave trip relays in a trip condition for extended periods of time.

The microprocessor control cards and their programming were procured and installed to conform with industry guidelines for development and implementation of quality-related software applications (Ref.5). Each control card is programmed to compare sensed RPV pressure to internal setpoint values corresponding to the mechanical lift points of the SRVs. The accuracy of these electronic setpoints is greater than the accuracy of the SRV mechanical lift points. Control card programming for this application was subjected to verification and validation at the vendors facility through Factory Acceptance Testing. Benchtesting at Millstone Unit One prior to field installation ensured that program integrity was maintained. Integrated system testing after field installation confirmed that the programming developed by Foxboro does not create unintended interactions with interfacing systems. The Foxboro Spec 200 Micro software and hardware used at Millstone Unit One for this application has successfully passed V&V audits for quality related software applications at Connecticut Yankee and at the Donald Cook Generating Station.

Each train of SRV Electric Lift circuitry has Wide Range and Narrow Range RPV pressure inputs with trip points stored in separate microprocessor control cards. The contact outputs of each control card are wired to separate analog buffer cards which actuate trip relays. Both Wide Range and Narrow Range control card trip logic for a train must be satisfied to initiate an SRV lift. This interface configuration ensures that failure of one control card either low or high does not cause inadvertent SRV actuation. Following vendor recommendations, power distribution modules in the PAM cabinets have been upgraded for the higher loading from the new microprocessor control cards. The new microprocessor control cards are installed in different nests within the PAM cabinets to minimize any voltage excursion effects on the programming logic and further minimize the potential for an inadvertent SRV actuation as a result of a single active device failure. This distribution of control cards within the PAM cabinets also minimizes the probability that any single point source of EMI could spuriously satisfy trip logic in more than one card.

Industry reports and in-house experience with Spec 200 Micro reliability indicate that failure of the microprocessor control cards is an extremely uncommon occurrence. The failures that have occurred have been passive in nature, i.e. failure to actuate when trip logic is satisfied. Failure of an individual card would be detected by failure to satisfy diagnostics. This control card failure mode is front panel annunciated, minimizing the probability that a control card failure would remain undetected for an extended period of time. Each control card performs its own diagnostics, to prevent a single card failure from propagating beyond the individual card . As a result, failure of a single control card will neither cause inadvertent SRV electric lift nor degrade safety related functions of adjacent analog Spec 200 circuit cards. Successful

completion of SRV electric lift logic would not be blocked by random failure of a single control card, since the other train would still function as designed.

The interface of control card outputs to control relays may introduce EMI effects to previously unaffected circuits. Efforts to minimize inadvertent introduction of EMI effects in this design include use of arc-suppression diodes on control relay coils, integral economizer contacts on the relay coils, separate routing and termination of control and instrumentation cables, comprehensive and consistent grounding of instrumentation cables, use of twisted signal leads within the PAM cabinets, and minimized lengths of unshielded cables within the PAM cabinets. The micro-control cards themselves utilize solid-state technology for contact closure functions, and as such do not create EMI when the card logic changes state. Integrated system testing has confirmed that no EMI effects were introduced to other circuits by installation of the SRV Electric Lift circuitry.

The extensive efforts to minimize introduction of EMI/RFI by the SRV Electric Lift circuit design also serve to minimize the possibility of an RFI-initiated disturbance of the SRV Electric Lift circuitry. The noise rejection efforts expended in this design change are consistent with Foxboro application recommendations and input from consultants who performed EMI testing on Spec 200 Micro circuitry at Connecticut Yankee in 1993 (Ref. 6). To validate the effectiveness of these noise rejection efforts for the SRV Electric Lift circuitry, comprehensive in-situ testing was performed. This testing involved deliberate actuation of various portable radio transmitters in close proximity to SRV Electric Lift Pressure Transmitters and Spec 200 micro circuit cards. The testing confirmed that no common mode susceptibility exists by which random portable radio transmitter use at the Millstone Station could initiate a spurious actuation of the SRV Electric Lift circuitry.

From the discussion above, there is no possibility that a malfunction of a different type than previously evaluated has been created by the proposed design change.

2.3 *Impact on the Margin of Safety*

The margin of safety previously analyzed for the SRVs was based on the current nominal setpoints and percentage of drift from these setpoints. This design modification improves the reliability of the SRVs to lift at the nominal setpoints. The setpoint uncertainty of the SRV electric lift circuitry has been calculated to be less than the Technical Specification uncertainty of the SRVs. Additionally the response time of the proposed circuit changes is such that RPV pressure peaks will not exceed values stated in the Safety Analysis for any analyzed accidents in the event that individual SRVs should experience sticking. The existing functions of the SRVs (safety, manual, or automatic lift) remain unaffected by the proposed design change. The design of the analog pressure transmitters, combined with the logic configuration, minimizes the possibility of inadvertent opening of the SRVs.

Therefore, there is no adverse impact on the margin of safety in implementing this design modification.

3. *Safety Determination*

3.1 *Qualitative Safety Determination*

The proposed Design Change does not increase public risk. The Design Change as identified in PDCR 1-034-95 does not adversely impact safety related or non-safety related systems. Based on this evaluation, the change is considered safe and not an Unreviewed safety question.

3.2 *Detailed Safety Determination (If ISE and Change is an USQ)*

N/A - The proposed modification has been evaluated and determined NOT to be an USQ.

3.2.1 *Effect on the Probability of Initiation of an Accident (A.5.1)*

N/A - The proposed modification has been evaluated and determined NOT to be an USQ.

3.2.2 *Effect on the Probability that Operators Will Fail to Mitigate an Accident (A.5.2)*

N/A - The proposed modification has been evaluated and determined NOT to be an USQ.

3.2.3 *Effect on the Probability that Mitigating Equipment Will Fail (A.5.3)*

N/A - The proposed modification has been evaluated and determined NOT to be an USQ.

3.2.4 *Effect on the Consequences of an Accident (A.5.4)*

N/A - The proposed modification has been evaluated and determined NOT to be an USQ.

ISE# MP1-95-060
Rev 4

4. *Approval*

Prepared By: Donald V. Clemons Jr Date: 23 May 96
Donald V. Clemons
MP1 Electrical Design Engineering

Nirmal Jain Date: 5/23/96
Nirmal Jain
Safety Analysis Branch

Approved By: Gilbert M. Olsen Date: 5/23/96
Gilbert M. Olsen
Supervisor, MP1 Electrical Design Engineering

Bruce E. Beuchel Date: 5/23/96
Bruce E. Beuchel
Manager, MP1 Design Engineering

M S Kai Date: 5/23/96
Michael S. Kai
Supervisor, Safety Analysis Branch

M S Kai for D. A. Dube Date: 5/23/96
Donald A Dube
Manager, Safety Analysis Branch

INFORMATION ONLY

Docket No. 50-245
B15692

Attachment 6

Millstone Nuclear Power Station, Unit No. 1

Proposed Technical Specifications Revision
Safety Relief Valves

Description of Electric Lift Design Change

July 1996

Millstone Nuclear Power Station, Unit No. 1
Proposed Technical Specifications Revision
Safety Relief Valves
Description of Electric Lift Design Change

The Main Steam Safety Relief Valve Electric Lift control logic provides backup (diversified) means to energize the pilot solenoids and open the Main Steam Safety Relief Valves (SRVs). The installation is consistent with the recommendations of BWROG/GE evaluation NEDC-32121P, Revision 1 (August 1995) and serves to mitigate the effects of SRV mechanical setpoint drift during power operation.

The Main Steam SRV Electric Lift control logic consists of two independent trains of instrumentation, either of which may initiate protective action by energizing SRV pilot solenoids. Each train consists of two separate logic subchannels. Both subchannels of a train must trip from a trip condition to initiate protective action, making the system logic "two out of two taken once". The trip setpoints for the SRV Electric Lift control logic are the same as the mechanical lift setpoints for the individual SRVs. Refer to Figure 1.

Each train of SRV Electric Lift consists of a wide range and a narrow range subchannel. In each subchannel, a Reactor Vessel Pressure sensor inputs to a microprocessor. The microprocessor compares Reactor Vessel Pressure to internal trip setpoints, and generates a trip when Reactor Vessel Pressure exceeds the trip setpoint. The logic from a microprocessor causes a trip relay to energize when a trip setpoint is exceeded. Both wide range and narrow range subchannels of a train must trip before protective action is initiated.

The protective action of the SRV Electric Lift control logic energizes SRV pilot solenoids which supply nitrogen to the air-actuated primary pilot control valves. This in turn actuates the second stage control valve that opens the main relief valve. Steam escapes from the main steam line through the valve and into the torus to relieve pressure. The Electric Lift control logic is considered a backup to the mechanical lift of the SRVs in an overpressure condition. As such, the actuation signal is not sealed in. Once the control logic actuates the pilot solenoids, the SRVs are shut by mechanical blowdown of pressure, independent of the circuitry. Backup power is available for the SRV pilot solenoids from power monitor relays.

Alarms, annunciation, and recording are provided within the Control Room.

Integrated testing on a train basis (to include energizing trip relays) may be performed during plant shutdowns, when power leads to the SRV pilot solenoids are lifted to support interfacing system testing, such as for the APR system. Partial train testing during power operation may be accomplished by use of the Maintenance Bypass switches. When these switches are in bypass, 125 VDC power to the trip relays is blocked. During either subchannel or train testing at power, the train not under test is able to initiate protective action if needed.

FIGURE 1

SRV ELECTRIC LIFT

ACTUATION TRAIN LOGIC