NRC FORM 366 (4-95) U.S. NUCLEAR REGULATORY COMMISSION

APPROVED BY OMB NO. 3150-0104
EXPIRES 04/30/98
ESTIMATED BURDEN PER RESPONSE TO COMPLY WITH THIS MANDATORY INFORMATION COLLECTION REQUEST [illegible] HRS. REPORTED LESSONS LEARNED ARE INCORPORATED INTO T[illegible]SING PROCESS AND FED BACK TO INDUSTRY. FORWARD [illegible] REGARDING BURDEN ESTIMATE TO THE INFORMATION AND REC[illegible]NAGEMENT BRANCH (T-6 F33), U.S. NUCLEAR REGULATORY COM[illegible]ON, WASHINGTON, DC 20555-0001, AND TO THE PAPERWORK REDUCTION PROJECT (3150-0104), OFFICE OF MANAGEMENT AND BUDGET, WASHINGTON, DC 20503.

LICENSEE EVENT REPORT (LER)

(See reverse for required number of digits/characters for each block)

FACILITY NAME (1)	DOCKET NUMBER (2)	PAGE (3)
Millstone Nuclear Power Station Unit 1	05000245	1 of 5

TITLE (4)

Reactor Pressure Vessel High Level Trip System Single Failure Vulnerability

EVENT DATE (5)			LER NUMBER (6)			REPORT DATE (7)			OTHER FACILITIES INVOLVED (8)	
MONTH	DAY	YEAR	YEAR	SEQUENTIAL NUMBER	REVISION	MONTH	DAY	YEAR	FACILITY NAME	DOCKET NUMBER
11	15	96	96	059	00	12	16	96	FACILITY NAME	DOCKET NUMBER

OPERATING MODE (9)	N	THIS REPORT IS SUBMITTED PURSUANT TO THE REQUIREMENTS OF 10 CFR §: (Check one or more) (11)			
POWER LEVEL (10)	000	20.2201(b)	20.2203(a)(2)(v)	50.73(a)(2)(i)	50.73(a)(2)(viii)
		20.2203(a)(1)	20.2203(a)(3)(i)	[X] 50.73(a)(2)(ii)	50.73(a)(2)(x)
		20.2203(a)(2)(i)	20.2203(a)(3)(ii)	50.73(a)(2)(iii)	73.71
		20.2203(a)(2)(ii)	20.2203(a)(4)	50.73(a)(2)(iv)	OTHER
		20.2203(a)(2)(iii)	50.36(c)(1)	50.73(a)(2)(v)	Specify in Abstract below or in NRC Form 366A
		20.2203(a)(2)(iv)	50.36(c)(2)	50.73(a)(2)(vii)	

LICENSEE CONTACT FOR THIS LER (12)

NAME	TELEPHONE NUMBER (include Area Code)
Robert W. Walpole, MP1 Nuclear Licensing Manager	(860)440-2191

COMPLETE ONE LINE FOR EACH COMPONENT FAILURE DESCRIBED IN THIS REPORT (13)

CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS		CAUSE	SYSTEM	COMPONENT	MANUFACTURER	REPORTABLE TO NPRDS

SUPPLEMENTAL REPORT EXPECTED (14)		EXPECTED SUBMISSION	MONTH	DAY	YEAR
[ ] YES (if yes, complete EXPECTED SUBMISSION DATE).	[X] NO				

ABSTRACT (Limit to 1400 spaces, i.e., approximately 15 single-spaced typewritten lines) (16)

On November 15, 1996, at 1700 hours, with the plant in the COLD SHUTDOWN condition, it was determined that the Reactor Pressure Vessel (RPV) High Level Trip System, which provides Reactor Feed Pump (RFP) trips on vessel high water level could be vulnerable to a single failure, rendering the entire system inoperable in the event of the failure of the Vital AC supply to the level transmitters. The RPV High Level Trip System consists of two redundant trip systems. Two Yarway level transmitters make up one trip system, and two Gould level transmitters make up the other trip system. The trip logic is designed as "one-out-of-two-taken-twice", and thus a signal input from at least one Yarway and at least one Gould level transmitter is required to enable the RFP to be tripped on High Vessel Level. Both Yarways are powered from Vital AC. A loss of Vital AC would make both Yarways inoperable, as well as the entire RPV High Level Trip System. The RPV High Vessel Level Trip system was designed and installed in 1982 with the intention that all redundant components meet the separation criteria of IEEE-279 and be capable of fulfilling their design function despite a single failure. The failure to meet separation and single failure criteria is a result of the implementation of design modifications that failed to delineate specific separation and single failure criteria. These criteria will be reevaluated for applicability to the RFP trip system and plant modifications will be implemented as necessary prior to startup for Cycle 16. There were no actual safety consequences as a result of this event.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)					PAGE (3)
		YEAR	SEQUENTIAL NUMBER			REVISION NUMBER	
Millstone Nuclear Power Station Unit 1	05000245	96	--	059	--	00	2 of 5

TEXT *(If more space is required, use additional copies of NRC Form 366A)* (17)

I. Description of Event

On November 15, 1996, at 1700 hours, with the plant in the COLD SHUTDOWN condition, maintenance was being performed on two of four Reactor Pressure Vessel (RPV) level indicators which provide input to the RPV High Level Trip System. A momentary short occurred, which blew a fuse in the circuit which supplies Vital AC power to the Yarway level indicators. This de-energized relays which provide power to both Yarway level indicators. While the RPV Hi Level Trip System was not required to be operable at the time, the event revealed a single failure vulnerability in the RPV High Level Trip System. The RPV High Level Trip System provides Reactor Feed Pump (RFP) trips on high vessel water level.

II. Cause of Event

The failure to identify and properly evaluate all single failure and separation issues relating to the design of the RFP Trip on High Vessel Level was a result of the failure to effectively implement the design control process. In conjunction with this failure, it is evident that the actual design requirements for the RPV High Level Trip System were neither understood nor properly documented in the design change documentation.

III. Analysis of Event

The RPV High Level Trip System was installed in 1982 to specifically address and resolve the issue of the potential for vessel overfill following plant trips. This system installed controls, cabling, and instrumentation to trip the Reactor Feed Pumps on High Reactor Vessel Level. Continued flow of feedwater after a plant trip could cause a vessel overfill condition that could in turn cause a water hammer in the piping to the isolation condenser or main steam lines.

The overfill protection system is based on a one-out-of-two-taken-twice logic to detect an RPV high water level condition. There are two trip systems, each with two instrument channels. One trip system consists of the Yarway level indicators (LITS 263-59A&B) and the other trip system consists of the Gould level transmitters (LT-646A&B). A high water level trip signal is required in at least one channel in each trip system (one Yarway and one Gould high level signal) to initiate a feedwater pump trip (see Figure 1). This one-out-of-two-taken-twice trip logic minimizes the likelihood of an inadvertent signal which would cause the feedwater pumps to trip, resulting in a loss of feedwater event. The Yarway level transmitters also provide level input signals to the Main Turbine trip system to trip the turbine on high vessel level. This turbine trip feature requires a high level sensed by both Yarways. The Gould level transmitters also provide level input signals to the Feedwater Control System, to control feedwater flow to maintain constant vessel level during normal plant operation.

In March 1990, it was noted in our response to Generic Letter 89-19, "Request For Action Related to Resolution of Unresolved Safety Issue A-47, 'Safety Implication of Control Systems in LWR Nuclear Power Plants' Pursuant to 10CFR50.54(f)", that the existing overfill protection system "provides adequate protection for Millstone 1 even though the overfill protection system lacks redundancy for the power source of the trip logic and the relays and controllers for the high level trip are not in separate cabinets". These issues, which primarily focused on a postulated Loss of Vital AC scenario, were evaluated per Integrated Safety Assessment Program (ISAP) Topic 1.43, "Water Hammer". Design and procedural modifications were made to specifically address the potential Loss of Vital AC scenario. In addition, ISAP Topic 1.43.1, "Reactor Vessel Overfill Protection" specifically evaluated changing the power supply from Vital AC to Instrument AC for two of the four vessel level transmitters which are part of the Feed Pump Trip Logic. However, this evaluation concluded that the overall benefit of implementing this modification was minimal. Therefore, no further evaluations nor plant modifications

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)			PAGE (3)
		YEAR	SEQUENTIAL NUMBER	REVISION NUMBER	
Millstone Nuclear Power Station Unit 1	05000245	96	-- 059 --	00	3 of 5

TEXT *(If more space is required, use additional copies of NRC Form 366A)* (17)

were made at that time. Recently, however, additional single failure vulnerabilities, including that of the fuse in the Vital AC power supply circuitry to the Yarways, have raised additional questions as to the reliability of the RPV High Level Trip System. It was also recently discovered that the design change documentation (which was used to install the overfill protection system in 1982) required separation and single failure criteria to be specifically addressed by the system design. The design change which added the vessel overfill protection system states that all redundant components meet the separation criteria of IEEE-279-1971 and are capable of fulfilling their design function despite a single failure, with the exception of the Feed Pump Trip Defeat Switch. The single failure of this defeat switch was evaluated in the design change documentation, but no other vulnerabilities were identified and evaluated at that time. It is apparent that the system was neither designed nor installed as a fully redundant single failure proof system that also meets standard separation criteria.

Since the design change documentation is considered to be the design basis of the RPV High Level Trip System, the single failure vulnerability identified in the Vital AC power supply circuitry was considered to be promptly reportable per 10CFR50.72(b)(1)(ii)(B) as an event or condition that is outside the design basis of the plant. This and other known separation and single failure vulnerabilities of the RPV High Level Trip System identified below are being reported per 10CFR50.73(a)(2)(ii)(B) as conditions that were outside the design basis of the plant.

The additional separation and single failure vulnerabilities of the RPV High Level Trip System are:

1. Inadequate isolation between the feedwater control system and the Gould Level Transmitter Feed Pump trip circuits, since both share the Gould level transmitter input signals.

2. A loss of Vital AC, which powers the level transmitters and feedwater controllers would also result in the loss of the entire RPV High Level Trip System, with a coincident lock-up of the Feed Regulating Valves.

3. A single fuse or control switch contact failure could also result in the loss of the entire RPV high Level Trip System.

4. The existing design of the RPV overfill protection system and feedwater control system includes protective trip relays and feedwater control instrumentation installed without sufficient separation to preclude a single failure and/or fire within the control room panel from affecting both feedwater control and the RPV overfill protection circuitry.

The occurrence of a single failure or an electrical fault has the potential to inadvertently make one or both of the trip systems inoperable. Without the Reactor Feed Pump trip on high RPV water level, a failure of the feedwater control system or a plant trip could result in an overfill condition that would need to be mitigated through operator action to secure the Reactor Feed Pumps. The RPV High Level Trip System was designed so as not to interfere with operation of the safety-related Feedwater Coolant Injection (FWCI) system. If a FWCI actuation signal is generated on low reactor level following a Feed Pump trip, the FWCI-selected Feed Pump will auto-start and will run until the high level trip setpoint is reached at which point it will trip again. If a FWCI actuation signal is generated on high drywell pressure following a Feed Pump trip, the FWCI-selected Feed Pump will not auto-start, thus preventing rapid cycling of the feed pump around the high level setpoint. Operator action is credited in this case to manually restart the feed pumps when the high level trip condition clears, or to defeat the high level trip function and manually restart the pumps. Both the bypass of the high drywell pressure FWCI function and defeat of the feed pump trip function is annunciated in the control room. Therefore, the inoperability of the RPV High Level Trip System would have no adverse affect on the operability of the FWCI system.

Due to the system interfaces between the vessel level indicators and the main turbine trip and feedwater control systems, the potential exists that failure of these level transmitters will adversely affect these systems. A loss of Vital AC to the Yarways due to a single failure would prevent the Main Turbine trip on a vessel high water level condition, as well as prevent the Feedwater Pump trip on vessel high water level. The design basis of the main turbine trip on high water level, which is designed for equipment protection only, does not require redundancy nor compliance with single failure requirements. However, with no overfill protection available, operator action would be required to recognize a loss of Yarway level indication to mitigate any potential overfill transient by manually tripping the Reactor Feed Pumps. A loss of Vital AC to the Gould due to a single failure would cause a "lock-up" condition of the Feedwater Regulating Valves, as well as prevent the Feedwater Pump trip on vessel high water level. Operator action would also be required to recognize a loss of Gould level indication to mitigate any potential overfill transient by manually tripping the Reactor Feed Pumps. To assist the operator in recognizing a loss of Vital AC, a "Loss of Vital AC" undervoltage alarm for the Vital AC bus was installed during the 1991 outage, procedural guidance to address the specific Loss of Vital AC scenario was implemented along with associated training and other vessel level indication improvements.

IV. Corrective Action

The design basis of the RFP High Level Trip Circuitry will be reevaluated to verify the proper applicability of the physical separation, redundancy and single failure requirements specified in the design change documentation. If it is determined that these design requirements are valid for this application, the RFP High Level Trip Circuitry will be modified to provide separate, redundant, and single failure proof vessel overfill protection. This reevaluation and any potential plant modifications associated with it will be completed prior to startup for Cycle 16. If it is determined that these design requirements are not valid for this application, a design change will document this.

The design control process and the design engineering organization has been strengthened since 1982, when the RPV High Level Trip system was installed. The design control improvements include a revised Design Control Manual. The current revision to the Design Control Manual became effective for Millstone Unit 1 on July 15, 1996.

A review of other systems to identify and resolve design basis discrepancies is ongoing as part of the design basis verification program to address 10 CFR 50.54(f) concerns. This will also include a review of all open issues that were previously being evaluated in the ISAP. The 10 CFR 50.54(f) review and recommendation implementation will be completed before startup for Cycle 16 as committed to in Commitment No. B16022-3.

V. Additional Information

Similar Events

There are no other similar events relating to the RPV High Level Trip System.

Manufacturer Data

None.

FACILITY NAME (1)	DOCKET NUMBER (2)	LER NUMBER (6)					PAGE (3)
		YEAR	SEQUENTIAL NUMBER			REVISION NUMBER	
Millstone Nuclear Power Station Unit 1	05000245	96	--	059	--	00	5 of 5

TEXT *(If more space is required, use additional copies of NRC Form 366A)* (17)

FIGURE 1
REACTOR HIGH WATER LEVEL
FEEDWATER PUMP TRIP