REGULATORY INFORMATION DISTRIBUTION SYSTEM (RIDS)

ACCESSION NBR:8202020282 DOC.DATE: 82/01/29 NOTARIZED: NO DOCKET #
FACIL:50-361 San Onofre Nuclear Station, Unit 2, Southern Californ 05000361
50-362 San Onofre Nuclear Station, Unit 3, Southern Californ 05000362
AUTH.NAME AUTHOR AFFILIATION
BASKIN,K.P. Southern California Edison Co.
RECIP.NAME RECIPIENT AFFILIATION
MIRAGLIA,F. Licensing Branch 3

SUBJECT: Forwards revised response to NRC Question 222.44 re effects of control sys failures in Section 7.7.2 of draft SER, Suppl 4.Revisions to FSAR Sections 5.4.7 & 6.3 & NRC Questions 212.65,212.66,212.67 & 212.68 encl.

DISTRIBUTION CODE: B001S COPIES RECEIVED:LTR 1 ENCL 63 SIZE: 52
TITLE: PSAR/FSAR AMDTS and Related Correspondence

NOTES:L Chandler:all FSAR & ER amends.1 cy:J Hanchett(Region V). 05000361
D Scaletti:1 cy all envir info.
L Chandler:all FSAR & ER amends.1 cy:J Hanchett(Region V). 05000362
D Scaletti:1 cy all envir info.

	RECIPIENT ID CODE/NAME		COPIES LTTR	COPIES ENCL	RECIPIENT ID CODE/NAME		COPIES LTTR	COPIES ENCL
ACTION:	A/D LICENSNG		1	0	LIC BR #3 BC		1	0
	LIC BR #3 LA		1	0	ROOD,H.	01	1	1
INTERNAL:	ELD		1	0	IE	06	3	3
	IE/DEP/EPDB	35	1	1	IE/DEP/EPLB	36	3	3
	MPA		1	0	NRR/DE/CEB	11	1	1
	NRR/DE/EQB	13	3	3	NRR/DE/GB	28	2	2
	NRR/DE/HGEB	30	2	2	NRR/DE/MEB	18	1	1
	NRR/DE/MTEB	17	1	1	NRR/DE/QAB	21	1	1
	NRR/DE/SAB	24	1	1	NRR/DE/SEB	25	1	1
	NRR/DHFS/HFEB	40	1	1	NRR/DHFS/LQB	32	1	1
	NRR/DHFS/OLB	34	1	1	NRR/DHFS/PTRB	20	1	1
	NRR/DSI/AEB	26	1	1	NRR/DSI/ASB	27	1	1
	NRR/DSI/CPB	10	1	1	NRR/DSI/CSB	09	1	1
	NRR/DSI/ETSB	12	1	1	NRR/DSI/ICSB	16	1	1
	NRR/DSI/PSB	19	1	1	NRR/DSI/RAB	22	1	1
	NRR/DSI/RSB	23	1	1	NRR/DST/LGB	33	1	1
	REG FILE	04	1	1				
EXTERNAL:	ACRS	41	16	16	BNL(AMDTS ONLY)		1	1
	FEMA-REP DIV	39	1	1	LPDR	03	1	1
	NRC PDR	02	1	1	NSIC	05	1	1
	NTIS		1	1				

TOTAL NUMBER OF COPIES REQUIRED: LTTR ~~63~~ 64 ENCL ~~58~~ 59

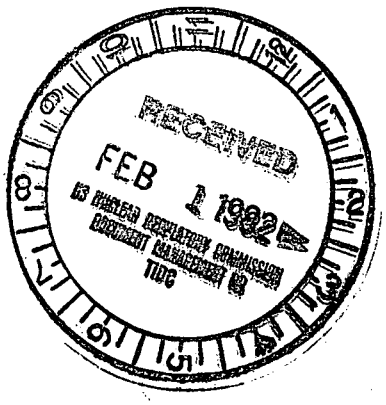
Southern California Edison Company

P. O. BOX 800
2244 WALNUT GROVE AVENUE
ROSEMEAD, CALIFORNIA 91770

K. P. BASKIN
GER OF NUCLEAR ENGINEERING,
SAFETY, AND LICENSING

TELEPHONE
(213) 572-1401

January 29, 1982



Director, Office of Nuclear Reactor Regulation
Attention: Mr. Frank Miraglia, Branch Chief
Licensing Branch No. 3
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

Gentlemen:

Subject: Docket Nos. 50-361 and 50-362
San Onofre Nuclear Generating Station
Units 2 and 3

Enclosed are sixty-three copies of the revised response to NRC Question 222.44 concerning Effects of Control System Failures addressed in Section 7.7.2 of the Draft Safety Evaluation Report, Supplement No. 4. Also enclosed are sixty-three copies of revisions to FSAR Sections 5.4.7 and 6.3, and to NRC Questions 212.65, 212.66, 212.67 and 212.68 to reflect changes to the shutdown cooling system and related operating procedures.

These revisions will be incorporated into the FSAR and direct distribution of this information will be made as part of Amendment 29 distribution and will be in accordance with the service list provided by SCE's letter of October 29, 1979. An affidavit attesting to the fact that distribution has been completed will be provided within ten days of docketing of Amendment 29.

If there are any comments or questions regarding this information, please contact me.

Very truly yours,

K P Baskin

Enclosures

B001
S
1/63

D. The shutdown cooling heat exchangers are sized to remove decay heat at 27-1/2 hours after shutdown based upon a refueling water temperature of 130F and a component cooling water temperature of 95F (both trains operable). The system is designed to attain a refueling temperature of 130F, 27-1/2 hours after shutdown and 212F approximately 5-1/2 hours after shutdown during normal conditions with both trains in operation. Further information on the cooldown times is provided in paragraph 5.4.7.3.

E. The SDCS is placed into operation when the reactor coolant system temperature and pressure are below 350F and 361 lb/in.^{2}g, respectively.

F. Materials are selected to preclude system performance degradation due to effects of short- and long-term corrosion.

G. Components of the SDCS are designed in accordance with the codes and classifications per section 3.2 and paragraph 5.4.7.2.

H. In the event of a single active failure, and to assure availability of the system when required, redundant components are provided. Redundant components are powered from independent emergency power sources (see section 8.3). Instrumentation to assure proper system operation is described in paragraph 5.4.7.2.2. Protection of system redundancy is covered in paragraph 5.4.7.1.3.

I. The system design provides for inspection and testing of components to ensure availability and proper operation.

5.4.7.1.3 Functional Description

The SDCS is shown in figures 6.2-33 and 6.3-1 as a subsystem of the low-pressure safety injection system. 6

The SDCS lineups for post-accident and normal shutdown cooling are shown in section 6.3; figures 6.3-6, 6.3-7, and 6.3-8. 6

During shutdown cooling, reactor coolant is circulated by the low-pressure safety injection (LPSI) pumps through the shutdown cooling heat exchangers to the LPSI headers and returned to the RCS cold legs through the four safety injection nozzles.

The initial cooldown rate is maintained at 75F/h or less. The cooldown rate is manually controlled by adjusting the flowrate through the heat exchangers with throttle valve HV-9316 on the discharge of heat exchangers. A relatively constant total flow rate is maintained by locally adjusting the manual SDC heat exchanger bypass flow control valve FV-0306 as SDC heat exchanger flow is increased or decreased. During initial cooldown the temperature differences for heat transfer are large, thus only a portion of the total shutdown flow is diverted through the heat exchangers. As cooldown proceeds, the temperature differences become less and the flowrate 29

through the heat exchangers is increased. The flow is increased periodically until full shutdown cooling flow is through the heat exchangers. This mode is maintained until the RCS reaches refueling temperature.

A warmup recirculation line is provided in the SDCS to limit thermal stress in the piping and components that would occur if a step change in temperature from ambient to reactor coolant temperature were permitted during system lineup. No credit, however, is taken for warmup in equipment selection.

The SDCS is designed to cool the RCS from 350F and 361 $lb/in.^2g$ to 130F and atmospheric pressure within 24 hours. The cooldown is assumed to commence 3-1/2 hours after shutdown. The system design point is 27-1/2 hours after shutdown with two shutdown cooling heat exchangers and two LPSI pumps in operation.

The RCS can be brought to refueling temperature using one LPSI and one shutdown cooling heat exchanger. However, with the design heat load, the cooldown would be considerably longer than the specified 27-1/2 hour time period. One LPSI pump will provide sufficient flow through the core to maintain the core ΔT at a value less than the full power ΔT(60F).

Provisions are included so that the SDCS may be used to supplement normal spent fuel pool cooling.

29 The SDCS flow control valve HV-9316 can be manually controlled from the control room. To preclude loss of cooling ability in the event of a single active failure, the valve is equipped with a manual handwheel for local operation. A manual bypass valve is also provided for the valve.

Shutdown cooling system components whose design pressure and temperature are less than the RCS design limits are provided with overpressure protection devices. The SDCS suction line is equipped with six isolation valves arranged in parallel pairs. Valves HV-9378, HV-9377, HV-9337 and HV-9339 are located inside containment. Valves HV-9379 and HV-9336 are located outside containment. With this arrangement, a redundant-parallel shutdown cooling path is provided in the event of a single active failure of a valve. Each valve inside containment is provided with an interlock to prevent opening and to initiate automatic closure whenever the RCS pressure exceeds a preset value (see paragraph 5.4.7.2.2). Additional interlocks to prevent SDCS overpressurization are provided on the safety injection tank isolation valves, as described in paragraph 6.3.2.2.1. Both interlocks are discussed further in section 7.6.

To assure availability of the SDCS and to assure positive isolation at the RCS pressure boundary, four independent emergency power supplies are utilized for the combination of six suction line isolation valves.

A pressure relief valve in the SDCS suction line protects the system from overpressurization during system operation when the suction valves are

The LPSI pump design flowrate of 4150 gal/min is based on maintaining a core ΔT (60F) at shutdown cooling initiation 3-1/2 hours after shutdown. The LPSI pump characteristics and the available NPSH are further discussed in subsection 6.2.2, section 6.3, and appendix 3A.

B. Shutdown Cooling Heat Exchangers (SDCHX)

The SDCHX remove core decay heat, RCS sensible heat, and safeguard pump heat during plant cooldown and cold shutdown. The SDCHX are sized to maintain refueling water temperature (130F) with the design component cooling water temperature (95F) at 27-1/2 hours after shutdown.

A conservative fouling factor is assumed, resulting in an additional area margin for the heat exchangers. The SDCHX characteristics for the shutdown cooling mode are given in table 5.4-6.

C. Piping

All SCS piping is austenitic stainless steel. All piping joints and connections are welded except for a minimum number of flanged connections that are used to facilitate equipment maintenance or accommodate component design.

D. Valves

Design pressures and temperatures for the SDCS valves are provided in table 5.4-7.

Manual isolation valves are provided to isolate equipment for maintenance. Throttle valves (FV-0306 and HV-9316) are provided for control of heat exchanger tube side and bypass flow. Throttle valve HV-9316 can be remotely controlled from the control room. During normal plant operation, the air supply to HV-9316 is valved out. Throttle valve FV-D306 must be manually controlled locally. Valve position indication (open-closed lights) are provided in the control room. Check valves in the discharge of the LPSI pumps prevent reverse flow through these pumps during shutdown cooling. 29

A remotely controlled isolation valve is provided on the inlet and outlet of each shutdown cooling heat exchanger. Valve position indication (open-closed lights on the inlet valves, continuous position indication on the outlet valves) is provided in the control room. These valves allow either heat exchanger to be remotely realigned to the containment spray system for containment iodine removal during POST-LOCA shutdown cooling operation. These valves also provide an alternative means of controlling the flow rate through the shutdown cooling heat exchangers. 29

The SDCS suction line is equipped with six remotely-controlled isolation valves in a parallel arrangement, with two parallel pairs

inside containment and one parallel pair outside containment. Valve position indication lights (open/closed) are provided for each valve in the control room.

In addition to normal offsite power, four independent emergency power supplies are provided for the isolation valve combination. This arrangement assures that a single failure of an isolation valve or power supply does not preclude availability of the system or preclude positive isolation at the boundary with the RCS.

Since the SDCS is not designed to accommodate full RCS pressure, isolation of the system suction line is assured by interlocks on

Table 5.4-7
SHUTDOWN COOLING SYSTEM VALVES
DESIGN PRESSURES AND TEMPERATURES (Sheet 3 of 4)

Valve	Valve No.	Design Pressure lb/in.^{2} g	Design Temp. °F
CVCS Shutdown Purification Inlet Isolation Valve	3" - 092-C-105	650	550
Shutdown Cooling Heat Exchangers Inlet Isolation Valves	HV-8152 HV-8153	615 615	400 400
LPSI Header Check Valves	8" - 072-A-552 8" - 073-A-552 8" - 074-A-552 8" - 075-A-552	2485 2485 2485 2485	650 650 650 650
CCS Pump Discharge Isolation Valves	8" - 014-C-406 8" - 012-C-406	615 615	400 400
Shutdown Cooling Heat Exchangers Vent Valves	3/4" - 019-C-376 3/4" - 021-C-376 3/4" - 022-C-376	615 615 615	400 400 400
Shutdown Cooling Heat Exchangers Drain Valves	3/4" - 023-C-376 3/4" - 020-C-376 3/4" - 024-C-376	615 615 615	400 400 400
CSS Header Manual Isolation Valves	8" - 005-C-173 8" - 003-C-173	615 615	400 400
Shutdown Cooling Heat Exchangers Return Line Isolation Valves	HV-8150 HV-8151	615 615	400 400
Refueling Water Storage Jack Return Line Isolation Valve	6" - 162-C-075	615	400

29

29

Table 5.4-7
SHUTDOWN COOLING SYSTEM VALVES
DESIGN PRESSURES AND TEMPERATURES (Sheet 4 of 4)

Valve	Valve No.	Design Pressure lb/in.^{2} g	Design Temp. °F
Spent Fuel Pool Cooling Isolation Valve	8" - 018-C-173	615	400
Shutdown Cooling Heat Exchangers Return Line Sample Line Isolation Valve	3/4" - 205-C-376	615	400

applicable. Valves PSV-9338 and PSV-9363 have a capacity of 5 gal/min each with a setpoint of 2485 lb/in.^{2}g. Valve PSV-9387 has a capacity of 5 gal/min and a setpoint of 435 lb/in.^{2}g.

E. Instrumentation

Operation of the SDCS is controlled and monitored through the use of installed instrumentation. The instrumentation provides the capability to determine heat removal, cooldown rate, shutdown cooling flow, and the capability to detect degradation in flow or heat removal capacity. The instrumentation provided for the SDCS consists of:

1. Temperature measurements - shutdown cooling heat exchanger inlet and outlet temperature and the temperature of the shutdown cooling flow to the low pressure header. All temperatures are indicated in the control room. The shutdown cooling heat exchangers' inlet temperature, and the low pressure header temperatures are recorded to facilitate control of the RCS cooldown rate.

2. Pressure measurements - LPSI header pressure and shutdown cooling heat exchanger inlet pressure. These pressures are indicated in the control room and, when used with the low-pressure pump performance curves, provide an alternate means of measuring system flowrate.

29 3. Total shutdown cooling flowrate is measured by FE-0306 and indicated in the control room.

F. Component Cooling Water System

The component cooling water system provides the heat sink to which the residual heat is rejected. Cooling water flows through the shell side of the shutdown cooling heat exchangers and also functions to cool the shaft seals on the LPSI pumps as they circulate the heated reactor coolant (see section 9.2).

5.4.7.2.4 Applicable Codes and Classifications

Piping	ASME III, Class 1, 2, or 3, as applicable
Pumps and Valves	ASME III, Class 1, 2, or 3, as applicable
Heat Exchangers	Tubular Exchangers Manufacturing Association (TEMA) and ASME III, Class 2 and 3 as applicable

Further information on component codes and classifications is given in section 3.2.

5.4.7.2.5 System Reliability Considerations

29 The SDCS is designed to perform its design function assuming a single failure, as described in paragraph 5.4.7.1.2, items A through C.

To assure availability of the SDCS when required, redundant components and power supplies are utilized. The RCS can be brought to refueling temperature utilizing one of two LPSI pumps and one of two SDCHX. However, with the design heat load the cooldown would be considerably longer than the specified 27-1/2-hour time period.

A loss of instrument air to the shutdown cooling system will not result in a loss of cooling ability. The air-operated shutdown cooling throttling valve is equipped with a hand wheel, which permits adjustment of the valve. In addition, a manual bypass valve is provided for the valve.

The power to the shutdown cooling heat exchanger valves (HV-8150, -8151, -8152, -8153) is locked out during normal operation to preclude inadvertent connection of the shutdown cooling and containment spray systems. Power must be restored prior to the initiation of shutdown cooling. The valves may then be operated remotely to allow alignment of the shutdown cooling heat exchangers to either the containment spray system or the shutdown
29 cooling system.

During post-LOCA operation of the shutdown cooling system, the power to the containment spray isolation valves (HV-9367, -9368) is locked out to preclude a breach of the reactor coolant pressure boundary due to spurious valve opening. Power must be restored if it becomes necessary to operate the containment spray system after post-LOCA shutdown cooling has been initiated.

The air supply to SDC heat exchanger flow control valve HV-9316 is normally valved out to insure that the valve is not inadvertently closed. The air supply is restored prior to SDC initiation.

29 The power supply to the SDC warmup valves is locked out following completion of the warm-up stage of shutdown cooling. This precludes spurious opening of the valves, which could cause the shutdown cooling flow to short circuit through the warm-up line, back to the LPSI pump suction lines.

Inadvertent overpressurization of the SDCS is precluded by the use of pressure relief valves and interlocks installed on the shutdown cooling suction line isolation valves and safety injection tank isolation valves (see section 7.6).

The instrumentation, control, and electric equipment pertaining to the SDCS were designed to applicable portions of IEEE Standards 279-1971 and 308-1971.

In addition to normal offsite power sources, physically and electrically separated and redundant emergency power supply systems are provided to power safety-related components. See chapter 8 for further discussion.

Since the SDCS is essential for a safe shutdown of the reactor, it is a Seismic Category I system and designed to remain functional in the event of a design basis earthquake.

For long-term performance of the SDCS without degradation due to corrosion, only materials compatible with the pumped fluid are used.

Environmental conditions are specified for system components to ensure acceptable performance in normal and applicable accident environments (see section 3.11).

5.4.7.2.6 Manual Actions

The SDCS is a manually aligned and actuated system. Alignment to the shutdown cooling mode is accomplished via a combination of manual/local and remote (from the control room) operated valves. 29

Required manual actions from outside the control room for normal SDCS alignment and operation are listed in table 5.4-8. Position indication is provided in the control room (open-closed lights) for valves 16"-022-C-173, 16"-023-C-173, 14"-015-C-173, 14"-018-C-173, 2"-037-C-329, and 2"-063-C-329 to allow remote verification of the shutdown cooling alignment status. 29

Additional valve actuations required for normal SDCS alignment and operation that are accomplished from the control room are given in table 5.4-9. 29

In addition to the valves mentioned above, both LPSI pumps are activated from the control room. Each pump may also be started via local control.

For the most limiting single active failure, whereby only one SDCHX and one LPSI pump are in operation, the required manual actions are no greater than for normal shutdown cooling operation described above with all SDCS component operable. 29

For post-LOCA operation, locally operated SDC heat exchanger bypass flow control valve FV-0306 will be closed prior to the initiation of SDC. Since the air supply to flow control valve HV-9316 is not safety related, it remains disconnected. HV-9316 can be prepositioned prior to recirculation initiation. The shutdown cooling heat exchanger valves HV-8150 and HV-8151 can also be used to throttle flow to provide adequate shutdown cooling control capability. 29

Table 5.4-8
REQUIRED MANUAL ACTIONS ACCOMPLISHED OUTSIDE THE CONTROL ROOM

Valve No.	Valve	Operation
14"-018-C-173	Shutdown cooling line isolation	Open
16"-023-C-173	Shutdown cooling isolation	Close
16"-022-C-173	Shutdown cooling isolation	Close
2"-099-C-376	RWT return line containment isolation(a)	Open/Close
6"-162-J-075	RWT return line isolation(a)	Open/Close
FV-0306	SDCS bypass flow control valve	Throttle
2"-037-C-329	LPSI pump miniflow isolation valve	Close
2"-063-C-329	LPSI pump miniflow isolation valve	Close
HY-9316B	Air supply and vent valves to HV-9316	Open/Close

29

a. Valves required for reducing pressure in the SIT's under normal operation (see section 6.3)

Table 5.4-9
REQUIRED VALVE ACTUATIONS ACCOMPLISHED FROM THE CONTROL ROOM (Sheet 1 of 2)

Valve No.	Valve	Operation
HV-9337	Shutdown cooling suction line isolation	Open
HV-9339	Shutdown cooling suction line isolation	Open
HV-9377	Shutdown cooling suction line isolation	Open
HV-9378	Shutdown cooling suction line isolation	Open
HV-9336	Shutdown cooling suction line isolation	Open
HV-9379	Shutdown cooling suction line isolation	Open
HV-9353 or HV-9359	Warmup bypass	Open/Close
HV-9322	LP header injection	Open
HV-9325	LP header injection	Open
HV-9328	LP header injection	Open
HV-9331	LP header injection	Open
HV-9306	Miniflow isolation	Close
HV-9307	Miniflow isolation	Close
HV-9347	Miniflow isolation	Close
HV-9348	Miniflow isolation	Close
HV-9316	SDCHX flow control	Throttle
HV-9340	SIT isolation	Open/Close
HV-9350	SIT isolation	Open/Close

29

a. Valves required for reducing pressure in the SIT's under normal operation (see section 6.3)

b. Valves required for alternate means of SIT pressure reduction under normal operation (see section 6.3). Valves required for reducing pressure in the SIT's under accident conditions (see section 6.3)

5.4.7.3 Performance Evaluation

The design point of the SDCS is taken at 27-1/2 hours after plant shutdown. At this point, the heat load design basis is to maintain the 130F refueling temperature with 95F component cooling water. Two shutdown cooling heat exchangers plus two LPSI pumps were assumed to be in operation at the design flow of 4150 gal/min each. The SDCHX size is determined at this point since it requires the greatest heat transfer area due to the relatively small 6
ΔT between primary fluid and component cooling water.

The design heat load at 27-1/2 hours is based on decay heat at 27-1/2 hours assuming infinite reactor operation. Additional energy input to the RCS from two LPSI pumps running at design flowrate of 4150 gal/min each was also included; no credit is taken for component energy losses to the external environment.

For the cooldown process from the shutdown cooling initiation temperature of 350F to the refueling temperature of 130F, the heat load utilized is comprised of the instantaneous decay heat, LPSI pump heat input, and sensible heat of the primary and secondary liquid and metal masses. Metal mass is assumed to be steel with a specific heat of 0.12 Btu/lb ^{o}F. The temperature of the component cooling water to the SDCHX is taken as 120F initially, gradually decreasing to 95F, when 130F refueling temperature is arrived at.

At each time interval in the cooldown, an iterative process is utilized to analyze transient performance whereby the permissible heat removal is established by balancing the available heat load with the SDCHX heat removal capability. Maximum cooldown rate is limited to $\leq$75F/h throughout the cooldown. The normal cooldown is shown in figure 5.4-6.

With the most limiting single active failure in the SDCS, RCS temperature can be brought to 212F in approximately 7.5 hours and to the refueling temperature of 130F in approximately 155 hours following shutdown using only one LPSI pump and one SDCHX. The cooldown curve is shown in figure 5.4-7.

To prevent damage to both LPSI pumps in the event of a pump isolation valve closure, the following is provided:

Motor-operated valves HV-9337, HV-9339, HV-9377, HV-9378, HV-9336, and HV-9379 in the shutdown cooling suction line are arranged in parallel paths and are all maintained open during SDCS operation. In the event of a power supply failure, the valves fail-as-is.

In addition, four independent emergency power supplies are provided for the valve combination. With the arrangement, a single active failure or inadvertent closure associated with any one of the above valves will not result in total isolation of the LPSI pump suction.

Pneumatically operated shutdown cooling flow control valve HV-9316 is designed to fail open upon loss of air or power. The availability of either the SDC heat exchanger flow path or the SDC heat exchanger bypass flow path insures that the LPSI pumps will not be deadheaded. 29

29 The four LPSI header valves HV-9322, HV-9325, HV-9328, and HV-9331 in the LPSI pump discharge piping are paired to two separate emergency power supplies and fail-as-is on loss of power. With this arrangement, isolation of the pump discharge path is precluded in the event of a single active failure or an inadvertent closure related to these valves.

LPSI pump isolation due to hand-operated valves in the pump suction and discharge paths is prevented by locking those valves in the appropriate position during SDCS alignment and operation.

A failure modes and effects analysis for the SDCS can be found in table 5.4-5. The analysis demonstrates that the SDCS can withstand any single active failure and still perform its design function. The analysis is based on the following assumptions:

A. One active failure of a component or a single operator error is assumed to occur in the system.

B. The analysis considers only failures that occur during the time period of SDCS operation.

C. Relief and check valve failures are not considered credible failures.

D. Failure to respond to an external signal is considered an active failure.

5.4.7.4 Preoperational Testing

Preoperational tests are conducted to verify proper operation of the SDCS. The preoperational tests include testing of the automatic flow control, verification of adequate shutdown cooling flow, and verification of the operability of all associated valves. In addition, a preoperational hot functional performance tests is made on the installed shutdown cooling heat exchangers.

For availability of the SDCS, components of the systems are periodically tested as part of the safety injection system testing, as described in section 6.3. The system and component tests, together with shutdown cooling heat exchanger thermal performance data taken during refueling, are sufficient to demonstrate the continued operability of the SDCS.

In addition to flow tests, the SDCS also undergoes a series of preoperational and inservice hydrostatic tests. Preoperational hydrostatic tests are conducted in accordance with Section III of the ASME Boiler and Pressure Code while inservice hydrostatic tests are carried out as required by Section XI of the ASME Code.

D. High-Pressure Safety Injection Header Thermal Relief Valves

These values are sized to protect the HPSI lines against the pressure developed due to a temperature increase: They discharge into the penetration area sump. The set pressure is 1900 lb/in.^{2}g with a capacity of 5 gal/min. | 21

E. High-pressure Safety Injection Header Relief Valve

The HPSI header to which the charging pumps discharge is protected from the charging pumps discharge pressure by this valve. It discharges into the penetration area sump. The set pressure is 2735 lb/in.^{2}g with a capacity of 160 gal/min. | 27

F. High-Pressure Safety Injection Pump Suction Relief Valves

These valves protect the pump suction line to each HPSI pump from overpressurization due to check valve leakage in the discharge piping. The set pressure is 110 lb/in.^{2}g. | 29

6.3.2.2.5.2 Actuator-Operated Throttling and Stop Valves. The position of each valve on loss of actuating signal or power supply (failure position) is selected to ensure safe operation. System redundancy is considered when defining the failure position of any given valve. Valve position indication is provided at the main control panel. A locking type control switch on the main control panel and/or manual override handwheel is provided where necessary for efficient and safe plant operation.

Orifice plates upstream or downstream of HPSI and LPSI valves (HV-9322, 9323, 9324, 9325, 9326, 9327, 9328, 9329, 9330, 9420, and 9434) are field adjusted during pre-operational flow tests to prevent the safety injection pumps from exceeding runout flow during emergency operation. To prevent inadvertent actuation, the hot leg injection valves have power locked out in the closed position during normal operation and post-LOCA prior to hot leg injection. | 21

6.3.2.3 Applicable Codes and Classifications

The codes and classifications applicable to the ECCS components are listed in section 3.2.

6.3.2.4 Materials Specifications and Compatibility

See section 6.1.

6.3.2.5 System Reliability

6.3.2.5.1 Safety Injection Tanks

The safety injection tanks containing borated water pressurized by a nitrogen cover, constitute a passive injection system, because no outside operation action or electrical signal is required for operation. Each tank is connected to its associated reactor coolant cold leg by a separate line

Table 6.3-3
POST-LOCA INSTRUMENTATION (Sheet 3 of 3)

Item	Post-LOCA Function
Shutdown cooling suction isolation valves RCS pressure interlocks	Prohibit the opening of the isolation valves when RCS pressure is above SDCS design pressure. Initiate shutdown cooling.
Shutdown cooling heat exchanger inlet and outlet isolation valve handswitches HS-8150-1, HS-8150-2, HS-8152-1, HS-8153-2	Control of shutdown cooling heat exchangers for post-LOCA shutdown cooling.
LPSI pump suction cross connect valve position indication ZL-9298-1, ZL-9299-2	Indicate position of valves 14"-015-C-173 and 14"-018-C-173.
LPSI pump suction from RWST isolation valve position indication ZL-9296-1, ZL-9297-2	Indicate position of valves 16"-022-C-173 and 16"-023-C-173.
LPSI pump miniflow valve position indication ZL-9295-1, ZL-9287-2	Indicate position of valves 2"-037-C-329 and 2"-063-C-329.

29

post-LOCA. The margin provided for the prevention of boric acid accumulation by the net core flushing flow over the minimum flow of 20 gal/min is shown in figure 6.3-11. The time at which all hot leg steam entrainment of injection water terminates has been calculated to be 1.4 hours post-LOCA.

17 Therefore, the 2 hour cold/hot side injection time is initiated after any potential for hot leg entrainment has been terminated and more than 7 hours prior to the time at which boric acid precipitation might occur.

The small break LTC plan applies to those break sizes for which the RCS refills before all of the auxiliary feedwater is used. The small break analysis determined that 7.6 hours is the minimum time required to exhaust all of the auxiliary feedwater during cooldown of the RCS. The plot of break area versus time to refill the RCS in figure 6.3-12 determines that the .02 ft^2 break is the largest that can satisfy the small break criteria with adequate margin. Therefore, the .02 ft^2 break is the largest for which the small break LTC plan is applicable.

These results demonstrate that breaks as large as .02 ft^2 will be able to use SDC for the long-term cooling and flushing of the core. The LTC analysis determined that the LTC large break procedures can flush the core for break sizes down to .005 ft^2. This overlap in break sizes for which either the large or small break procedures can be used is illustrated in figure 6.3-13.

At 6 hours post-LOCA, the operator decides which LTC procedure is appropriate according to the RCS pressure. If the pressure is below 300 $lb/in.^2a$, the large break procedures are initiated. If above 300 $lb/in.^2a$, then the break is small enough to initiate SDC. A plot of RCS pressure versus break size is shown in figure 6.3-14. This plot indicates that the decision point pressure of 300 $lb/in.^2a$ fits well within the break size range of .005 to .02 ft^2 for which both large and small break procedures are functional.

6.3.3.5 Interconnections with Other Systems

The safety injection water flows to the reactor vessel through a safety injection nozzle on each of the four RCS cold leg pipes. This arrangement 9 provides four separate flow paths to the reactor. In addition, high pressure hot leg injection capability is provided, via the SDC suction line and drain line in the hot legs, in order to supply hot leg injection (simultaneous with cold leg injection) during long-term ECCS operation.

During shutdown cooling, the LPSI pumps take suction from the RCS via the shutdown cooling suction line. To prevent ECCS flow from recirculating 29 through the shutdown cooling warmup valves (HV-9353, -9359), the power to these valves is locked out during normal operation. See subsection 5.4.7.

A connection is provided from the discharge side of the CVCS charging pumps to the HPSI header. Its primary purpose is to allow testing operability of 6 the safety injection check valves upstream of the RCS safety injection nozzles when the RCS is pressurized. The connection can also be used to correct boron concentration in the safety injection tanks, and it provides an alternate injection path for the charging pumps.

Question 212.65

If valve 2FV0306 were to fail in the closed position during shutdown cooling due to a failure of the instrument air system, the RCS might be cooled at a rate of excess of the Tech. Spec. limits. State the operator actions as they would appear in the Emergency Procedures to terminate this problem. List the items which would alert the operator to this problem. State the time frame within which the operator must act in order to remain within Tech. Spec. limits. What would be the maximum cooldown rate for one-half hour, one-quarter hour, or for five minutes?

Response

SDCHX bypass flow control valve FV-0306 is a locally operated manual valve. If the valve were to fail closed due to mechanical binding, its bypass valve 14"-153-C-173 could be opened. Total flow would be limited by throttling the LPSI header valves. 29

Reference

See revised FSAR subsection 5.4.7.

Question 212.66

In the event of loss of instrument air (possibly due to a seismic event) while operating in a shutdown cooling mode, valves 2FV0306 and 2HV9316 would fail closed. Closure of these valves would produce a loss of shutdown cooling. State the Emergency Procedures used to terminate this event. State the time frame within which the operator must act in order to remain within Tech. Spec. limits. Provide the sequence of events with respect to time which will alert the operator to a loss of cooling.

Response

The failure mode of HV-9316 has been changed to fail open. Valve FV-0306 is a locally operated manual valve. In the event of a loss of instrument air supply, the oprator would receive early indication by the following in the control room:

1. Instrument air alarm
2. Position indication of HV-9316
3. Shutdown cooling flow indication - FI-0306
4. Shutdown cooling temperature indication - TI-303-1, TI-303-2, TI-351-1, TI-351-2

SDC operation for removal of RCS decay heat can begin as early as 3.5-4 hours following initiation of plant shutdown from power. If this event occurs coincident with the initiation of SDC, some increase in the cooldown rate is anticipated. The increase can be controlled by limiting total cooling flow with header valves HV-9322, -9325, -9328, and -9331. If this event occurs later in the shutdown cooling process, the cooldown rate diminishes, but RCS heat removal remains adequate. With the indications noted above, the operator has time to prepare for manual control of SDCHX flow via the handwheel provided on flow control valve HV-9316, and can restore the cooldown rate. The air receivers and backup N_2 supply to the instrument air system, which provides instrument air to HV-9316, may provide continued operation while the operator prepares for manual control. 29

As an additional margin of safety, the operator can stabilize the plant in a hot standby or hot shutdown condition by reinitiating steam generator dumping. This procedure would involve the turbine bypass system and condenser, if available, or the atmospheric dump valves.

Reference

See FSAR sections 5.4.7 and 9.3.

Question 212.67

Bypass valves 14"-153-C-173 or 14"-079-C-173 must remain partially open during shutdown cooling in order to provide protection for the LPSI pumps. Provide a description of how this protection is to be provided.

Response

Bypass valves 14"-153-C-173 and 14"-079-C-173 are locked closed. FV-0306, which is in parallel to 14"-153-C-173, is a locally operated manual valve. Its closure, and possible deadheading of the pumps will be precluded by procedure. HV-9316, which is parallel to 14"-074-C-173, is pneumatically operated and is designed to fail open on loss of air or power. Operating procedures, parallel flowpaths, and the failure position of HV-9316 insures that the pumps are protected. 29

Reference

See revised FSAR paragraph 5.4.7.3, table 5.4-5, and figure 6.3-8.

Question 212.68

GDC 19 implies that the RHR system must have the actions of its pertinent components controlled in the main control room. All the valves listed in Table 5.4-8 does not meet GDC 19. Modify your design so that you are in conformance with GDC 19.

Response

The SDCS design is being modified to allow the system to be aligned and completely operated from the control room. These modifications are to be completed on Unit 2 during the first refueling. On Unit 3, these modifications are to be completed prior to fuel load. 29

Reference

See the response to NRC Question 212.164.

Question 212.76

The staff requires that indication of the status of valves 16"-022-C-173 and 16"-023-C-173 be displayed in the control room. Modify your design accordingly.

Response

The status of valves 16"-022-C-173 and 16"-023-C-173 is indicated in the control room by ZL-9296-1 and ZL-9297-1, respectively.

29

Reference

See FSAR subsections 5.4.7 and 6.3.3.

Question 212.156

LPSI Valve Position Indication--The staff requires that position indication in the control room be provided for LPSI pump suction valves 16"-022-C-173 and 16"-023-C-173.

Response

Position indication in the control room has been provided for both of these valves. ZL-9296-1 has been added to 14"-022-C-173, and ZL-9297-2 has been added to 14"-023-C-173. 29

Reference

See FSAR subsection 6.3.3.

Table 212.157-2

SEISMIC CATEGORY I CONTROLS FOR COOLDOWN OPERABILITY

Instrumentation and Controls	Location
LP safety injection pumps, (P-015, P-016) handswitches	Control Room
LP safety injection header throttle valves (HV-9322, -9325, -9328, -9331) handswitches	Control Room
SIT isolation valves (HV-9340, -9350, -9360, -9370) handswitches	Control Room & Local
SIT nitrogen vent valves (HV-9345, -9355, -9365, -9375) handswitches	Control Room & Local
SDC suction isolation valves RCS pressure interlocks (PT-0103-1, -0104-2, 0105-3, 0106-4)	Control Room
Mini-flow line stop valves (HV-9347, -9348, -9306, -9307) handswitches	Control Room
SDC suction line isolation valves (HV-9337, -9339, -9377, -9378) handswitches	Control Room & Local
Backup Pressurizer Heaters (2 groups of 200 KW)	Control Room & Local
AFW valve and pump controls	Control Room
Atmospheric dump valve controls (HV-8419, -8421)	Control Room & Local
Charging and Boric Acid Makeup Pump controls	Control Room & Local
Charging isolation valve (HV-9200) handswitch	Control Room & Local
Shutdown Cooling Heat Exchanger to LPSI Header Valve (HV-9316)	Manual/Local
Shutdown cooling heat exchanger valves (HV-8150, -8151, -8152, -8153) handswitches	Control Room
LPSI pump suction from RWST isolation valves (16"-022-C-173, 16"-023-C-173) position indication	Control Room
LPSI pump suction cross connect valves (14"-015-C-173, 14"-018-C-173) position indication	Control Room
LPSI pump miniflow valves (2"-037-C-329, 2"-063-C-329) position indication	Control Room

21

29

Question 222.44 Control System Failures

The analyses reported in chapter 15 of the FSAR are intended to demonstrate the adequacy of safety systems in mitigating anticipated operational occurrences and accidents. Both Congress and ACRS have raised an issue on this area. Commissioner Ahearne has responded to Congress regarding this issue (Refer to attachment to this enclosure) and part of his response re-ferred to control system reviews to be performed in connections with OL licensing.

Based on the conservative assumptions made in defining these chapter 15 design-basis events and the detailed review of the analyses by the staff, it is likely that they adequately bound the consequences of single control sys-tem failures.

To provide assurance that the design basis event analyses adequately bound other more fundamental credible failures you are requested to provide the following information:

(1) Identify those control systems whose failure or malfunction could seriously impact plant safety.

(2) Indicate which, if any, of the control systems identified in (1) receive power from common power sources. The power sources considered should include all power sources whose failure or malfunction could lead to failure or malfunction of more than one control system and should extend to the effects of cascading power losses due to the failure of higher level distribution panels and load centers.

(3) Indicate which, if any, of the control systems identified in (1) receive input signals form common sensors. The sensors considered should include, but should not necessarily be limited to, common hydraulic headers or impulse lines feeding pressure, temperature, level or other signals to two or more control systems.

(4) Provide justification that any simultaneous malfunctions of the control systems identified in (2) and (3) resulting from failures or malfunctions of the applicable common power source or sensor are bounded by the analyses in chapter 15 and would not require action or response beyond the capability of operators or safety systems.

Response

(1) The failures or malfunctions of the following control systems may impact plant safety.

29

- Feedwater control system (FWCS)

- Turbine generator control system (TGCS)
- Steam bypass control system (SBCS)
- Boron control system (BCS)
- Reactor regulating system (RRS)
- Control element drive mechanism control system (CEDMCS)
- Pressurizer pressure control system (PPCS)
- Pressurizer level control system (PLCS)

(2) The following common power sources have been identified as supplying power to the control systems listed in Item (1):

a. 208/120 V-ac (Volts Alternate Current) distribution panel 2Q0612:
Supplies power to CEDMCS, BCS, TGCS, and RRS

b. 208/120 V-ac distribution panel 2Q065:
Supplies power to CEDMCS, FWCS, SBCS, TGCS and the RRS

29

c. 480 V MCC (Motor Control Center) distribution panel BO:
Supplies power to 208/120 V-ac distribution panel 2Q0612

d. 480 V MCC distribution panel 2BX:
Supplies power to 208/120 V-ac distribution panel 2Q065

e. 125 V-dc (Volts Direct Current) vital distribution panel 2D1P1:
Supplies power to PLCS and PPCS

f. 125 V-dc vital distribution panel 2D2P1:
Supplies power to PLCS and PPCS

(3) The common sensors and common instrument taps/lines which have been identified for the control systems listed in item (1) are provided in table 222.44-1.

Table 222.44-1

SENSORS AND INSTRUMENT LINES/TAPS FOR CONTROL SYSTEMS (Sheet 1 of 2)

Tap Location	Instrument	System Input
Pressurizer (steam space)	2PT-0100-X (Pressure)	RRS, PPCS, SBCS
	2LT-0110-1 (Level - Upper Tap)	PLCS
Pressurizer	2PT-0100-Y (Pressure)	RRS, PPCS, SBCS
	2LT-0110-2 (Level - Upper Tap)	PLCS
Pressurizer	2LT-0110-1 (Level - Lower Tap)	PLCS
Pressurizer	2LT-0110-2 (Level - Lower Tap)	PLCS
S/G No. 1	2LT-1105 (Level - Upper Tap)	FWCS
S/G No. 1	2LT-1105 (Level - Lower Tap)	FWCS
S/G No. 1	2LT-1111 (Level - Upper- Tap)	FWCS
S/G No. 1	2LT-1111 (Level - Lower Tap)	FWCS
S/G No. 2	2LT-1106 (Level - Upper Tap)	FWCS
S/G No. 2	2LT-1106 (Level - Lower Tap)	FWCS
S/G No. 2	2LT-1121 (Level - Upper Tap)	FWCS
S/G No. 2	2LT-1121 (Level - Lower Tap)	FWCS
Reactor Vessel	TY-111X (T_{hot})	RRS
	TY-111Y (T_{cold})	RRS
	TY-121X (T_{hot})	RRS
	TY-121Y (T_{cold})	RRS
	JI-010 (reactor power)	RRS

29

Table 222.44-1 (cont'd)

SENSORS AND INSTRUMENT LINES/TAPS FOR CONTROL SYSTEMS (Sheet 2 of 2)

Tap Location	Instrument	System Input
Main Steam Line	FT-1011 (Flow)	FWCS, SBCS
Main Steam Line	FT-1021 (Flow)	FWCS, SBCS
Main Steam Line	PIT-8239 (Steam Hdr Pres)	SBCS
Main Steam Line	PIT-8241 (Steam Hdr Pres)	SBCS
Feedwater Line	FT-1111 (Flow)	FWCS
Feedwater Line	FT-1121 (Flow)	FWCS
Boric Acid Makeup Tank A	2LT-0206 (Level)	BCS
Boric Acid Makeup Tank B	2LT-0208 (Level)	BCS

29

(4) 1. Impact of Loss of Common Power Sources

The control systems identified in (1) that receive power from common power sources are identified in (2). The effect of losing the power sources and an evaluation of plant response are provided below. The results of this evaluation provide justification that any simultaneous malfunctions of control systems identified herein, resulting from common power supply malfunctions are bounded by the analyses of chapter 15 and/or would not require action or response beyond the capability of operators or safety systems.

a. Loss of 120 V-ac from Distribution Panel 2Q0612

29 This power loss will impact the control element drive mechanism control system (CEDMCS), the boron control system (BCS), the turbine-generator control system (TGCS), and the reactor regulating system (RRS). The loss of power to the CEDMCS will not cause the CEAs to drop, since the CEDMCS is also powered by distribution panel 2Q065. The BCS will not be completely lost. That is, the boric acid flow transmitter will lose power, but the reactor makeup water flow controller will be unaffected. The turbine generator control system will not lose power, since it is also powered by panel 2Q065. The RRS will lose power if the selector switch is on the channel powered by this distribution panel. Otherwise, it will be unaffected as the switch will be on the other channel powered by distribution panel 2Q065. For the case of a power loss, the regulating group CEAs will remain in their position prior to the power loss.

Evaluation of Plant Response:

The loss of the CEDMCS, BCS, TGCS, and RRS due to loss of 120 V-ac from power panel 2Q0612 will not seriously impact plant safety. The CEDMCS and TGCS are redundantly powered from two distribution panels, and only loss of power to the RRS and BCS may have an impact on plant operation. The loss of power to the RRS may result in inability to follow turbine load transients. Thus, in the absence of operator action, the reactor will eventually trip (on high or low pressurizer pressure). However, the operator will be alerted to an abnormal behavior by means of alarms and/or indications in the control room (e.g., pressurizer pressure, core temperature, secondary system pressure). At this time, the operator may choose to switch to the redundant channel for correct operation of the

RRS. The loss of power to the boric acid flow transmitter can be bypassed by the operator by providing borated water directly to the charging pumps or by aligning the refueling water tank to charging.

As indicated, the power loss to the RRS and the BCS may result in a heat removal imbalance between the primary and secondary sides, and a reduction in the boron concentration in the reactor coolant. The analysis of the CVCS malfunction, inadvertent boron dilution, in the FSAR paragraph 15.4.1.4 bounds the above scenario. The analysis in this section assumes all three charging pumps to be on, and the demineralized water supply system aligned to supply water directly to the charging pump suction. The operator is alerted to the event by means of alarms (e.g., high pressurizer pressure and level), and can take necessary mitigating actions.

b. Loss of 120 V-ac from Distribution Panel 2Q065

This power loss will impact the control element drive mechanism control system (CEDMCS), the feedwater control system (FWCS), the steam bypass control system (SBCS), the turbine generator control system (TGCS), and the reactor regulating system (RRS). As indicated earlier, redundant power is supplied to the CEDMCS and TGCS from panel 2Q0612. The FWCS of both steam generators will be impacted by loss of power from panel 2Q065. Additionally, the steam bypass control will be lost. The RRS may also lose its ability to follow small turbine load transients due to this power loss depending on the position of the selector switch. 29

Evaluation of Plant Response:

The inability of the RRS to follow small turbine load transients has been previously discussed. The consequences of loss of power to the FWCS and SBCS will most probably be a reactor trip on either high pressurizer pressure or low steam generator level. Automatic actuation of the auxiliary feedwater system and opening of the main steam safety valves, if there is no operator action, will relieve the high secondary system pressure resulting from the primary to secondary heat removal imbalance. Upon operator action, the atmospheric dump valves and the auxiliary feedwater will be employed to control RCS heat removal.

The analysis of the loss of condenser vacuum (LOCV) event provided in the FSAR paragraph 15.2.1.3 assumes a loss of feedwater flow and unavailability of the SBCS on turbine trip. The primary and secondary system pressures increase rapidly for this event until the auxiliary feedwater is actuated on low SG level and the main steam safety valves are opened on high steam generator pressure. Susbequently, the atmospheric dump valves are opened when the operator takes manual actions to control RCS

heat removal. Radiological releases and RCS pressure increase are maximized for this event. The consequences of a power loss to the RRS, FWCS, and SBCS would be no more limiting than those for the LOCV event. Therefore, the FSAR analysis for this event bounds the consequences of a power loss to these control systems.

c. Loss of 480 V MCC Distribution Panel BO

The impact of losing this motor control center (MCC) is similar to the loss of 120 V-ac from panel 2Q0612, since power panel 2Q0612 receives power from this MCC.

Evaluation of Plant Response:

The plant response for loss of power panel 2Q0612 applies.

d. Loss of 480 V MCC Distribution Panel 2BX

The impact of losing this MCC is similar to the loss of 120 V-ac from power panel 2Q065, since panel 2Q065 receives its power from this MCC.

Evaluation of Plant Response:

The plant response for loss of power panel 2Q065 applies.

29 e. Loss of 125 V-dc Distribution Panel 2D1P1

This power loss will impact the pressurizer level control system (PLCS), and the pressurizer pressure control system (PPCS). The PLCS and PPCS will lose control power, only if the selector for each switch is on that channel. Otherwise, both control systems will be unaffected as the selector for each switch will be on the other channel (2D2P1).

If power is lost to the PLCS, the letdown control valve will go to its fail closed position and the charging pumps will remain powered and available for manual control. If power is lost to the PPCS, the pressurizer spray valve will go to its fail closed position and the pressurizer heaters will remain powered and available for manual control. Additionally, the low-low level automatic cut-off of the pressurizer heaters will lose control power. Secondary system pressure reduction and RCS heat

removal can be accomplished by means of the SBCS, the FWCS, and the condenser, or the atmospheric dump valves (manual control from the control room for one ADV and manual local control for the other).

Evaluation of Plant Response:

The loss of PLCS and PPCS will not seriously impact plant safety. The reactor could operate for a time without operator action before a trip (most probably on high pressurizer pressure). The operator can take necessary mitigating actions prior to a reactor trip based on indications in the control room. These include the high pressurizer pressure indication and the high pressurizer level indication. Manual control of the charging pumps, pressurizer heaters, and auxiliary sprays are available to the operator to mitigate the consequences of this power loss. Additionally, he can select the other available channel (power supply from Panel 2D2P1) for each of the control systems (PLCS and PPCS) affected.

f. Loss of 125 V-dc Distribution Panel 2D2P1:

The impact of losing power supply to this panel is similar to the loss of 125 V-dc from panel 2D1P1.

Evaluation of Plant Response:

The conclusions for the loss of 125 V-dc from panel 2D1P1 also apply to this scenario. 29

(4) 2. Impact of Failure in Common Sensors

Description of the effect of malfunctions of the common sensors identified in table 222.44-1 on the control systems are provided below. Additionally, an evaluation of plant response and backup system availability are also provided. Prudent engineering judgement based on knowledge of system design and transient analysis was used to develop these descriptions. The results of this evaluation provide justification that any simultaneous malfunctions of control systems identified herein, resulting from common sensor malfunctions are bounded by the analyses of chapter 15 and would not require action or response beyond the capability of safety systems or operators.

a. Malfunction of Pressurizer Pressure Signal to RRS, SBCS, and PPCS

a.1 Pressurizer Pressure Signal Fails Low to RRS, SBCS, and PPCS

If a malfunction causes a low pressurizer pressure signal to be transmitted, the pressurizer heaters will be turned on, and the pressurizer sprays will be shutoff. The pressurizer pressure is only a compensating input to the RRS, which employs the turbine load index signal to effect a CEA motion. Therefore, the regulating group CEAs will not be withdrawn or dropped due to a low pressurizer pressure signal. Also, the SBCS will not be impacted since the pressurizer pressure input is employed as a "bias" signal for this system.

Evaluation of Plant Response:

The effect of turning on the pressurizer heaters would be an increase in the RCS pressure. The reactor would eventually trip on high pressurizer pressure, if the operator did not take any mitigating actions. The operator could de-energize the heaters manually, and control the pressure with the charging and letdown systems and auxiliary sprays. Should the reactor not trip, because the appropriate setpoints were not reached by the affected parameter (pressure) a new steady state operational plateau would be reached. Operator action could then maintain the reactor at power until the sensor could be repaired.

29

The scenario described above is bounded by the loss of condenser vacuum (LOCV) event analysis provided in the FSAR paragraph 15.2.1.3. This analysis assumes a loss of feedwater flow and unavailability of the SBCS. The above scenario would cause a primary to secondary heat removal imbalance and a RCS pressure rise no more limiting than the LOCV. Radiological consequences and RCS pressure increase are maximized for the LOCV event and remain well within the acceptance criteria.

a.2 Pressurizer Pressure Signal Fails High to RRS, SBCS, and PPCS

If a malfunction causes a high pressurizer pressure signal to be transmitted, the pressurizer sprays would come on and the pressurizer heaters would be de-energized. The RRS will not adjust the regulating group CEAs in response to the high pressurizer pressure signal, since this is only a compensating input to this system. Additionally, the SBCS will not modulate the turbine bypass valves, since the pressurizer pressure signal is employed as a "bias" signal for determining the extent of the valve modulation required.

Evaluation of Plant Response:

The reactor would trip on a low pressurizer pressure setpoint and a SIAS may result. The operator would close the spray valves and use the charging and letdown systems and auxiliary spray to control RCS pressure. Should the reactor not trip due to affected parameters (e.g., pressurizer pressure) not reaching the setpoints, a new steady state operational plateau would be reached. Operator actions, as required, could maintain the reactor at power until the sensor could be repaired.

The above scenario is bounded by the analysis presented in FSAR paragraph 15.6.3.4 for the inadvertent opening of a pressurizer safety valve. RCS depressurization is more rapid for this event. For this event, the reactor trips on a low pressurizer pressure trip setpoint, and no fuel pins experience a DNBR less than 1.19, thus, preventing any violation of the fuel thermal limits. Additionally, there are no event related offsite doses since the integrity of the primary and secondary system is maintained.

b. Malfunction of Main Steam Flow Signal to FWCS and SBCS

b.1 Main Steam Flow Signal Fails Low to FWCS and SBCS

If a malfunction causes a low steam flow signal to be transmitted, the FWCS will reduce the feedwater flow. The SBCS will not open the turbine bypass valves, since the steam flow rate is perceived by this control system as being smaller than what can be accommodated by the turbine. 29

Evaluation of Plant Response:

The mismatch between feedwater flow and turbine demand may produce a reactor trip on either a high pressurizer pressure or low steam generator level. The auxiliary feedwater system and manual control of the SBCS (and/or atmospheric dump valves) is available to achieve a stabilized plant condition. The loss of condenser vacuum (LOCV) event described in the FSAR paragraph 15.2.1.3 bounds this scenario, as it results in a more severe secondary side transient prior to reactor trip on high pressurizer pressurizer.

b.2 Main Steam Flow Signal Fails High to FWCS and SBCS

If a malfunction causes a high steam flow signal to be transmitted, the FWCS will increase the feedwater flow and the SBCS may open the turbine bypass valves, due to its perception of a high steam flow through the turbine.

Evaluation of Plant Response:

The mismatch between feedwater flow and turbine demand may result in an increase in the steam generator level and pressure. The operator could manually control the FWCS and the SBCS based on steam generator level and pressure indications in the control room. Should the operator not take action, a high steam generator level signal would close the feedwater regulating valves and trip the turbine. A reactor trip on turbine trip or high steam generator level would follow with actuation of auxiliary feedwater on steam generator low level signal. Auxiliary feedwater and manual operation of the SBCS (and/or atmospheric dump valves) provide a mechanism for RCS heat removal to stabilize the plant.

The increase in feedwater flow (with a loss of offsite power) event analyzed in the FSAR paragraph 15.1.2.2 bounds the above scenario. This analysis assumes maximum increase in feedwater flow due to a failure in the FWCS. This maximizes the increased heat removal aspects of the transient, and, therefore, results in a more adverse fuel performance transient. A turbine trip signal is generated on a high steam generator level and no credit is taken for the SBCS so that steam is released through the main steam safety valves and the ADVs.

(4) 3. Impact of Failure in Common Instrument Lines/Taps

Table 222.44-1 identifies the instrument lines/taps that feed the sensors for the control systems identified in (1) above. This table has been reviewed and common
29 instrument lines/taps feeding sensors of these control systems were identified. Only the pressurizer pressure snesors (2PT-0100-X, 2PT-0100-Y) and the pressurizer level sensors (2LT-0110-1, 2LT-0110-2) are impacted by the common instrument line/tap failure. The malfunctions of these sensors, do to this failure may affect the performance of the RRS, SBCS, PPCS, and PLCS.

a. Evaluation of Pressure and Level Signals Failing Low Due to Instrument Tap Damage on Plant Response

This event can only be caused by the unlikely occurrence of a broken process sensing line coincident with rupture of the level transmitter diaphram. Nevertheless, the following analysis is provided.

If the failure causes a low pressure and level signals to be transmitted, the pressurizer heaters would turn on and the pressurizer sprays would decrease flow. The PLCS would decrease letdown flow and increase charging flow. The RRS will not adjust the CEAs in response to a low pressurizer pressure signal due to reasons indicated earlier.

The low pressurizer pressure input to the SBCS would not cause the turbine bypass valves to open, since a

low primary pressure would indicate overcooling of the primary. Due to increased charging flow and actuation of the pressurizer heaters, the reactor may trip on high pressurizer pressure. The operator has safety grade instrumentation from which to evaluate the event progress. Manual control of charging, auxiliary sprays, and atmospheric dump valves will bring the plant to a stable condition, without the use of the PLCS, the PPCS and the SBCS. The CVCS malfunction (PLCS malfunction) event described in FSAR paragraph 15.5.2.1 bounds this scenario.

b. Evaluation of Pressure and Level Signals Failing High Due to Instrument Tap Damage on Plant Response

This event is considered unlikely since a process sensing line break causes pressure to fail low and a perfect line crimp would not in itself result in a high pressure. Nevertheless, the following analysis is provided:

If the failure causes a high pressure and level signals to be transmitted then the pressurizer heaters would de-energize and the sprays would increase flow. The RRS will not adjust the CEAs since the pressurizer pressure is a compensating input to this system. The SBCS will not open the turbine bypass valves, since the pressurizer pressure is employed as a "bias" signal. The PLCS would increase letdown flow and decrease charging flow. As a result of these control system actions, a low pressurizer pressure situation may result, leading to a possible reactor trip and SIAS on low pressurizer pressure. The operator has adequate instrumentation from which to evaluate the event progress (e.g., pressurizer pressure and level signals from other sensors using other instrument taps). Isolation of letdown on SIAS or by the operator, manual control of charging with pressurizer spray isolation, and use of heaters will bring the plant to a stable condition without using the PLCS, PPCS, and SBCS. 29

The reactor trip on low pressure would prevent any fuel rods from experiencing a DNBR less than 1.19 (CE-1 CHF correlation) and there is no over-pressurization. Since there is no fuel failure and release of primary fluid to the atmosphere, the letdown line break event of paragraph 15.6.3.1 clearly bounds the radiological consequences.

c. Evaluation of Pressure Signal Failing High and Level Signal Failing Low Due to Instrument Tap Damage on Plant Response:

This event is considered unlikely since it requires the process sensing line to be perfectly crimped coincident with a high pressure transient. Nevertheless, the following analysis is provided:

The plant response is similar for the PPCS, RRS, and SBCS as discussed above for the pressure signal failing high. The PLCS, however, would increase charging and decrease letdown. The increases in charging and pressurizer spray flows with no pressurizer heaters will lead initially to a low pressure condition, and subsequently to a steadily increasing pressurizer level. The operator has adequate instrumentation from which to evaluate event progress. Manual control of charging and turning off of pressurizer sprays will bring the plant to a stable condition. During the initial time period when a low pressure condition exists, the conclusions stated for the pressure and the level signals failing high also apply to this scenario.

29

d. Evaluation of Pressurizer Pressure Signal Failing Low and Level Signal Failing High Due to Instrument Tap Damage on Plant Response:

As discussed in the evaluation of both signals failing low, the PPCS, RRS, and SBCS response will be similar. The PLCS, however, would increase letdown flow and decrease charging flow. A reactor trip may occur as a result of low pressure, brought about by the increased letdown flow. The operator can manually control charging flow and isolate letdown flow to increase the pressurizer level. The plant can be brought to a stable condition through operator action and manual control of the PPCS, PLCS, and SBCS. The conclusions stated for the pressure and level signals failing high also apply to this scenario.

References

FSAR chapter 15. No FSAR change was made.

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 1 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
1	SDCS suction line primary isolation valve; 2HV-9377 or 2HV-9378 or 2HV-9337 or 2HV-9339	a. Fails in closed position	Mechanical binding, valve operator	Loss of one shutdown cooling flow path.	Valve position indicator in control room	Parallel redundant flow paths	N/A	Only single train SDC is permitted if HV-9337 or HV-9339 fail closed 29
		b. Fails to close	Electrical or mechanical fault	Degraded redundancy in isolation of primary coolant system from low pressure piping	Valve position indicator in control room	Redundant valve in series	N/A	
		c. Seat leakage	Contamination	Primary coolant leakage to low pressure piping	Temp. indicator in control room for relief valve drain line.	Each closed section of SDCS protected by relief valve plus parallel redundant flow paths	N/A	
2	SDCS suction line drain valves inside containment 3/4"-035-A-334 3/4"-048-A-334	a. Fails in closed position	Mechanical binding	Usable to drain SDCS suction lines	Operator (local/visual)	None required	N/A	
		b. Fails partly open	Seat leakage	No impact on SDC due to blind flange in line	Operator (local/visual)	None required	N/A	
3	SDCS suction line drain valves outside containment 3/4"-037-c-367 3/4"-036-c-367	a. Fails closed	Mechanical binding	Unable to drain SDCS suction lines	Operator (local/visual)	None required	N/A	
		b. Fails partly open	Seat leakage	No impact on SDC due to blind flange in line	Operator (local/visual)	None required	N/A	
4	SDCS suction line containment isolation valves 2HV-9366 or 2HV-9379	a. Fails in closed position	Mechanical binding, valve operator	Loss of one shutdown cooling flow path.	Valve position indicator in control room	Parallel redundant flow paths	N/A	Only single train SDC is permitted if HV-9336 fails closed 29
		b. Fails to close or inadvertently opened	Electrical, malfunction/ operator	Same as above	Valve position indicator	Series redundant isolation valves upstream and relief valves prevent overpressure	N/A	
		c. Seat leakage	Contamination	Potential overpressurization of SDCS by RCS	None	Same	N/A	

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 2 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
5	Return cross-over valve; 2HV-9353 2HV-9359	a. Fails in closed position	Mechanical binding, valve operator	Unable to initiate pre-shutdown cooling warmup recirculation cycle, (only if both valves fail)	Operator (local/visual), control room indication	Parallel redundant flow path	N/A	
		b. Fails in open position	Malfunction	Portion of shutdown cooling flow would short-circuit core through an 8-inch pipe	Operator (local/visual), control room indication	SDC can be accomplished over an extended period at reduced flow.	N/A	
6	SDCS suction line sampling valve; 1"-017-C-376	a. Fails in open position	Mechanical binding	Unable to isolate sampling line from SDCS suction line	Operator (local/visual)	None required	N/A	
		b. Fails in closed position	Mechanical binding	Unable to take sample from SDCS suction line	Operator (local/visual)	None required	N/A	
7	Spent fuel pool suction line valve; 10"-033-C-173	a. Fails in closed position	Mechanical failure	No impact on shutdown cooling. Unable to use shutdown heat exchanges for Aux cooling of spent fuel pool	Operator (local/visual)	None required	N/A	
		b. Fails partly open	Seat leakage	No impact on SDC due to blind flange in line	Operator (local/visual)	None required	N/A	
8	CVCS shutdown purification line isolation valve; 3"-031-C-170	a. Fails in closed position	Mechanical failure	Unable to purify shutdown cooling flow	Operator	None required	N/A	
		b. Fails partly open	Seat leakage	Inadvertent suction on CVCS. Possible damage to purification ion exchange	None	Series redundant isolation valves in CVCS	N/A	
9	Shutdown cooling suction valve; 14"-015-C-173 or 14"-018-C-178	a. Fails in closed position	Mechanical binding	Unable to establish shutdown cooling flow through one low pressure safety injection pump. (LPSI)	Operator (local/visual), control room indication	Shutdown cooling can be accomplished using only one LPSI pump - time extended	N/A	
		b. Fails partly open	Seat leakage	None	None	Several series redundant isolation valves in return line	N/A	

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 3 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
10	LPSI suction line isolation valve; 16"-022-C-173 or 16"-023-C-173	a. Fails in open position	Mechanical failure operator error	Possible to draw down the refueling water tank (RWT)	Operator, possibly level alarms in RWT, control room indication	Redundant isolation valves in RWT	N/A	29
		b. Fails in closed position	Mechanical failure	Unable to use affected LPSI pump for safety injection. No effect on shutdown cooling	Operator (local/visual), control room indication	None required	N/A	
11	Low-pressure safety injection pump, P015 or P016	Fails to pump	Electrical malfunction, mechanical failure	Loss of half of shutdown cooling flow capacity	Low flow indications from flow indicator FI-306	Shutdown cooling can be achieved using only one pump-but time is extended	N/A	
12	LPSI pump minimum flow line stop check valve 2"-037-C-329 or 2"-063-C-329	Fails closed	Mechanical failure, blockage	Miniflow line normally closed during shutdown cooling.	Control room indication	N/A	N/A	29
13	High-pressure safety injection or CS pump minimum flow line stop check valve; 2"-036-C-329 or 2"-034-C-329 or 2"-035-C-329 or 2"-104-C-329 or 2"-010-C-329 or 2"-011-C-329	Fails open	Seat leakage, blockage	Back leakage into CS or HPSI lines during shutdown cooling. Possible damage to HPSI or CS pumps due to reverse flow	HP header pressure	Check valves in CS and HPSI lines prevent appreciable reverse flow; redundant pumps would not be affected	N/A	8
14	LP safety pump minimum flow line primary isolation valve; 2HV-9348 or 2HV-9347 or 2HV-9306 or 2HV-9307	a. Fails in open position	Mechanical binding, valve operator malfunction	Possible diversion of primary coolant to RWT during shutdown cooling	Valve position indicator in control room minimum flow line flow indicators	Series redundant valves	N/A	
		b. Fails in closed position	Mechanical binding, valve operator malfunction	Unable to establish safety pump minimum flow recirculation to RWT for one LPSI pump	Valve position indicator in control room, low flow indications from min flow line flow indicators	Redundant LPSI pump	N/A	

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 6 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
23	Containment spray header manual isolation valve; 8"-005-C-173 or 8"-003-C-173	a. Fails in open position	Mechanical binding	No impact during shutdown cooling	Operator (local/visual)	N/A	N/A	Valve normally locked open except during CS, nozzle test
		b. Fails in closed position	Mechanical binding	No impact during shutdown cooling	Operator (local/visual)	N/A		
24	Containment spray valve; 2HV-9367 or 2HV-9368	a. Fails in closed position	Mechanical binding, valve operator malfunction	No impact on shutdown cooling.	Valve position indicator in control room	N/A	N/A	
		b. Fails open	Seat leakage, valve operator malfunction, spurious signal	Portion of shutdown cooling flow diverted to CS header. Primary coolant released inside containment	Containment radiation monitors; shutdown cooling flow indicator, FI-306, low flow indications	Containment spray line series manual isolation valve can be closed	N/A	Valves are locked closed (power lock-out) during SDC 29
25	CS Nozzle test connection isolation valve; 4"-008-C-174 or 4"-009-C-174	a. Fails closed	Mechanical binding	No impact on shutdown cooling	Operator (local/visual)	N/A	N/A	Valves are manually operated and locked closed except during spray nozzle tests
		b. Fails open	Seat leakage	No impact on SDC due to blind flange in line	Operator (local/visual	None required		
26	Shutdown cooling return valve; HV-8150 or HV-8151	a. Fails in closed position	Mechanical binding, valve operator malfunction	Effective loss of one shutdown cooling tain	Valve position indicator in control room	Shutdown cooling can be achieved using one train, but time extended	N/A	25
		b. Fails in open position	Mechanical binding, valve operator malfunction	Effective loss of one containment spray tray	Valve position indicator in control room	One spray train, if required, would be sufficient	N/A	
27	Refueling water tank refill valve; 6"-162-C-075	a. Fails closed	Mechanical binding	No impact on shutdown cooling ability	Operator (local/visual)		N/A	8
		b. Fails partly open	Seat leakage	Portion of shutdown cooling flow diverted to RWT. Loss of primary coolant inventory	RWT level indicators	Series redundant manual isolation valve in RWT refill in line (6"-060-D-075)	N/A	29 29
28	Spend fuel pool cooling line isolation valve; 8"-018-C-173	a. Fails closed	Mechanical binding	No impact on shutdown cooling	Operator (local/visual)	None required	N/A	
		b. Fails partly open	Seat leakage	No impact on SDC due to blind flange in line	Operator (local/visual)	None required	N/A	

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 7 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
29	Shutdown cooling return line sampling valve; 3/4"-205-C-376	a. Fails in closed position	Mechanical binding	No impact on shutdown cooling	Operator (local/visual)	None required	N/A	
		b. Fails partly open	Seat leakage	Portion of shutdown cooling flow diverted to sampling system	Low flow indications from shutdown cooling flow indicator, FI-306. Possibly indications from leak and radiation monitors if sampling system damage occurs	Series redundant isolation valve in sampling system	N/A	
30	Shutdown cooling control valve bypass valve; 14"-079-C-173	a. Fails in closed position	Mechanical binding	No impact on normal shutdown cooling	Operator (local/visual)	None required	N/A	Valve is locked closed during normal SDC
		b. Fails partly open	Seat leakage	Increased cooldown rate due to increased flow through heat exchangers	Shutdown cooling differential temp. indicator, 2TT-0351	Shutdown cooling in manually controlled Flow can be adjusted to achieve desired cooldown rate	N/A	
31	Shutdown cooling control valve manual isolation valve; 14"-078-C-173 or 14"-080-C-173	a. Fails in closed position	Mechanical binding	Unable to establish shutdown cooling flow through control valve 2HV-9316	Unable to cooldown as indicated by temperature indicators TE-0351 and TE-0352	Shutdown cooling control valve can be bypassed through the bypass valve and flow controlled manually using the bypass valve	N/A	Valves are manually operated, normally open, closed only for maintenance on HV-9316 29
		b. Fails in open position	Mechanical binding	No impact on shutdown cooling	Operator (local/visual)	Two series redundant isolation valves	N/A	
32	Shutdown cooling control valve; 2HV-9316 (S1-657)	a. Controls flow low	Mechanical binding, valve operator malfunction	Slow cooldown rate	Shutdown cooling differential temp. indicator, 2TI-0351	Shutdown cooling is manually controlled so valve can be opened until desired cooldown rate achieved or bypass valve can be used	N/A	
		b. Controls flow too high	Mechanical binding, valve operator malfunction	Excessive cooldown rate	Shutdown cooling differential temp. indicator, 2T-0351			

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 8 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
32 (cont)		c. Fails closed	Mechanical binding	Possible loss of flow through SDC heat exchangers	Valve position indication, and possibly FI-0306 flow indication and temperature indication TI-303-1, TI-303-2, TI-351-1 or TI-351-2	See Remarks		Parallel flow path available through bypass valve 14"-079-C-173
		d. Fails open	Loss of power or mechanical binding	Possible increase in flow through SDC heat exchanger: increase in cooldown rate	See 32.c	See Remarks		If valve fails due to loss of power, it may be operated manually. If valve binds, flow-rate may be controlled by LPSI header valves HV-9322, -9325, -9328, -9331
33	Shutdown cooling differential temp. detector indicator TI-0351	a. Reads high	Electrical or mechanical malfunction	No direct impact on shutdown cooling but possible incorrect flow throttling by operator resulting in reduced cooldown rate	Shutdown cooling heat exchanger discharge temp. indicators plus temp. indicator 2TI-0352	Cooldown can be achieved at the reduced rate, but time extended; or cooldown can be achieved at "normal" rate using alternate temp. indicators for control reference	N/A	
		b. Reads low	Electrical or mechanical	No direct impact on shutdown cooling but possible incorrect flow throttling by operator resulting in excessive cool-down rate	Shutdown cooling heat exchanger discharge temp. indicators plus temp. indicator, 2TI-0352		N/A	

29

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 8A of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
34	Shutdown heat exchanger bypass flow control valve isolation valves; 14"-081-C-173 14"-082-C-173	a. Fail in open position	Mechanical binding	No direct impact on shutdown cooling	Operator (local/visual)	None required	N/A	
		b. Fails in closed position	Mechanical binding	Loss of heat exchanger bypass flow control capability. Possible excessive cooldown rate	Operator, flow indicator FI-306	Bypass flow control valve and isolation valves can be bypassed. Local manual bypass flow control possible using valve, 14"-153-C-173	N/A	Valves are manually operated, normally open, closed only for maintenance on flow control valve 2FV-306
35	Heat exchanger bypass flow control valve; 2FV-306	a. Deleted						
		b. Deleted						
		c. Fails closed	Mechanical binding	Increased cooldown rate	Operator	Bypass valve 14"-153-C-173 may be opened		If 14"-153-C-173 must be opened, the total flow rate will be controlled by the LPSI header valves HV-9322, -9325, -9328, -9331
		d. Fails open	Mechanical binding	Decreased cooldown rate	Operator	Isolation valves 14"-081-C-173 or 14"-082-C-173 may be closed to isolate the SDC heat exchanger bypass path		FV-0306 is a locally operated manual valve

8

29

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 9 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects Upon	Remarks and Other Effects
36	Heat exchanger bypass flow control valve manual bypass valve; 14"-153-C-173	a. Fails in closed position	Mechanical binding	No impact on normal shutdown cooling	Operator (local/visual)	None required	N/A	Valve locked closed during normal operation 29
		b. Fails partly open	Seat leakage	No impact	None	Bypass flow control valve available	N/A	
37	LPSI pump discharge pressure indicator 2PI-0307	a. Erroneous readings (high or low)	Electrical or mechanical malfunction	No impact on shutdown cooling	Reference to other instrumentation	None required	N/A	This pressure indicator is not used for control reference during shutdown cooling
38	Shutdown cooling flow control, FI-0306	a. Indicates flow too high	Electrical or mechanical malfunction	Decreased cooldown rate-shutdown cooling time extended	Shutdown cooling differential temp. indicator, 2TI-0351 shutdown cooling temp. indicator, 2TI-0352	Cooldown can be controlled using temp. indicators	N/A	The heat exchanger bypass flow control valve is used only during the initial portion of shutdown cooling when part of the flow bypasses the heat exchangers. During the latter part, all flow goes through the heat exchangers and the bypass flow control valve is closed. 29
		b. Indicates flow too low	Electrical or mechanical malfunction	Increased cooldown rate	Same as 34a	See 38.a	N/A	29
39	Shutdown cooling temp. indicator; TI-0352	a. Reads high	Electrical or mechanical malfunction	No direct impact on shutdown cooling	Shutdown cooling differential temp. indicator, 2TI-0351, heat exchanger temp. indicators, primary coolant system temp. indicators	None required	N/A	

Table 5.4-5
FAILURE MODE AND EFFECTS ANALYSIS
OF SDCS (Sheet 11 of 11)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
44	LPSI line pressure indicators; PI-0319 PI-0329	a. Erroneous high pressure alarms	Electrical or mechanical malfunction	No impact on shutdown cooling	N/A	N/A	N/A	
	PI-0339 PI-0349	b. Erroneous low pressure indications	Electrical or mechanical malfunctions	No impact on shutdown cooling	None	None required	N/A	
45	LPSI header line pressure bleed valves; 2HV-9341	a. Fails partly open	Seat leakage	No impact on shutdown cooling	Valve position indicator in control room	Series redundant isolation valves in bleedline to RWT	N/A	
	2HV-9351 2HV-9361 2HV-9371	b. Fails in closed position	Mechanical binding, valve operator malfunction	No impact on shutdown cooling	Valve position indicator in control room	None required	N/A	
46	Safety injection line check valve; 12"-027-A-551 12"-029-A-551	a. Fails partly open	Seat leakage	No impact on shutdown cooling	Safety injection line pressure indicator	Pressure can be bled-off to the RDT through pressure bleed valve	N/A	
	12"-031-A-551 12"-033-A-551	b. Fails closed	Mechanical binding, blockage	Loss of one shutdown cooling flow path	Periodic test		N/A	
					Possibly safety injection line pressure indicators	Shutdown cooling can be achieved using only two safety injection lines, but extra time might be required		
47	Air supply valve to HV-9316	Fails closed	Mechanical binding,	Loss of remote operability of HV-9316	Operator	Handwheel on HV-9316 allows manual operation		
48	Air vent valve to HV-9316	Fails open	Mechanical binding,	Loss of remote operability of HV-9316	Operator	Handwheel on HV-9316 allows manual operation		
49	Solenoid air supply valve to HV-9316 (HV-9316B)	a. Fails closed	Mechanical fault or loss of power	Loss of remote operability of HV-9316	Control room indication	Handwheel on HV-9316 allows manual operation		
		b. Fails open	Mechanical fault or loss of power	Valve HV-9316 fails open. Possible increase in flow through SDC heat exchanger: increase in cooldown rate	Control room indication	Handwheel on HV-9316 allows manual operation		

29

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 1 of 12)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects Upon	Remarks and Other Effects
1.	Shutdown cooling valve HV-8152 or HV-8153	a. Inadvertantly open	Operator error	Some cross flow to LPSI system from one control spray subsystem. Reduced LPSI flow. CS pump runout.	High flow indication in one CS train and different outlet temp's at the SDC Hx's.	Redundant spray subsystem would be uneffected. See remarks.		Valve is normally locked closed (power lockout) 25
		b. Fails to open	Mechanical binding, valve operator malfunction	Inability to use one shutdown cooling heat exchanger for shutdown cooling mode of operation.	Valve position indicator in control room, and T303X or T303Y.	Redundant heat exchanger		
2.	Shutdown cooling flow control valve FV-0306	a. Fails closed	Operator error	No LPSI flow during ECCS operation	Operator, control room position indication	None		Valve is normally locked open to pass ECCS flow. Valve is under administrative control per surveillance requirements of technical specifications.
3.	Bypass valve 14"-153-C-173	a. Fails open	Operator error	LPSI pump flow will increase to runout conditions	High flow indication by FI-0306 in control room	LPSI header valves HV-9322, -9325, -9328, and -9331 can be throttled		Valve is normally locked closed and under administrative control per technical specifications
		b. Fails closed	Mechanical	No effect	Control room position indication	See remarks		See 3.a
4.	Deleted							29

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 2 of 12)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effects Upon	Remarks and Other Effects
5.	Deleted							
6.	Deleted							29
7.	Deleted							

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 3 of 12)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
8.	LPSI pump P-015 P-016	Fails to pump	Electrical fault	Reduced LPSI flow	Possible low flow indication from 2FIC-Q306, Pump status lights and LPSI header pressure	Redundant LPSI pump		
9.	Stop/check valve 10"-024-C-406 or 10"-025-C-406	a. Fails closed	Corrosion	Reduced LPSI flow. Effective loss of one LPSI pump.	Low flow indication from 2FI-0306	Redundant LPSI pump		29
		b. Fails open	Contamination	No effect.	None	Suction isolation valve of the inoperative pump can be closed.		
10.	LPSI suction stop-valve 16"-022-C-173 or 16"-023-C 173	a. Fails open	Mechanical binding	Unable to realign one LPSI pump for post LOCA shutdown cooling mode of operation	Operator, control room indication	Redundant LPSI pump		29
		b. Inadvertantly left closed	Operator error	Effective loss of one LPSI pump	Possible low flow indication from 2FI-0306; LPSI header pressure, control room indication	Redundant LPSI pump		29
11.	Check valve, LPSI suction 16"-084-C-645 or 16"-077-C-645	a. Fails closed	Corrosion	Effective loss of LPSI pump				
		b. Fails open	Contamination	Normally no effect. Potential contamination of CS system and RWT with primary fluid during normal shutdown cooling. (requires double failure)	Periodic testing	Stop valves 16"-022-C-173 16"-023-C-173		Valves 16"-022-C-173 and 16"023-C-173 are locked closed during shutdown cooling operation.

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 4 of 12)

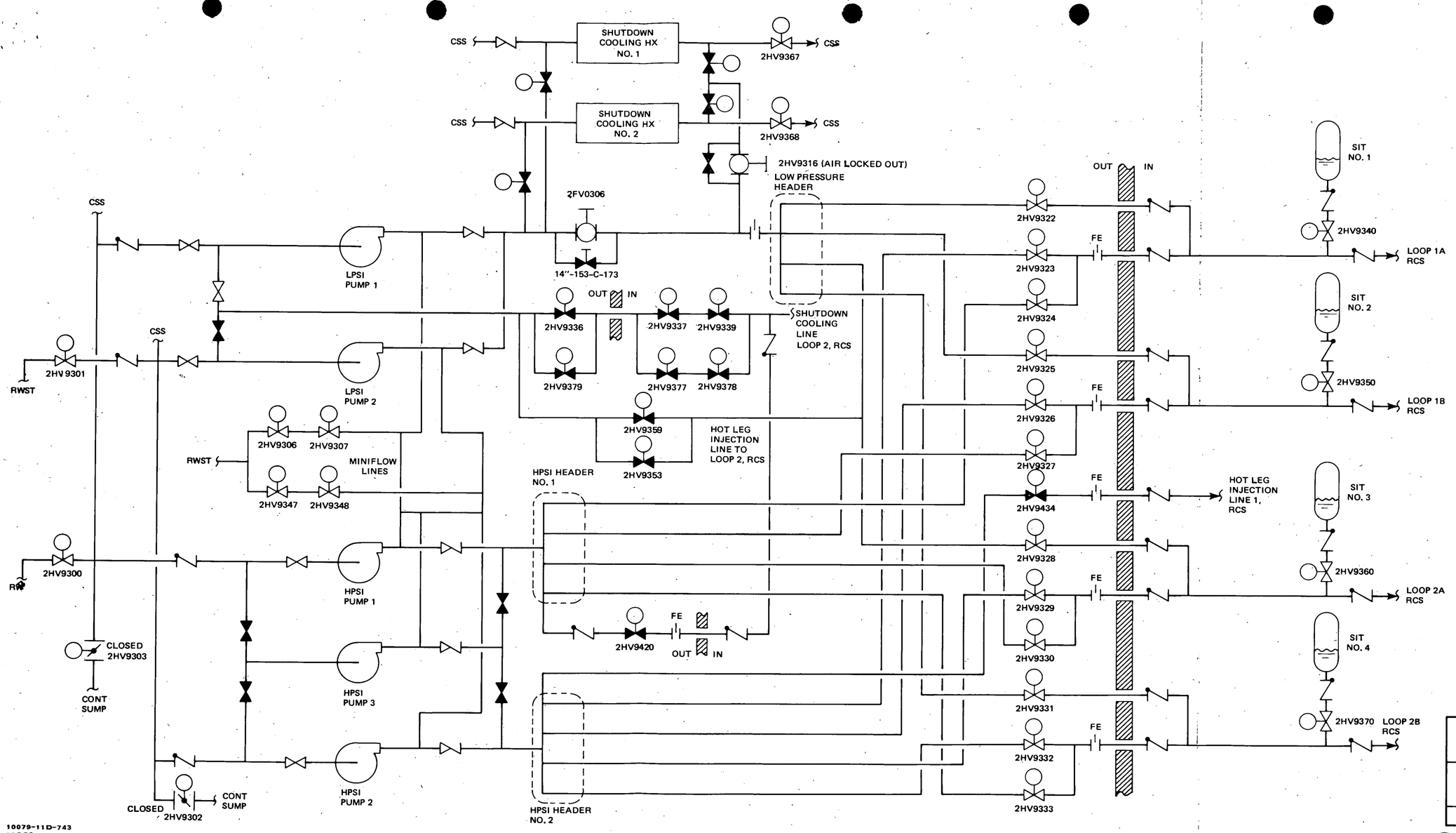
No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
12.	Stop Valve 14"-018-C-173 or 14"-015-C-173	a. Inadvertantly left open	Operator error	None	Period test Control room indication	Series valves		One of these valves will be normally left open 29
		b. Fails closed	Mechanical binding	Unable to realign one LPSI pump for post-LOCA shutdown cooling mode of operation.	Operator, control room indication	Redundant LPSI pump		
13.	HPSI Header check valve 4"-017-C-553	a. Fails closed	Corrosion	Effective loss of one HPSI subsystem	Possible low HPSI flow indications.	Redundant HPSI subsystem		
		b. Fails open	Contamination	Possible overpressure of one HPSI subsystem when charging through HPSI header	Increase in equipment drain tank level.	Relief valve SPSV-9319		
14.	HPSI flow path isolation valve 4"-013-C-075 or 4"-014-C-075 or 8"-010-C-212 or 8"-011-C-212 or 8"-007-C-212 or 8"-009-C-212	a. Fails open or closed	Mechanical binding	Unable to isolate a HPSI pump for maintenance. Major pump maintenance could only be performed by eliminating safety injection and containment spray redundancies.	Operator	Redundant Train available		

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 6 of 12)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
19.	Min-flow stop/check valve 2"-037-C-329 or 2"-063-C-329 or 2"-036-C-329 or 2"-034-C-329 or 2"-035-C-329 or 2"-104-C-329	a. Fails closed	Operator error	Possible damage to one SI pump if it is run dead-headed.	Eventual pump status indication, control room indication for 2"-037-C-329 and 2"-063-C-329	Redundant SI pumps		29
		b. Fails open	Seat leakage	Unable to isolate associated pump for maintenance without eliminating all SI and CS redundancy.	Leakage during maintenance	Redundant full capacity subsystems available		
20.	LPSI Valve 2HV-9322 or 2HV-9325 or 2HV-9328 or 2HV-9331	a. Fails to open on SIAS	Mechanical binding	Loss of LPSI flow to one RCS cold leg	Valve position indicator in control room	Adequate flow to remaining three cold legs		
		b. Fails open	Electrical fault	None	Valve position indicator in control room	In line check valves prevent back-flow		
21.	HPSI Valve 2HV-9325 or 2HV-9324 or 2HV-9326 or 2HV-9327 or 2HV-9329	a. Fails to open on SIAS	Mechanical binding	Degradation of HPSI flow to one RCS cold leg	Valve position indicator and HPSI flow meters in control room	Redundant flow paths redundant HPSI subsystems		

Table 6.3-1
FAILURE MODE AND EFFECTS ANALYSIS
SAFETY INJECTION SYSTEM
(Sheet 12 of 12)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon	Remarks and Other Effects
34.	Drain valve, hot side injection 2HV-9433 or 2HV-9437	a. Fails closed	Mechanical binding	Unable to drain off reactor coolant which may leak past check valve during normal operation	Valve position indicator and pressure indication.	None required		
		b. Fails to close on SIAS	Electrical or mechanical malfunction while line is being drained	Degradation of one of two redundant hot side injection flow paths	Valve position indicator	Redundant flow path		
35.	Emergency sump iso. valves 2HV-9302 or 2HV-9303 or 2HV-9304 or 2HV-9305	Fails to open on RAS	Electrical or mechanical malfunction	Loss of one of two redundant safeguards trains	Valve position indicators, CSS and HPSI flowmeters	Redundant safeguards system train		ZHV-9304 and ZHV-9305 are normally open. 21
36.	Isolation valves 14"-081-C-173 or 14"-082-C-173	a. Inadvertently closed	Operator error	No LPSI flow during ECCS operation	Operator	See remarks		Valve is normally locked open, closed only for maintenance on FV-0306 29
37.	Shutdown cooling warmup valves HV-9353 HV-9359	a. Inadvertently open	Operator error	ECCS flow is partially recirculated back to LPSI pump suction line	Control room position indication	See remarks		Valve is normally locked closed (power lockout)

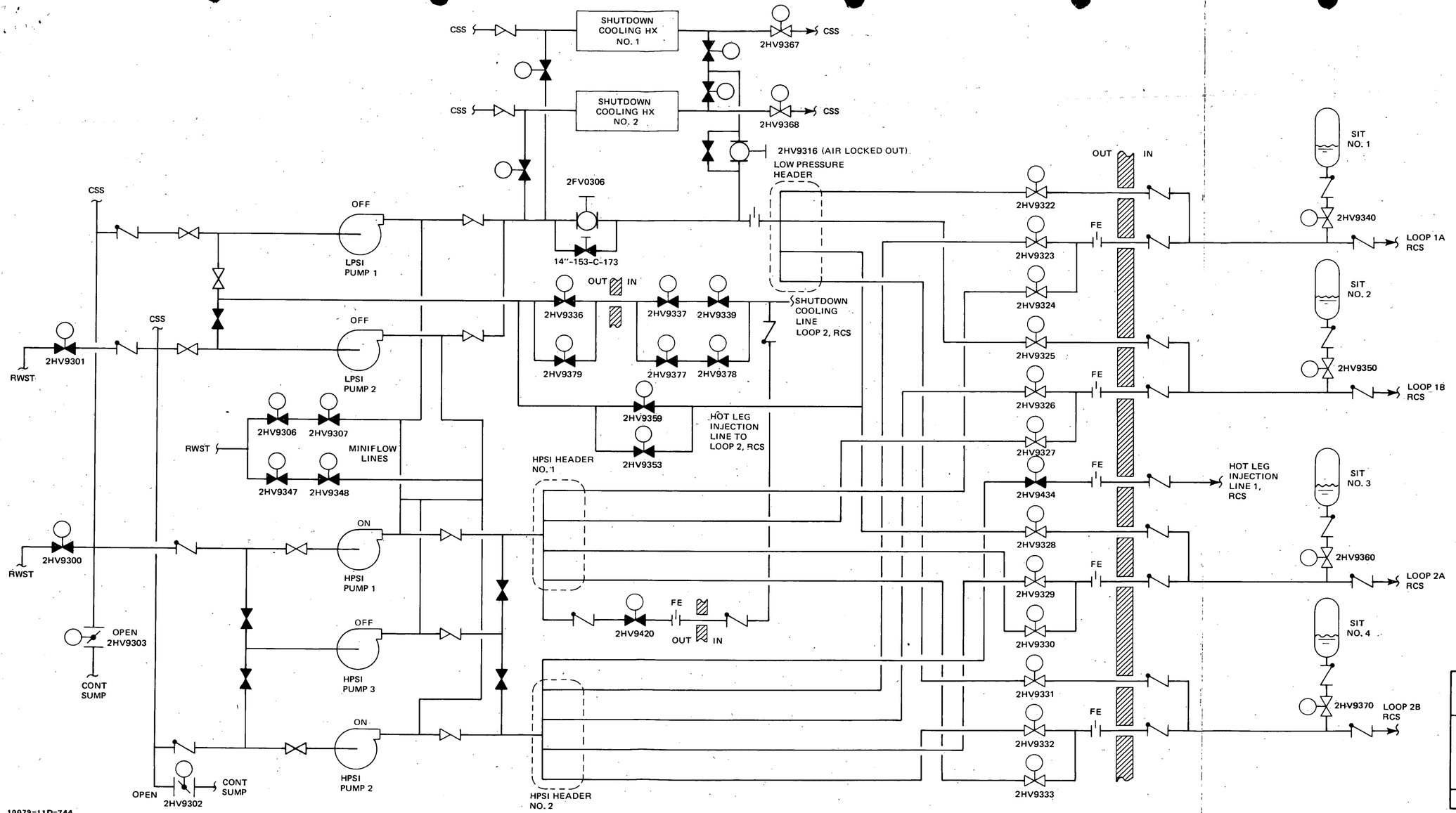


10079-11D-743
110C6

APERTURE CARD

SAN ONOFRE NUCLEAR GENERATING STATION Units 2 & 3
SAFETY INJECTION SYSTEM FLOW DIAGRAM INJECTION MODE
Figure 6.3-4

8002020282-01



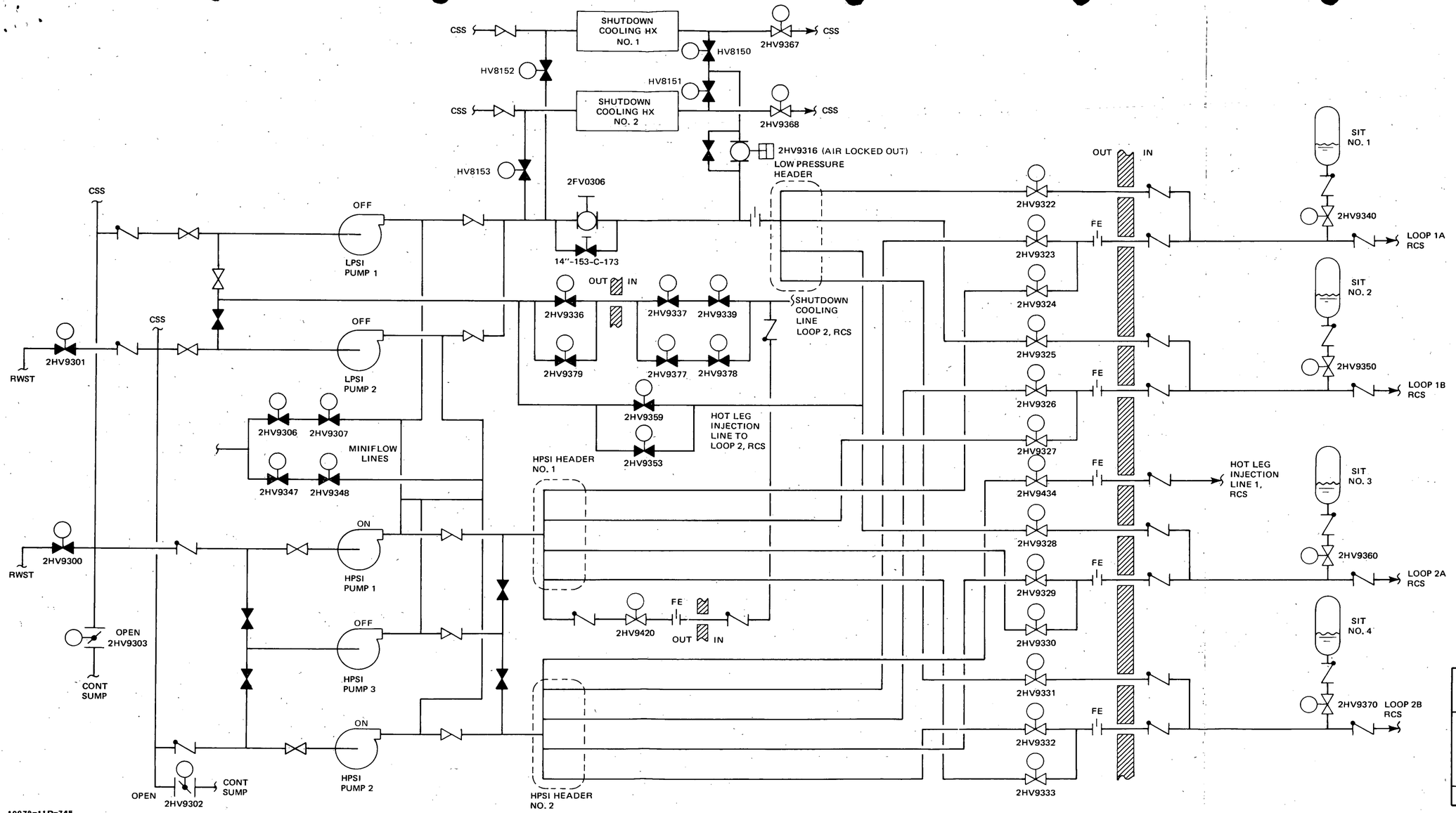
APERTURE CARD

SAN ONOFRE NUCLEAR GENERATING STATION
Units 2 & 3

SAFETY INJECTION SYSTEM
FLOW DIAGRAM
SHORT-TERM RECIRCULATION MODE
< (2 HOURS)

Figure 6.3-5

8202020282-02



10078-11D-745
110C6

APERTURE CARD

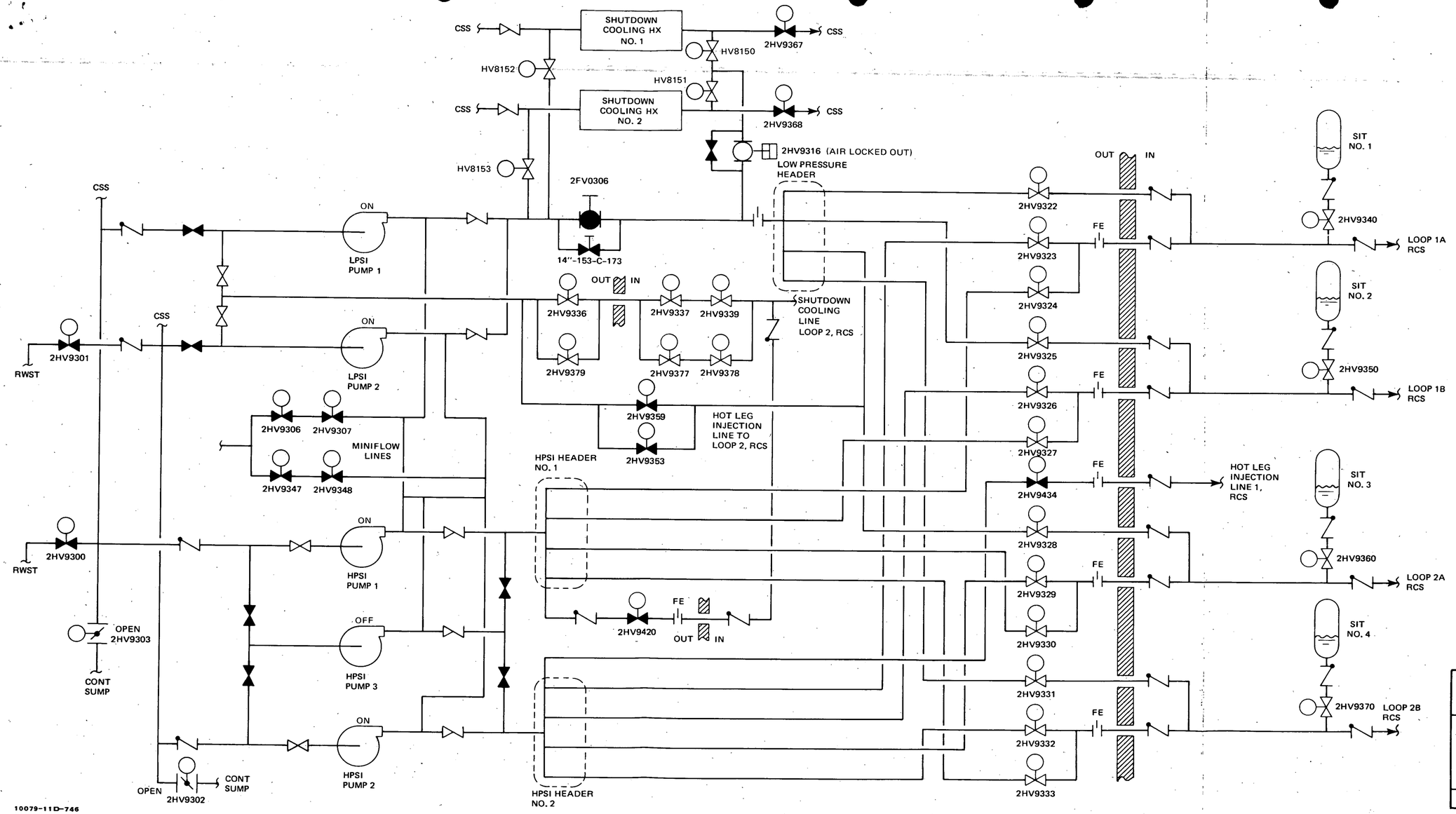
SAN ONOFRE NUCLEAR GENERATING STATION
Units 2 & 3

SAFETY INJECTION SYSTEM
FLOW DIAGRAM
LONG-TERM RECIRCULATION MODE
(HOT AND COLD LEG INJECTION)

Figure 6.3-6

8202020282-03

Amendment 29



10079-11D-746
23MR7

APERTURE CARD

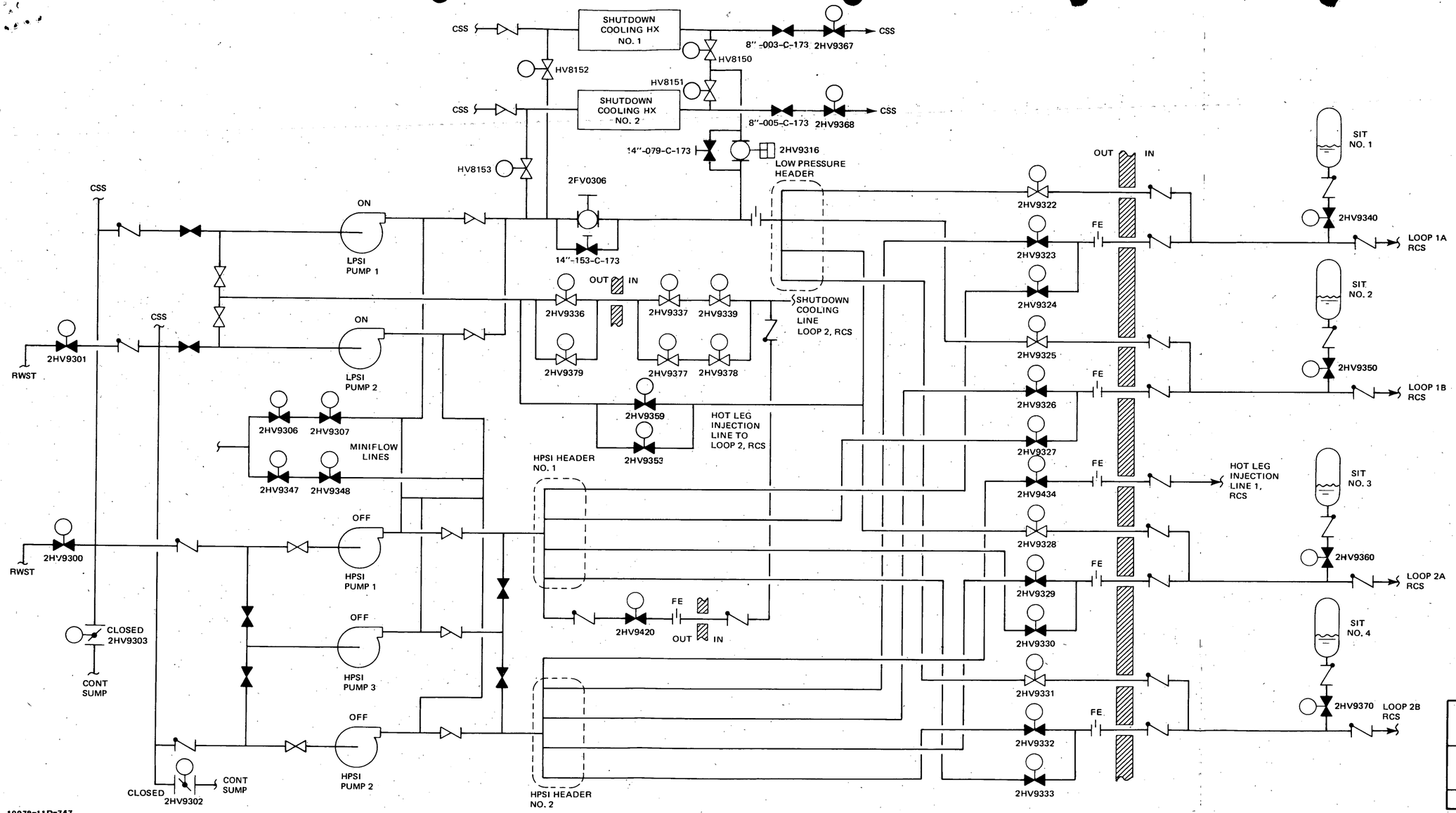
SAN ONOFRE NUCLEAR GENERATING STATION
Units 2 & 3

SAFETY INJECTION SYSTEM
FLOW DIAGRAM
LONG-TERM RECIRCULATION MODE
(POST-LOCA SHUTDOWN COOLING)

Figure 6.3-7

Amendment 29

8209020282-01



10079-11D-747
23MR7

SAN ONOFRE NUCLEAR GENERATING STATION
Units 2 & 3

SAFETY INJECTION SYSTEM
FLOW DIAGRAM
NORMAL SHUTDOWN COOLING MODE

Figure 6.3-8