Docket No. 50-336
B14005

Attachment 2

Millstone Nuclear Power Station, Unit No. 2

Plant-Specific Analysis for the
Shutdown Cooling System
Autoclosure Interlock Deletion

January 1992

NUSCO 175

# SDC Auto-Closure Interlock Removal at Millstone Unit 2

Probabilistic Risk Assessment Section
Northeast Utilities Service Co.

December 1991

DISCLAIMER

The information contained in this topical report was prepared for the specific requirements of Northeast Utilities Service Company (NUSCO) and its affiliated companies, and may contain materials subject to privately owned rights. Any use of all or any portion of the information, analyses, methodology or data contained in this topical report by third parties shall be undertaken at such party's sole risk. NUSCO and its affiliated companies hereby disclaim any liability (including but not limited to tort, contract, statute, or course of dealing) or warranty (whether express or implied) for the accuracy, completeness, suitability for a particular purpose of merchantability of the information.

TABLE OF CONTENTS

## 1.0 INTRODUCTION

The purpose of this analysis is to investigate the risk impact of removing the auto closure interlock (ACI) from the shutdown cooling system (SDCS) suction valves 2-SI-651 and 2-SI-652 at Millstone Point Nuclear Power Station Unit 2 (MP2). In place of the ACI, an alarm will be provided in the control room. The alarm will cause the annunciator to light and sound a horn when either of the valves is not fully closed with the reactor coolant system (RCS) at high pressure.

Figure 1 is based on information provided in References 1 and 2. It is a simplified P&ID of SDC which illustrates components associated with this design change. The pressure transmitters PT103 and PT103-1 generate the high pressure signals that will close the isolation valves. Note that the valves are shown in their power operation (Mode 1) position.

The ACI is designed to minimize the likelihood of failing to close the SDC isolation valves during plant heat up. In addition, the ACI prevents the SDCS, whose design pressure is approximately 500 psi, from being overpressurized due to transients during shutdown. When the plant is shutdown and the SDCS is aligned to the RCS, the SDCS is subjected to the same pressure as the RCS. If a transient were to occur that increased RCS pressure, the pressure within the SDCS would also rise. As a result, the ACI would operate and close isolation valves 2-SI-651 and 2-SI-652. Given an adequate response time, the ACI will prevent the SDCS from exceeding its design pressure. It is this interlock function that is proposed to be replaced by an alarm.

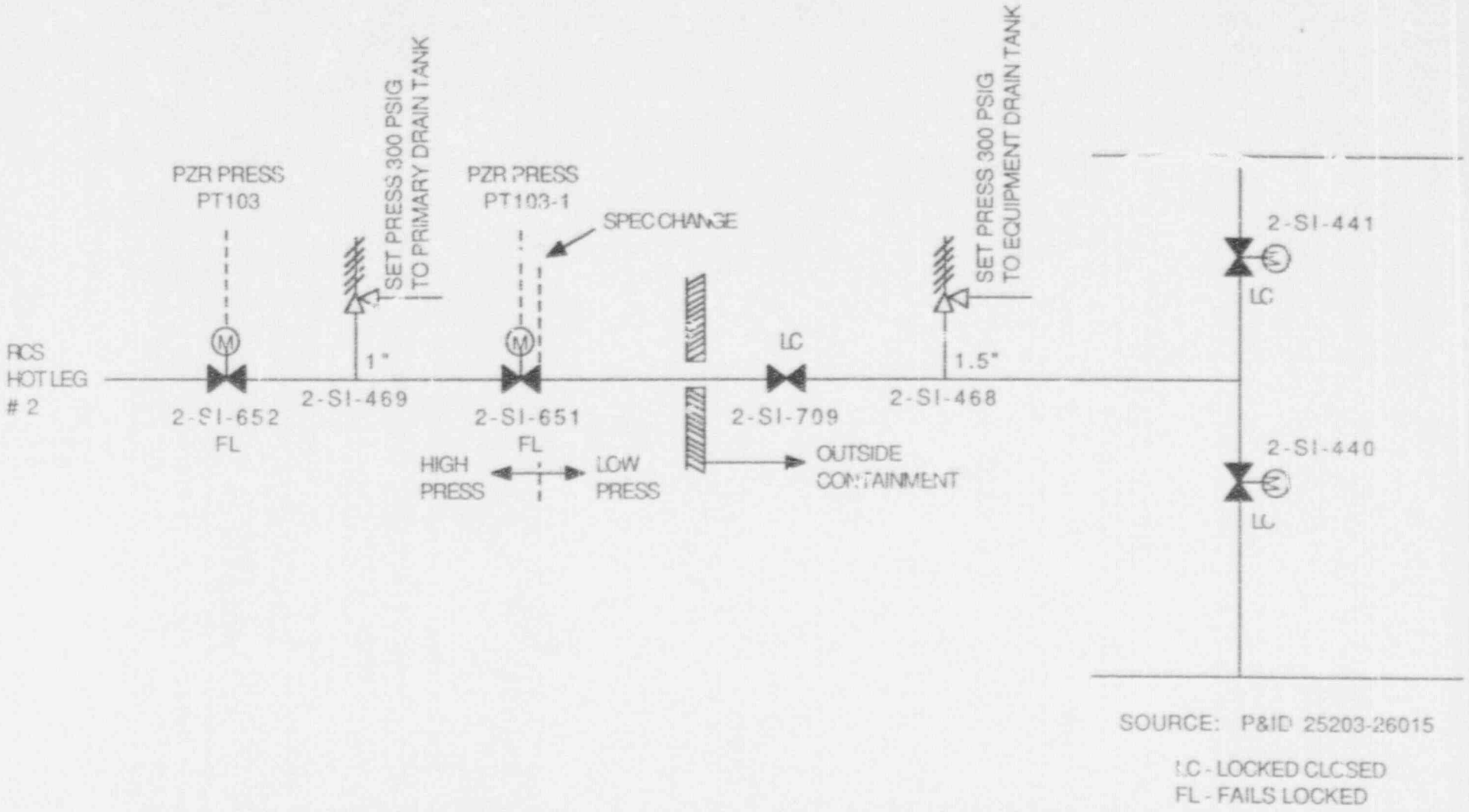


FIGURE 1 SIMPLIFIED P&ID OF SDC SUCTION PATH

## 2.0 BACKGROUND

Loss of SDC during shutdown operation has been a concern to the Regulators and the Industry for a considerable period of time. These events have continued to occur at a rate of several per year in spite of the increased attention given. (References 3 and 4.)

A major contributor to the loss of decay heat removal events has been the spurious actuation of ACI. The Electric Power Research Institute (EPRI) and the Nuclear Regulatory Commission (NRC) have analyzed loss of decay heat removal events at pressurized water reactors (References 5 and 6). The results reported indicate 130 loss of decay heat removal events for the period between 1976 and 1983.

Table 1 (extracted from Reference 6) summarizes these 130 events by the categories which cause loss of the decay heat removal function. Of the 130 events, 37 events have been caused by the automatic closure of the suction isolation valves. That is, 28.5 percent of the loss of decay heat removal events have been caused by the inadvertent actuation of the ACI.

Table 1*

Categories of Total DHR System Failures at U.S. PWRs, 1976-1983, When Required to Operate (Loss of Function)

| | | |
|---|---|---|
| Automatic Closure of Suction/ Isolation Valves | 37 | (28.5) |
| Loss of Inventory | | |
| • Inadequate RCS Inventory Resulting in Loss of DHR Pump Suction | 26 | (20.0) |
| • Loss of RCS Inventory Through DHR System Necessitating Shutdown of DHR System | 10 | (7.7) |
| Component Failures | | |
| • Shutdown or Failure of DHR Pump | 21 | (16.2) |
| • Inability to Open Suction/ Isolation Valve | 8 | (6.1) |
| • Others | 26 | (21.5) |
| TOTAL | 130 | (100.0) |

*This table has been extracted from Reference 6.

Removal of the ACI has several impacts on risk. As pointed out in the previous section, removal of the ACI benefits public safety (reduces public risk) by reducing the loss of decay heat removal events. However, sin the ACIs do participate in lowering the likelihood of interfacing system LOCAs (ISLOCAs) by automatically closing the SDC suction isolation valves during mode transition from mode 6 to mode 1, removal of the ACI may have a potentially negative benefit on the ISLOCA frequency. Finally, the plant response to overpressure transients during non-power operations will be affected due to this change. The analysis that follows investigates the impact of the ACI removal on SDC unavailability, ISLOCA potential, and low temperature overpressure (LTOP) transients.

## 3.0 SCOPE

NRC, in an internal memo (Reference 7) expressed seven concerns in stating the Reactor Systems Branch (RSB) position on requests for removal of the SDCS ACI. These seven concerns are:

1) The means available to minimize interfacing systems LOCA or event V concerns.

2) The alarms to alert the operator of an improperly positioned SDCS MOV.

3) The SDCS relief capacity must be adequate.

4) Means other than the ACI to ensure that both MOVs are closed.

5) Assurance that the function of the open permissive circuitry is not affected by the proposed change.

6) Assurance that MOV position indication will remain available in the control room regardless of the proposed change.

7) Assessment of the proposed change's effect on SDCS reliability, as well as on Low Temperature Overpressure (LTOP) concerns.

The PRA analysis will address items (1), (3), and (7). The investigations on other items will be limited in that other engineering disciplines will provide final assurances and verifications.

## 4.0 PRA ANALYSIS

### 4.1 Interfacing Systems LOCA (Event V) Analysis

The MP2 event V analysis was revisited to examine the impact of ACI removal on event V frequency. Only the Event V frequency through the SDC suction path can potentially be affected due to ACI removal.

Based on MP2 valve configuration provided in Figure 1, an event V through the SDC suction path is defined as alignment of RCS and SDC during plant operation due to the failure of valves 2-SI-651 and 2-SI-652. Since the relief valve 2-SI-469 plays a major role in the detection of a failed 2-SI-652 valve, that valve is also included in the Event V sequence analysis. The failure modes of suction isolation valves considered are:

- CATASTROPHIC RUPTURE
- LEFT OPEN BY THE OPERATOR
- SPURIOUS OPENING

Figure 2 provides an event tree showing different combinations of events that can lead to event V sequences. Not all sequences on Figure 2 are credible. A large number of sequences are extremely low in frequency so that they can be disregarded. The paragraphs that follow develops screening values for branch fractions and perform a screening type evaluation to simplify the event tree and compare the ISLOCA frequency through the SDC suction path with and without the ACI.

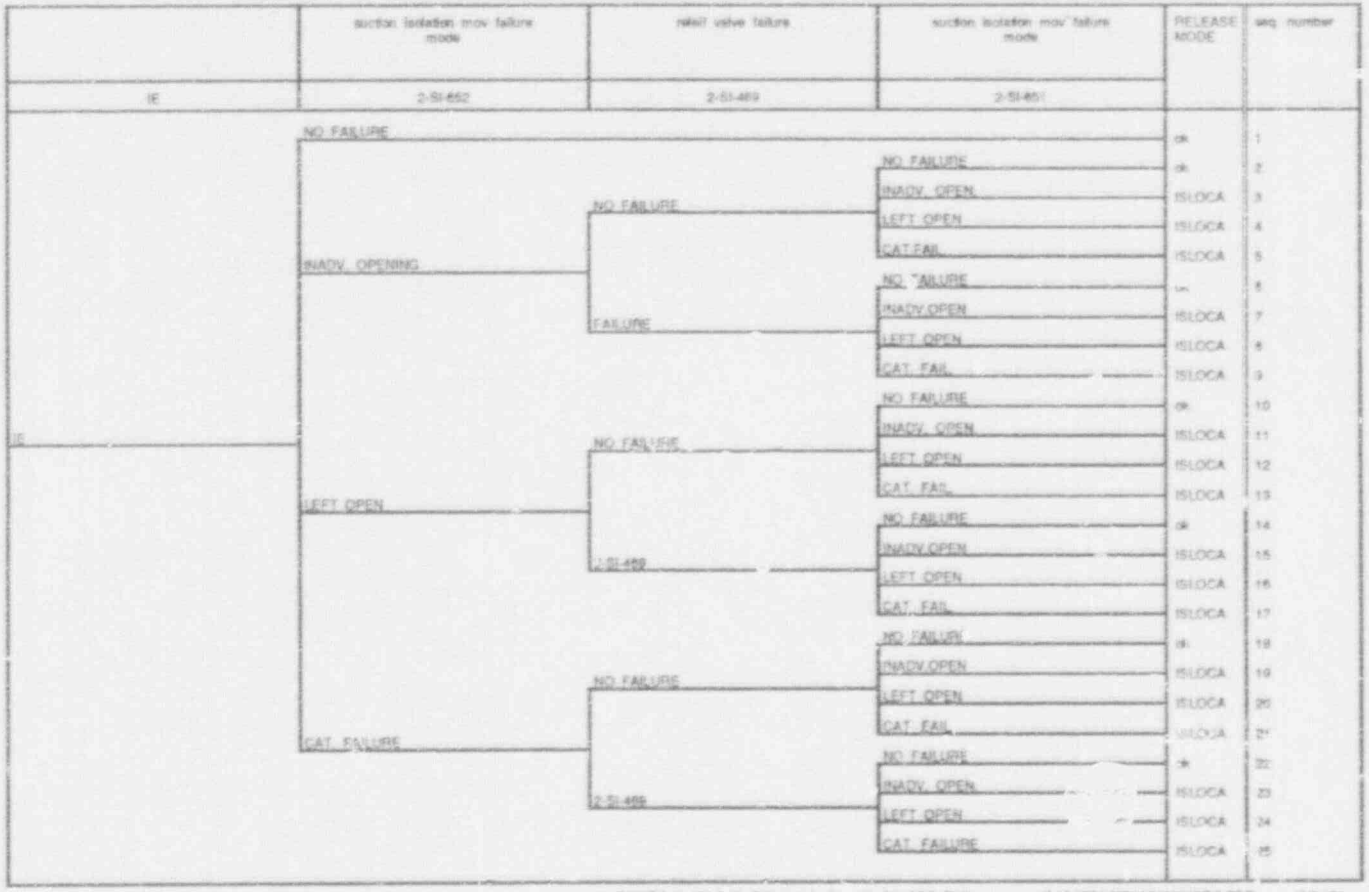


FIGURE 2: ISLOCA Sequences through the SDC Path C:\CAFTA\MP2ACTM\VSEQ.TRE 10/24/91

4.1.1 Inadvertent Opening of 2-SI-652

Several defenses exist against inadvertent opening of 2-SI-652. The unit operating procedure OP 2310 (Ref. 8 "Shutdown Cooling") instructs the operator to close the SDC inlet valves 2-SI-651 and 2-SI-652. These valves are key locked to shut. Further, the same procedure instructs disconnecting of a switch to remove power from the breaker to valve 2-SI-652.

The probability of failing to remove power from 2-SI-652 by the operator is assigned a value of $1.6 \times 10^{-3}$ based on analysis provided in WCAP-11736-A (Ref. 9). If the power is not removed from the MOV 2-SI-652, then an inadvertent opening can result from inadvertent closure of a contact pairs. Concurrent spurious closure of at least two contact pairs must occur for spurious closure. Assuming a $10^{-7}$/hour rate for spurious contact closure, Reference 10 estimates the annual frequency of 2-SI-652 spuriously opening to be approximately $8 \times 10^{-10}$ per year.

The other mechanism of inadvertent opening is the coincidence of the events "power not removed from valve 2-SI-652," "key locked hand switch turned to OPEN position (operator error)," and "Open prevent interlock spuriously closes." The frequency of this scenario is also extremely low.

Therefore, inadvertent opening of 2-SI-652 is not considered as a credible failure and that branch is eliminated from the event tree.

4.1.2 2-SI-652 Catastrophic Failure

Based on failure rate of $10^{-7}$/hour (Ref. 11) the frequency of catastrophic rupture of 2-SI-652 is estimated to be $8.76 \times 10^{-4}$ per year.

4.1.3 Frequency of 2-SI-652 "LEFT OPEN"

This sequence is considered insignificant due to a variety of reasons. They are as follows:

- OP 2310 (Ref. 8) instructs the operator to close isolation valves 2-SI-651 and 2-SI-652. This failure mode would require operator error of omission. The probability of that event is assumed to be $3.2 \times 10^{-3}$ following the assessment for MP3 RHR ACI removal (Ref. 9, WCAP-11736-A).

- Operator fails to perform Leak Rate Test "Containment Leak Test - Type C (LLRT)" (OPS Form 2605D-1) according to the operating procedure.

  Note that this leak rate test is applicable to 2-SI-651 only. It is not applicable to 2-SI-652. However, because of this test, a fully open 2-SI-652 would most likely be detected during the leak test of 2-SI-651.

- If the valve 2-SI-652 is open and the pressure is increased beyond the ACI setpoint, SDC will automatically isolate through the closing of 2-SI-652 and 2-SI-651. Even after the ACI deletion, the proposed alarm will let the operator know that 2-SI-652 or 2-SI-651 is open.

- Relief valve 2-SI-469 will open when pressure is increased beyond 300 psi while 2-SI-652 is open. Lifting of this relief valve should be known to Operations since the relief valve discharges to the primary drain tank which alarms on temperature, pressure and level. Further, the above normal RCS leak rate will eventually alert the operator of an unusual condition.

Considering the above, "2-SI-652 LEFT OPEN" path is not considered credible.

4.1.4 Relief Valve 2-SI-469

If for one reason or another 2-SI-652 fails, then the relief valve 2-SI-469 will be subjected to RCS pressure. The set point of this relief valve is 300 psi and its discharge gets routed to the primary drain tank (PDT). There are temperature, pressure, and level alarms associated with the Primary Drain Tank.

The mechanical failure of the passive relief valve to lift is relatively low. Alarm failure is also of low probability due to the diversity of alarms associated with PDT. The dominant failure mode of the relief valve as a defense against an ISLOCA will therefore be "Operator Failure to Recognize Lifted RV Based on PDT alarm." A screening value of $10^{-3}$ is assigned to this operator failure. This probability is justified considering other diverse means of detecting loss of inventory during plant startup. Such inventory imbalances warn the operator of an unusual condition and require the operator to suspend any increases in reactor power or RCS pressurization.

4.1.5 Inadvertent Opening of 2-SI-651

Since power is not removed from the 2-SI-651 as is the case for 2-SI-652, the probability of inadvertent opening of 2-SI-651 is relatively high compared to that of 2-SI-652.

Several mechanisms that can lead to the inadvertent opening of the valve are as follows:

- All three motor start relay contacts (42-O) short. The probability of such an event will be $(P(\text{contact pair transfers closed}))^3$ and is negligible.

- Contact pair 1-7 associated with the overpressure interlock coil transfers closed AND contact pair 2 of the handswitch transfers closed AND locking circuitry contact 42-O/b transfers open. Again the probability of this scenario is extremely low.

- The operator inadvertently opens the key-locked shut valve AND the overpressure interlock malfunctions. This scenario is also of extremely low probability.

4.1.6 LEFT OPEN 2-SI-651 (With ACI)

Three different defenses exist to prevent reaching power operation with a LEFT OPEN 2-SI-651 valve. They are:

- Unit operating procedure OP 2310 which instructs the operator to close 2-SI-651. A probability of $3.2 \times 10^{-3}$ is assigned for the failure of this event (Ref. 9).

- The same procedure requires a leak test of 2-SI-651. The probability of omission of this step is also assigned a probability of $3.2 \times 10^{-3}$.

- The SDC ACI will automatically close 2-SI-651 upon the receipt of high pressure signal. Failure to close upon receipt of the high pressure signal is assigned a screening probability value of $1 \times 10^{-4}$.

After considering the dependency among the above defenses, the probability of event "2-SI-651 MOV LEFT OPEN" has been estimated to be $3.2 \times 10^{-7}$ (Ref. 10).

4.1.7 LEFT OPEN 2-SI-651 (Without ACI)

The probabilities in Section 4.1.6 will change if the ACI is deleted. The SDC ACI which acts to automatically isolate 2-SI-651 will now be replaced by a manual action where the operator will close 2-SI-651 upon the receipt of an alarm.

Reference 10 recalculated the probability of the "2-SI-651 LEFT OPEN" event for the case where the ACI is replaced by an alarm. This new probability is $4.2 \times 10^{-7}$.

4.1.8 Catastrophic Failure of 2-SI-651

The probability of the catastrophic failure of 2-SI-651 following the catastrophic failure of 2-SI-652 will be based on the failure rate $1 \times 10^{-7}$ per hour used for 2-SI-652. It is assumed that the valve 2-SI-651 is exposed to the high RCS pressure upon 2-SI-652 failure. The failure probability is given by the expression:

$$\lambda T$$

where $\lambda$ is the failure rate ($= 1 \times 10^{-7}$ per hour) and T is the exposure time.

The average exposure time of the valve 2-SI-651 subsequent to 2-SI-652 failure will depend upon the function of the relief valve. If RV 2-SI-469 did successfully lift and the operators correctly identified the failed 2-SI-652, then the reactor will be shutdown. Even if the operators did not recognize the exact cause of the RCS leakage, leakage beyond the tech spec allowable rate for unidentified leakage would necessitate a prompt shutdown. Therefore, following Ref. 10, a 36-hour exposure time will be assumed. The failure probability will be $3.6 \times 10^{-6}$ ($= 36 \times 1 \times 10^{-7}$).

On the other hand, if the relief valve failed to lift, 2-SI-651 may be exposed to the high RCS pressure on the average half of the Refuel Cycle. Therefore, the failure probability will be $6.57 \times 10^{-4}$ ($= \frac{1}{2} \times (1.5 \times 8760)(10^{-7})$).

4.1.9 ISLOCA Frequency

The event trees (Figures 3 and 4) illustrate the credible ISLOCA scenarios through the SDC suction path with and without the ACI feature.

The total ISLOCA frequency for the "with ACI" case is $4.01 \times 10^{-9}$ per year compared to the total frequency of $4.10 \times 10^{-9}$ for the "without ACI and with Alarm" case.

Based on the absolute magnitudes of the above frequencies and the insignificant change in the frequencies, it is concluded that the impact of the ACI removal on the ISLOCA frequency is insignificant.

4.2 Loss of Shutdown Cooling System

The SDC ACI removal is encouraged due to its high contribution to loss of SDC events. The industry experience leaves no doubt in the fact that the ACI is a major cause for loss of SDC events during shutdown.

As illustrated by Table 1, of 130 total loss of DHR events which occurred during the period between 1976-1983, 37 events were attributed to the automatic closure of suction isolation valves. Using References 5, 6, 7, and 9 as bases, it is concluded that the removal of the ACI feature will provide a significant benefit (operational and safety) to the plant.

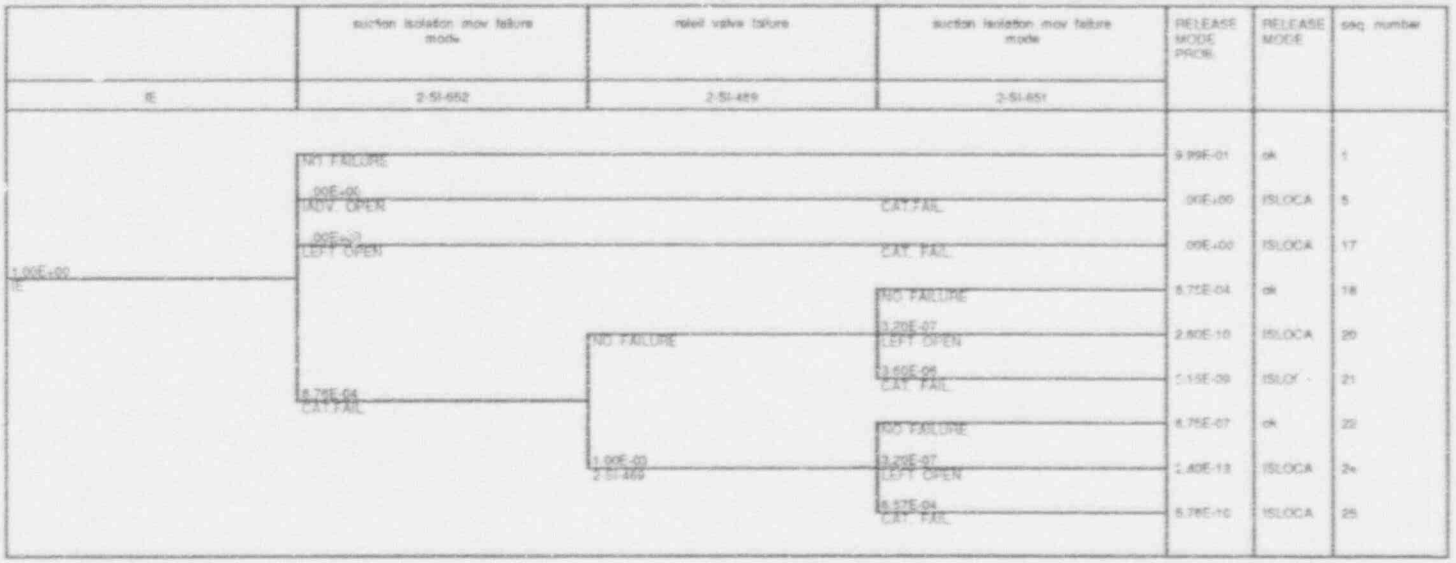


FIGURE 3: ISLOCA Sequences (with ACI) C:\CAFTA\MP2ACI\MZIWACI.TRE 10/24/91

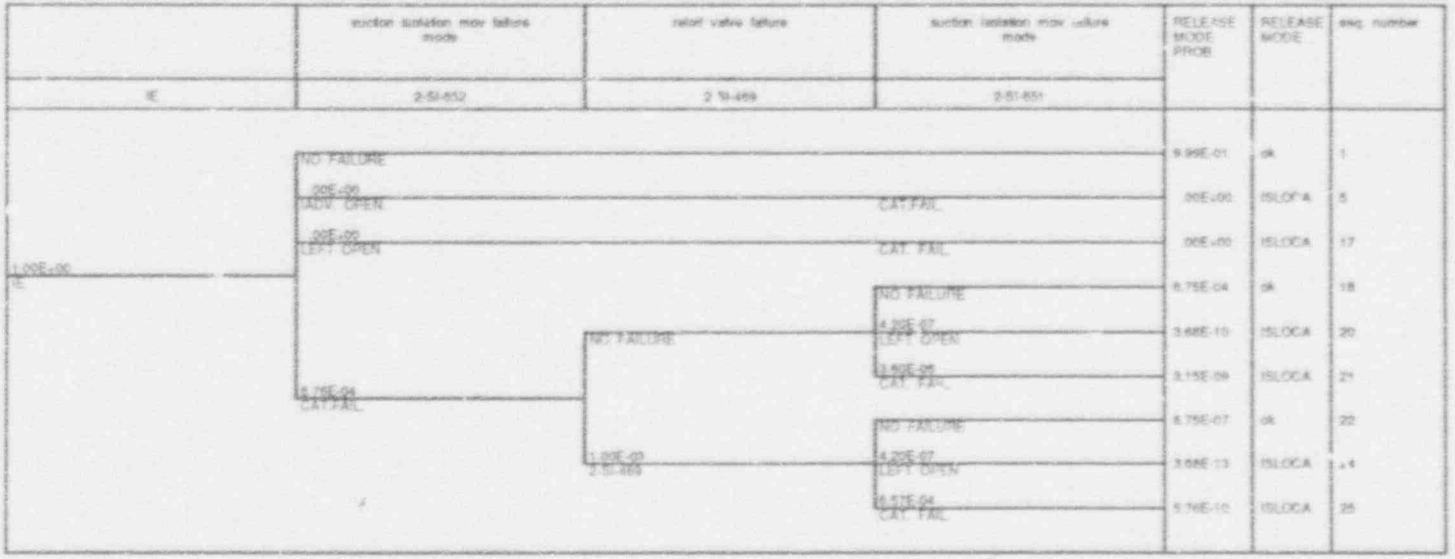


FIGURE 4: ISLOCA Sequences (without ACI) C:\CAFTA\MP2\ACI\MONACI.TRE 10/24/91

The risk to the public due to loss of shutdown cooling during shutdown events is expected to be reduced due to removal of the ACI.

## 4.3 Overpressure Transients

Equipment malfunctions, procedural deficiencies, and incorrect operator actions during startup can lead to pressure transients in the RCS while the SDC is in operation. These pressure transients are of concern because (a) the SDC may be subjected to pressures exceeding its design pressure, and (b) the RCS may be subjected to pressures that exceed the allowable limits at low temperatures.

The response to the overpressure transients and the potential for overpressure transients may be altered due to the removal of the ACI. This section identifies events whose potential or response may be affected by the ACI removal.

### 4.3.1 Method of Analysis

In the sections that follow, a large number of overpressure transient events are investigated. Several aspects of these overpressure transients are considered.

First of all, the potential (initiating event frequency) for an overpressure accident will be examined. This investigation will be plant specific in that the shutdown operating procedures and practices have a significant impact on most of the initiators considered. If the investigation of this potential reveals that the frequency of the overpressure transient under consideration is negligibly low, that is, the initiator is not credible for MP2, then further analysis of that initiator will not be performed.

If the frequency of an overpressure transient is relatively high, either based on the industry experience or the MP2 operating history, the importance of ACI to that initiator, either as a contributor to the initiator or as a part of the mitigating system, will be investigated. This will be

compared against the role of the ALARM and the OPERATOR RESPONSE that will replace the ACI.

4.3.2 Premature Opening of the SDCS

Several procedural steps, precautions and interlocks exist to prevent a scenario where the operator would align the RCS with SDC prior to sufficient depressurization of the system. These are as follows:

- Several precautions in unit operating procedure OP 2207 (Ref. 12) "Plant Cooldown" emphasize that the SDC system shall not be exposed to RCS pressures exceeding 265 psia.

- SDC suction valves are equipped with a prevent open Interlock. The function of the interlock is to prevent the opening of the SDC valves if the RCS pressure is higher than 280 psia. The operation of these interlocks will not be affected by ACI removal.

- Valve 2-SI-652 is key locked and power is removed from it. Therefore, accidental or inadvertent operation is not possible. Valve 2-SI-651 is also key locked. However, power is available at the breaker. These two valves are in series and premature opening of the SDCS requires opening of both these valves.

In consideration of the above, premature opening of the SDCS is considered a scenario with negligibly low frequency.

4.3.3 Rod Withdrawal

A prerequisite of the Unit 2 operating procedure OP 2207 requires that the control element drive mechanisms (CEDM) be de-energized before the cooldown from hot standby to cold shutdown is initiated. The CEDMs are de-energized by either setting the motor generator (MG) output breakers open and tagged by the Shift Supervisor or by de-energizing the coil power programmers for all control element assemblies and tagging by the Instrument and Control Department Head.

Withdrawal of rods in Modes 4, 5, and 6 is not credible since control rod drives are de-energized whenever the RCS boron concentration is less than the refueling concentration of 1720 ppm per Technical Specifications (MNP2 FSAR, Reference 13). Therefore, the potential for this accident and therefore, the impact of ACI removal is negligible.

4.3.4 Failure to Isolate SDCS During Start Up

During the startup, the operators are required to close the suction isolation valves 2-SI-651 and 2-SI-652 (Reference 14). Failure to isolate the SDCs during startup, if not detected early, will lead to overpressurization of the low pressure SDC piping.

Several operator errors must occur in order to fail to isolate SDCS during startup. They are:

- Operator fails to close 2-SI-651 and 2-SI-652 per operating procedure OP 2310.
- Operator fails to perform leak rate test of 2-SI-651.
- Operator fails to detect via the open relief valve 2-SI-469 discharging into the primary drain tank, which has alarms.
- Operator fails to detect due to loss of RCS inventory during startup.

Based on analysis performed in Reference 10, the probability of the scenario will be of the order of $10^{-10}$ and, therefore, is considered insignificant from a risk perspective.

4.3.5 Pressurizer Heater Actuation

This transient has no measurable impact on the LTOP risk when ACI is replaced by an alarm. The basis for this conclusion are as follows:

- Pressurizer heater actuation (inadvertent) during shutdown, should it occur, will lead to a slow developing transient. Therefore, the

Alarm (new) will be as timely as ACI in preserving the SDC integrity. That is, the operator response time introduced when the ACI is removed will not be a factor in isolating the SDC.

- The shutdown operating procedure (OP2310) is utilized to minimize inadvertent energizing of the pressurizer heaters.

4.3.6 Startup of an Inactive LOOP

When the RCPs have been stopped, the steam generator water may remain at a relatively constant temperature greater than the RCS temperature. When a significant difference between the SG temperature and the RCS temperature exists, if an RCS pump is inadvertently started, the sudden heat input to the RCS will result in a rapid increase in the RCS temperature.

The probability of occurrence of the above accident is minimized due to several operating practices. During plant cooldown (OP 2207) (Reference 12), the unit operating procedure OP 2207 instructs the operator to reduce the number of running RCPs to two. The same operating procedure instructs the operator to secure the two remaining RCPs when the RCS temperature is approximately 230°F and heat removal by steam from the S/Gs is stalled. Further, OP 2207 instructs the operator to verify that all RCPs are secured and their circuit breakers are racked down. In addition, operators are instructed to TAG all RCP circuit breakers OR RACKDOWN and TAG all 6.9-kV feeder circuit breakers.

During plant heat up, unit operating procedure OP 2201 (Reference 14) instructs the operator to TERMINATE shutdown cooling prior to exceeding RCS pressure of 265 psia and to start two RCPs and start the third pump after reaching 200°F.

Based on the above sequence of events for (i) securing RCP pumps, (ii) aligning SDC with RCS, (iii) terminating SDC, and (iv) starting RCPs, the likelihood of an inadvertent operation of an RCP when the SDC is aligned to the RCS is minimized, if not eliminated.

Several other factors mitigate the potential of occurrence of this transient. They are:

- For an inadvertent RCP transient to cause a pressure spike, the RCS PORVs would have to fail to lift. During shutdown, two PORVs are available to relieve pressure.

- A pressure spike cannot occur unless the reactor is water solid. The actual events that took place at Turkey Point Unit 4 supports this notion (Reference 5). If there is a steam space in the pressurizer, that will collapse to accommodate the RCS coolant expansion due to heat up.

Another point that is noteworthy is as follows. If an overpressure transient occurs due to an inadvertent RCP startup when the reactor is water solid, the pressure rise rate is rapid in comparison to the time taken to isolate SDC. Note that the SDC isolation MOVs need 1-2 minutes to close (with ACI) (or ~ 5-10 minutes without ACI). By that time the pressure transient would already have occurred. Therefore, consequences will not be different in the SDC for the with and without ACI cases. Further, also note that the potential consequences of overpressurizing the RCS is independent of SDC/RCS isolation. In fact, for the RCS, the consequences can be worse for the case where ACI effectively isolates the SDC from RCS because of the loss of additional pressure relief paths.

4.3.7 Loss of SDCS Cooling Train

The overpressure transient considered in this section is loss of SDCS cooling due to losses of equipment such as heat exchangers, service water, or pumps, rather than SDCS isolation events due to inadvertent ACI actuation.

Plant heat up rate subsequent to the loss of SDCS cooling event, and hence the rate of change of RCS/SDC pressure and temperature, is dependent upon the decay heat rate at the time of the event.

Due to the following reasons, the impact of removing the ACI is considered insignificant for this transient:

- Unless the event occurs soon after aligning the SDC when the decay heat levels are high, the transient will be relatively slow. For transients in which the pressure rise rate is relatively slow, replacing the ACI by an alarm (to be installed) requiring operator action will not have a significant impact.

- Since SDC stays aligned to the RCS if the ACI (or the Alarm + Operator Action) fails, the SDC RVs will be available to mitigate the transient.

- Irrespective of whether the SDC was isolated or not, the PORVs (2 redundant trains) will also be available to mitigate the transient.

4.3.8 Opening of Accumulator Discharge Isolation Valves

The nominal operating pressure of the MP2 Safety Injection Tanks (SIT) is 215 psig. Therefore, discharge of the SIT tanks into the RCS cannot overpressurize the SDC. The SDC ACI removal has no impact since this transient cannot occur. Further, per cooldown procedure OP 2207, several steps are taken to prevent discharge of SIT tanks to the RCS.

4.3.9 Letdown Isolation

The plant behavior following a letdown isolation event was modeled and analyzed using an event tree to an extent that allows analysis of the impact of SDC ACI removal (Reference 10). The event tree analysis used approximate order of magnitude analysis for probabilities to show that the ACI removal has minimal impact.

4.3.10 Charging Pump Actuation

Inadvertent actuation of charging pumps has the potential to create overpressure transients. This transient is not analyzed further due to the following:

- At MP2, the capacity of a single charging pump is 44 gpm. Therefore, even if all three charging pumps are operating, the maximum flow rate into the RCS cannot exceed 132 gpm. This flow rate is low compared to the PORV capacities. A single PORV can easily accommodate pressure rise associated with inventory input to the RCS.

- In addition to above, the capacity of the relief valve 2-SI-468 on the SDC suction path is 222 gpm and far exceeds the total capacity of all three charging pumps.

- As indicated by LER #90-015-Ø1 (Reference 15), MP2 has had an event where all three charging pumps started. During this event only 50 gallons of inventory was added to the system and the operator stabilized the plant using AOP 2571 (Reference 16).

4.3.11 Safety Injection Pump Actuation

In the event that one or both safety injection (SI) pumps inadvertently actuate when the plant is shutdown and SDC is aligned to the RCS, a significant mass input overpressure transient can occur. Unlike the charging pumps whose capacity is 44 gpm per pump, the three safety injection pumps at MP2 have a design flow of 315 gpm per pump. Although the PORVs are capable of handling this mass input, the relief valves on the SDC suction line are inadequate to prevent overpressurization due to inadvertent safety injection.

The event trees in Figures 5 and 6 model the response of the plant and the operator to an inadvertent SI actuation event and illustrate how the frequency of the end states may change when the ACI is replaced by an ALARM and an Operator action.

The basis for choosing an initiating event frequency of Ø.Ø1 per year and the basis for other probabilities used in the event trees in Figures 5 and 6 are provided in Reference 10.

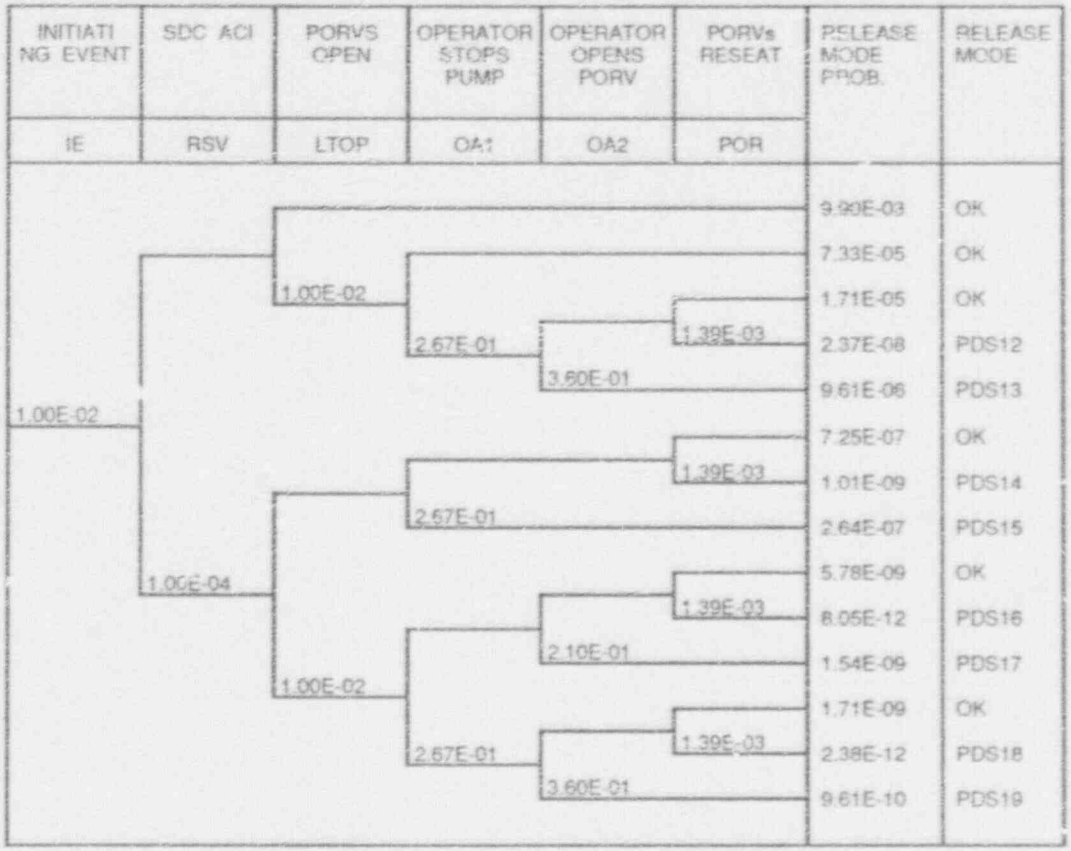


FIGURE 5: Inadvert. SI during Shutdown (with ACI) C:\CAFTA\MP2ACI\NADSI.TRE 10/24/91

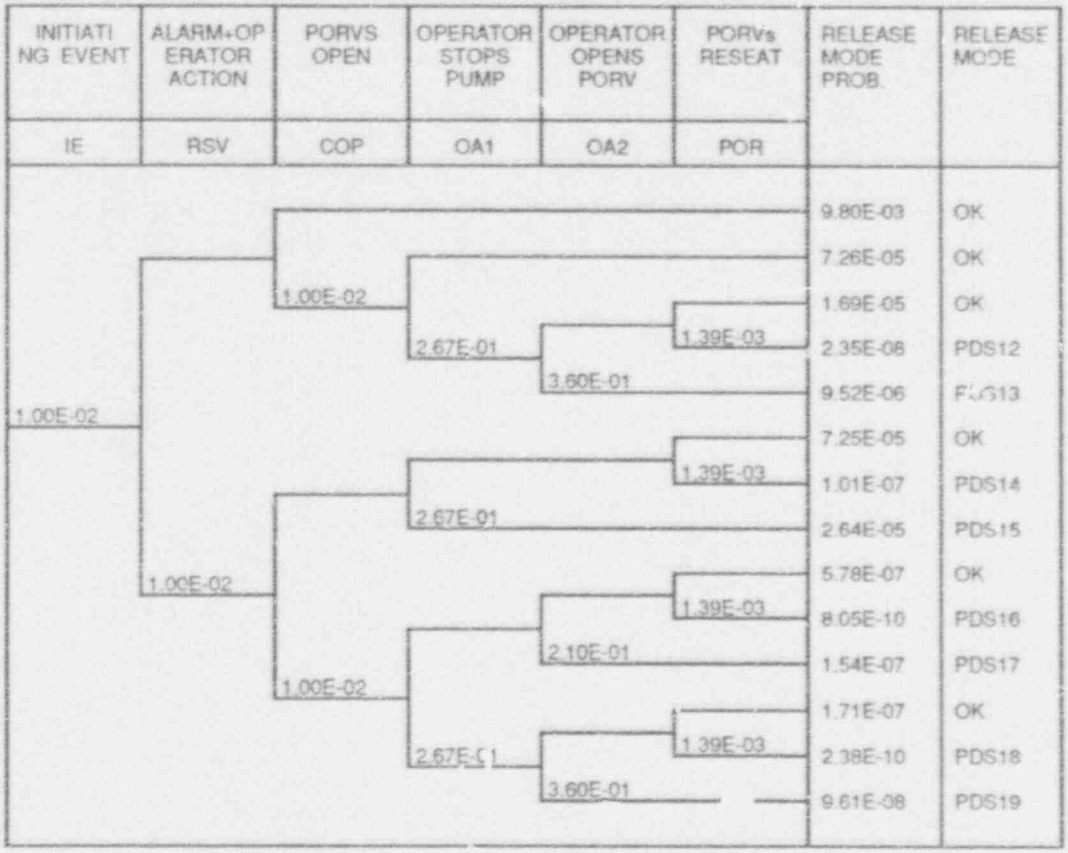


FIGURE 6: Inadver. SI during Shutdown (with alarm) C:\CAFTA\MP2AC\INADSI2.TRE 10/24/91

- Comparison Between WITH ACI and WITHOUT ACI Cases

As illustrated in Figures 5 and 6, the reduced reliability of "ALARM + OPERATOR ACTION" compared to the ACI is reflected by the increased frequencies of plant states PDS14 through PDS19 by about two orders of magnitude. However, before judging this increase as significant, (a) the risk significance of each of the PDSs and (b) the magnitudes of the frequencies need to be considered. It is emphasized that a PDS in the context of this analysis is not necessarily a core-melt or significant damage to the plant. Rather, the sequences identified as PDSs are plant conditions which require further operator actions in order to stabilize the plant.

For reasons such as "LIFTED PORV" or "SECURED SI PUMP," the overpressure transient has been arrested for the sequences, PDS12, PDS14, PDS15, PDS16, PDS17, and PDS18. They are treated as insignificant in risk.

For PDS13, since the ACI or the alarm resulted in the closure of the SDC suction isolation valves, SDC integrity is assured. However, since the automatic and manual attempts to open the PORVs failed, the RCS integrity is not assured. Further operator actions to secure the injection pumps must be made. This sequence may be treated as a risk significant sequence. However, its frequency is reduced by ACI removal.

The sequence frequency of PDS19 increases from $9.61 \times 10^{-10}$ to $9.61 \times 10^{-8}$ when the ACI is deleted. Further, this sequence is risk significant in that both automatic and manual actions to mitigate the transient have failed. The sum of the frequencies of the risk significant sequences PDS13 and PDS19 increases from $9.61 \times 10^{-6}$ ($9.61 \times 10^{-6} + 9.61 \times 10^{-10}$) per year for the WITH ACI case to $9.62 \times 10^{-6}$ ($9.52 \times 10^{-6} + 9.61 \times 10^{-8}$) per year for the WITHOUT ACI case. That is, when the ACI is removed, the total frequency of the risk significant sequences increased by one $10^{-8}$ per year.

This is a negligible increase in risk. In spite of this negligible increase in risk, the following investigations were performed as a part of this analysis to minimize the increases in risk due to ACI removal.

- Minimizing inadvertent SI actuations.

- Improving LTOPS reliability.

4.3.11.2 Minimizing Inadvertent SI Pump Actuations

The initiating event frequency used in the event trees in Figures 5 and 6 (.Ø1 per year) is based on a frequency of Ø.125 per shutdown year. The purpose of this section is to summarize the investigation of steps taken to minimize SI Pump actuations at MP2. In this discussion, an SI Actuation should be interpreted as the inadvertent SI signal starting an SI pump or pumps and discharging into the RCS. An inadvertent SI event that does not start the SI pumps is not significant since an overpressure transient does not result.

The operating procedures at MP2 were reviewed in order to examine the precautions taken to prevent inadvertent SI pump discharges into RCS. They are as follows:

- According to Unit 2 operating procedure OP 22Ø7, when "SIAS BLOCK PERMISSIVE" is annunciated at approximately 1750 PSIA, the SIAS signal is blocked and one HPSI pump is disabled by tagging the pump breaker open and by closing its discharge valve or header isolation valves.

- OP 22Ø7 instructs the operator to VERIFY one HPSI train disabled prior to decreasing temperature below 275°F.

- OP 22Ø7 cautions the operators to not allow any work to commence or continue on the ESAS panel since this will prevent a HPSI pump start and possible overpressurization.

The above procedural steps and the cautionary statement assume that only a single SI pump may start in the event of an inadvertent SI, and therefore, inadvertent actuation of the non-disabled SI train is minimized. Considering the relatively small capacities of the charging pumps at MP2, disabling both HPSI trains is not recommended since an adverse effect on LOCA risk can result.

4.3.11.3 Improving LTOP Reliability

The frequency of the risk significant sequence PDS13 is relatively high and could be reduced by improving LTOP reliability.

As shown in Figure 7, the two trains of LTOP are independent. This figure is based on information provided in References 17-24. The 120 VAC and 125 VDC supplies to the two trains are also independent. Given that the two LTOP trains are independent, it is determined that the LTOP unavailability is dominated most likely by other common cause failures (CCFs).

Functionally Coupled CCFs

Using References 17-24, functions or system hardware that could potentially fail both trains of LTOP were investigated. The support systems for instruments such as 120 VAC and 125 VDC were examined for shared dependencies. Such shared hardware were not found.

Human Couplings

CCFs attributable to human couplings were examined. Likely candidates for human errors of omission are discussed below:

- Operator fails to change PORV set point from HIGH to LOW during plant cooldown.

  Several defenses exist against the above operator error. There are several procedural steps and precautions on changing the PORV set point from HIGH to LOW. In addition, as illustrated by Figure 7, when the RCS temperature is less than 280°F and RCS pressure is less than 375 psia, "RESET TO LOW" will be annunciated on the control board. Given that procedural instructions, precautions, and alarms exist, the probability of this error is considered low.

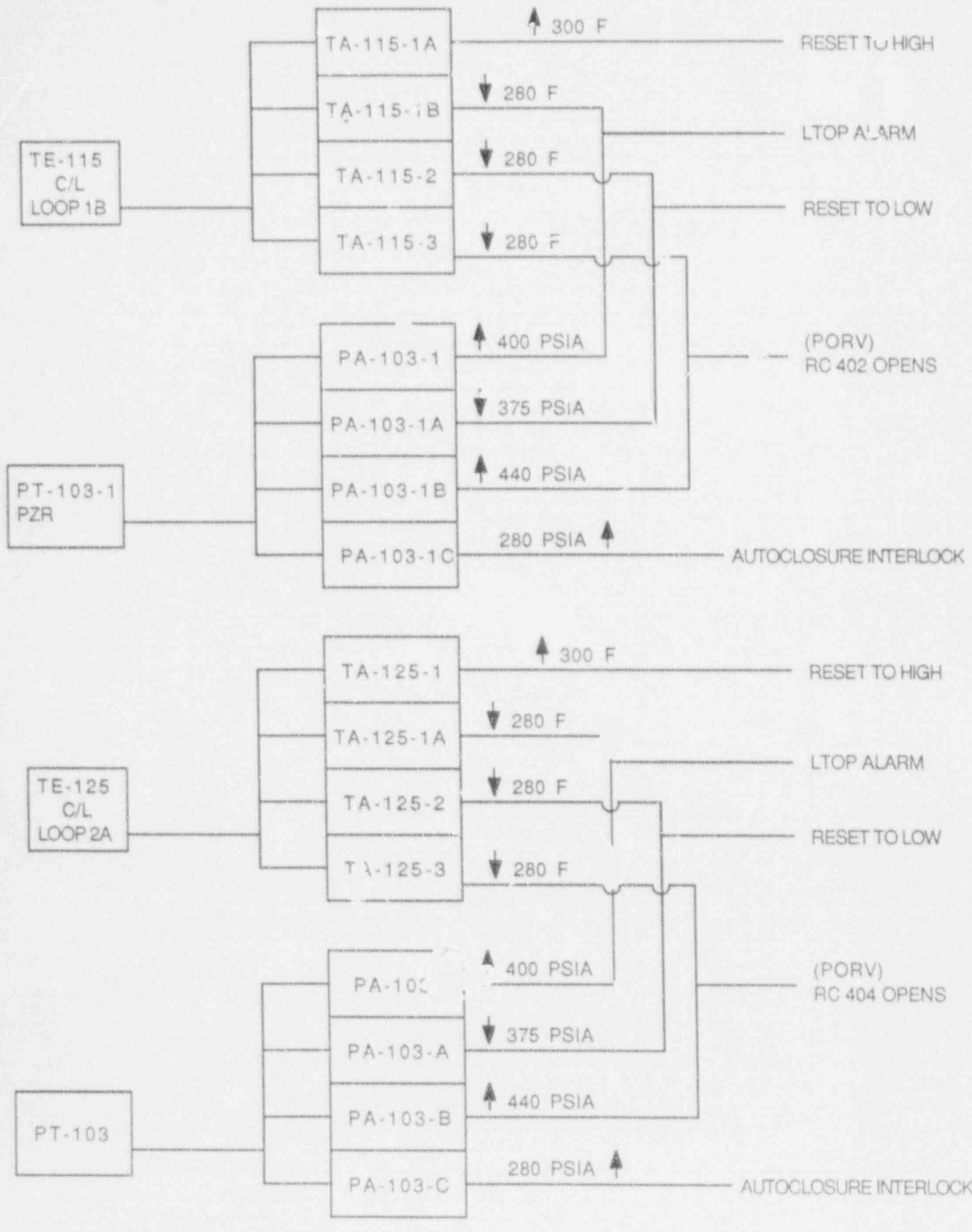


FIGURE 7 LTOP & ACI ALARMS & ACTUATIONS

- Operator unintentionally disables LTOP capability.

In spite of the Technical Specifications and other precautions, industry experience and MP2 plant specific experience indicate that the unintentional disabling of LTOP is a credible failure that may contribute to partial or total failure of LTOP.

For example, during the scenario described in LER 85-010, both LTOPs were out of service at MP2 due to procedural deficiency. Specifically, both PT-103 and PT-103-1 pressure transmitters used in the two independent LTOP trains were isolated and left in that state as a prerequisite for the containment building integrated leak rate test (ILRT). During this event, insufficient LTOP protection existed for up to 36 hours.

At MP3, during 1988 both trains of the overpressure protection system were disabled due to an operator error of commission (Reference 25). Specifically, both logic trains for the overpressure protection system were disabled when the RPS panels were disabled.

The above examples show that operator errors of commission rather than omission may contribute to the failure of both LTOP trains.

activities that are carried out during shutdown may affect significant portions of LTOP trains. It is concluded that ensuring that the shutdown activities and procedures do not interfere with LTOP performance may lead to an improved LTOP reliability.

## 5.0 CONCLUSIONS, INSIGHTS, AND RECOMMENDATIONS

This section summarizes the findings of the PRA analysis and, where appropriate, provides recommendations based on insights gained during the analysis.

### 5.1 ISLOCA Analysis

Removal of ACI and replacing it with the proposed alarm has negligible impact on ISLOCA frequency for power operation. The impact on this frequency may be minimal to none. The following insights gained are considered significant.

(i) The existence of the relief valve 2-SI-469, and more importantly its set point of 300 psig, results in the extremely low ISLOCA frequency associated with the SDC suction path. Note that, although the chosen set point for 2-SI-469 is 300 psig, the design basis set point for this valve is 2300 psig. From an ISLOCA point of view, the 300 psig set point is superior to a 2300 psig set point. This insight is considered significant and will be included in the MP2 FSAR.

(ii) The leak rate test (LRT) of the SDC isolation valve 2-SI-651 is performed usually during the plant heat up rather than the plant cooldown process. The ISLOCA frequency will not be significantly affected even if the LRT is performed during plant cooldown, in which case this valve will be cycled after the LRT. However, from a safety point of view, the LRT is preferred during plant heat up.

(iii) At MP2, the power to the suction isolation valves is removed prior to reaching the mid-loop operation with these two valves placed in the OPEN position. The purpose of this action is to prevent ACI induced loss of SDC events. However, this operating practice introduces the potential to leave the SDC isolation valves in the OPEN position after the midloop operation is completed. When the SDC ACI is removed, this potential operator error, which may contribute to an ISLOCA, will be eliminated.

5.2 Loss of Shutdown Cooling

Based upon industry experience, it is concluded that the frequency of loss of SDCS events could be reduced by approximately 28 percent when the ACI is removed. Inadvertent ACIs that cause the loss of the SDCS are risk significant if they occur during midloop operations. At MP2, the SDC isolation MOVs are de-energized in the OPEN position during midloop operation. This operation practice minimizes the risk associated with the inadvertent ACI events.

5.3 Overpressure Transients

In summary, ACI removal at MP2 has a minimal impact on the risk usually attributed to ACI removal. Specific insights on individual LTOP transients are as follows:

i. Effect of ACI removal on the "premature opening of the SDCS" is disregarded due to the low frequency of the initiator. That is, the interlocks and operating procedures reduce the likelihood of this transient to a minimum.

ii. Effect on the "Inadvertent Rod Withdrawal" accident is not analyzed in detail due to the low likelihood of the accident.

iii. Effect of ACI removal on the "Failure to Isolate SDCS During Start Up" overpressure transient is not analyzed in detail due to the very low likelihood of occurrence of this event.

iv. Effect of ACI removal on the "Inadvertent Pressurizer Heater Actuation" event is not analyzed in detail due to the low probability of this event and also due to slow development of the transient.

v. Effect of ACI removal on the "Startup of an Inactive RCP Loop" is minimal if not negligible due to:

   a. low probability of occurrence, and

b. mitigating systems (ACI or ALARM, Relief Valve, PORVs) available as defenses.

c. Consequences of the transient may be too rapid for either ACI or the ALARM to make a difference.

vi. Effect of ACI removal on the "Loss of SDCS Cooling Train" transient is minimal due to relatively low pressure rise rate (unless the transient occurs soon after aligning the SDC following shutdown), and availability of mitigating systems such as PORVs, SDC Relief Valves, in addition to the ACI or the new ALARM.

vii. ACI removal has no impact on the "Opening of Accumulator Isolation Valves" transient due to relatively low operating pressure of the SIT tanks and due to many operating practices used to prevent SIT tank discharge into the RCS.

viii. ACI removal has an insignificant impact on the risk attributed to the "Letdown Isolation, SDC Operable" transient due to multiple defenses such as the PORVs and the SDC relief valve 2-SI-468 in addition to ACI or the new ALARM. Adequacy of the capacity of 2-SI-468 (SDC relief valve, 222 gpm) with respect to the input from the charging pumps (44 gpm/pump) is a key to the insignificant impact.

ix. ACI removal has an insignificant impact on the "Charging Pump Actuation" Transient due to (a) adequate capacity of the relief valve 2-SI-468 compared to charging pumps and (b) PORV capability and operator capability illustrated during a plant specific event.

x. The risk increase associated with the "Inadvertent SI Pump Actuation Transient" is negligible.

Other insights gained from this transient analysis are summarized in Sections 5.4 and 5.5.

5.4 LTOP Reliab. y

The analysis of the inadvertent SI pump actuation transient above indicates the high importance of LTOP reliability since it is the single defense to prevent RCS overpressurization apart from the operator actions that are not proceduralized.

LTOP consists of two completely independent trains, but other common cause failures could play a major role in LTOP reliability. Based on further examination, it is concluded that the Errors of Commission, specifically, undesirable impacts on LTOP trains resulting from shutdown activities, most likely, is the single largest CCF contributor to LTOP unavailability. A review of procedures to minimize human errors of commission that can potentially disable both trains of LTOP will be a cost-beneficial effort. It is emphasized that the above is simply an important insight gained during the study, and the risk attributed to this overpressure transient is not significantly affected by the ACI removal. However, MP2 engineering reviewed existing procedures to verify that the potential for human errors of commission is minimized.

5.5 SDC Relief Valve 2-SI-468 Capacity

It is concluded that the capacity of the SDC relief valve 2-SI-468 is adequate except for the overpressure transient where one or more SI pumps may actuate. The operating practices at MP2 have minimized the potential for SI pump actuation as far as practicable and cannot be reduced further without adversely affecting the shutdown LOCA risk. MP2 Technical Specifications surveillance section 4.5.3.2 requires that all but one HPSI be disabled prior to cooling down below 275°F. In addition, procedure OP2207 also specifically directs this action (Step 4.22.5) and then cautions against allowing work that can cause a HPSI pump start until all pumps are disabled.

## REFERENCES

(1) P&ID 25203-26015, "L.P. Safety Injection System," Sh. 1 of 3, Revision 7.

(2) P&ID 25203-26015, "L.P. Safety Injection System," Sh. 3 of 3, Revision 5.

(3) Generic Letter 87-12, "Loss of RHR while the RCS is Partially Filled," USNRC, July 9, 1987.

(4) Generic Letter 88-17, "Loss of Decay Heat Removal," USNRC, October 17, 1988.

(5) G. Vine, et al, "Residual Heat Removal Experience Review and Safety Analysis - Pressurized Water Reactors," NSAC-52, January 1983.

(6) U.S. Nuclear Regulatory Commission, Office for Analysis and Evaluation of Operational Data, "Decay Heat Removal Problems at U.S. Pressurized Water Reactors," Case Study Report AEOD/C5Ø3, December 1985.

(7) Memorandum from B. W. Sheron, NRC to RSB members, "Auto Closure Interlocks for PWR Residual Heat Removal System," January 28, 1985.

(8) OP 2310, "Millstone Unit 2 Operating Procedure for Shutdown Cooling."

(9) WCAP 11736-A, "Residual Heat Removal System Auto Closure Interlock Removal Report for the Westinghouse Owner's Group," Rev. Ø.Ø, October 1989.

(10) Northeast Utilities Calc. File W2-517-999-RE, "MP2 SDC ACI Removal," Rev. Ø.

(11) Northeast Utilities Calc. File W2-517-787-RE (Revision Ø), "Interfacing Systems LOCA," July 8, 1987.

(12) MP2 Station Procedure OP 2207, "Plant Cooldown," Revision 16.

References (Continued)

(13) Millstone Nuclear Power Station Unit 2, Final Safety Analysis Report.

(14) OP 2201, "MP2 Unit Operating Procedure - Plant Heat-Up," Revision 19.

(15) MP2 LER 90-015-01, "Inadvertent ECCS Actuatis, Update Report," 09-19-90.

(16) AOP 2571, "Inadvertent ECCS Initiation," Revision 1.

(17) MP2 P&ID 25203-28500 "TE-111Y, TE-115, and PT-103-1 COLD LEG TEMP to Reactor LOOP Diagram," Sh. 75C, Revision 5.

(18) MP2 P&ID 25203-28500, "TE-111Y, TE-115, and PT-103-1 COLD LEG TEMP to Reactor LOOP Diagram," Sh. 75D, Revision 1.

(19) MP2 P&ID 25203-28500, "TE-121Y, TE-125, and PT-103 COLD LEG TEMP. to Reactor LOOP Diagram," Sh. 99D, Revision 1.

(20) MP2 P&ID 25203-28500, Sh. 99C, Revision 5.

(21) MP2 P&ID 25203-28500, Sh. 99B, Revision 11.

(22) MP2 P&ID 25203-32007, Sh. 23, Revision 7.

(23) MP2 P&ID 25203-32007, Sh. 24, Revision 6.

(24) MP2 P&ID 25203-28500, Sh. 75B, Revision 7.

(25) MP3 LER 88-005, "Cold Overpressure Protection System Fails to Operate During Pressure Transient," 02-18-88.