NUREG/CR-2585
SAND82-7011
RS,1S
Printed May 1982
CONTRACTOR REPORT

Nuclear Power Plant Damage Control Measures and Design Changes for Sabotage Protection

Peter Lobner
Energy Systems Group
Science Applications, Inc.
1200 Prospect Street
La Jolla, CA 92038

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

Available from

GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-2585
SAND82-7011
RS
1S

NUCLEAR POWER PLANT DAMAGE CONTROL MEASURES AND DESIGN CHANGES FOR SABOTAGE PROTECTION

Peter Lobner

Energy Systems Group
Science Applications, Inc.
1200 Prospect St.
La Jolla, California 92038

Printed May 1982

Final Report
31 January 1982

Sandia Principal Investigator David M. Ericson, Jr.

Prepared for
Sandia National Laboratories
Albuquerque, New Mexico 87185
Operated by
Sandia Corporation
for the
U.S. Department of Energy

Work Performed under Sandia Contract No. 61-1562

Funded by
Division of Facility Operation
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1210

Acknowledgement

The author wishes to thank Kathy Nesseler and Lorraine Trevino for their efforts in the preparation of this report.

Nuclear Power Plant Damage Control Measures and
Design Changes for Sabotage Protection

1. INTRODUCTION

This report documents the engineering evaluation of twenty-seven proposed damage control measures and associated system-level design changes that could be of potential benefit in providing protection against sabotage at commercial light water reactor (LWR) power plants. The damage control measures emphasize the use of existing systems in normal or alternate modes of operation. The proposed system-level design changes are those necessary to support the use of existing systems in alternate modes. To the extent practical, the system-level design changes have been limited in scope to those that could be retrofitted in existing nuclear power plants. The potential applicability of each damage control measure and system-level design change is defined, and the impact of its implementation is subjectively estimated.

Damage control measures and design changes are not stand-alone measures for providing protection against sabotage. However, the potential role of damage control and design change in an integrated sabotage protection system is discussed in this report.

2. BACKGROUND

Radiological sabotage is a deliberate act of destruction, damage or manipulation of vital equipment which results in the release, beyond the plant boundary, of sufficient radioactive materials to endanager public health and safety due to radiation exposure. A sabotage threat may arise from a determined violent external assault, attack by stealth, or deceptive actions, of several persons; or from the activities of an insider who could be an employee in any position.

The Nuclear Regulatory Commission (NRC) maintains an ongoing safeguards research program for the development and evaluation of the effectiveness of measures which provide sabotage protection for nuclear power plants. On the basis of previous studies, the following three categories of measures which provide protection against radiological sabotage have been identified (Ref. 1):

- Physical protection measures
- Damage control measures
- Plant design measures

Physical protection measures may include a combination of procedures, personnel and hardware (e.g., alarms, barriers and computer systems) which are specifically intended to deter, detect, assess, delay and respond to acts of radiological sabotage. Damage control measures are actions that can be taken by plant personnel within hours after an act of radiological sabotage to prevent or reduce a release of radioactive material from the plant. Plant design measures are features included in the design or fabrication of components or systems or in the layout of the plant to increase the difficulty of radiological sabotage or to better accommodate physical protection or damage control measures.

Sandia National Laboratories has conducted a two-phase, NRC-sponsored study to identify and evaluate nuclear power plant design concepts and damage control measures for sabotage protection. The results of Phase I of this study are described in NUREG/CR-1345 (Ref. 1). Among the results of Phase I were the identification and initial evaluation of the 25 potential damage control options listed in Table 2.1.

The basic assumptions made in developing the 25 damage control options were the following:

- At the onset of the sabotage event, all sources of offsite power are assumed to be indefinitely interrupted (e.g., the offsite power system could be disabled by separate, coordinated sabotage actions).
- The main turbine generator trips on loss of load and is unavailable as a source of electrical power.
- The reactor control rods are inserted when a scram signal is generated. Measures other than damage control are assumed to provide physical protection for the reactivity control system and reactor protection system.
- There is no coincident loss of coolant accident due to a pipe breach (e.g., onsite sabotage actions do not include the use of explosives). Coolant may be lost from the reactor coolant system by other means such as safety valve operation or reactor coolant pump seal leakage.
- The reactor has been operating at full power for an indefinite period of time prior to the sabotage event, resulting in maximum decay heat levels following reactor shutdown.
- Sabotage acts committed during shutdown periods or refueling are easier to counter since the time available and access conditions greatly expand the possible damage control options.

Based on the above assumptions, the following approach was taken in NUREG/CR-1345 to derive the damage control actions that could aid the operator in establishing and maintaining the plant in a hot shutdown condition following sabotage actions:

- The principal functions required to maintain the plant in a hot shutdown condition were determined. In particular, the basic considerations of coolant inventory control decay heat removal, and primary system pressure control were addressed.

Table 2.1. Summary of Damage Control Options Identified in NUREG/CR-1345

Option	Function	Target (System Sabotaged or Affected)
1. Manual-operated reactor vessel relief system (BWR)	Decay heat removal/ vessel blowdown	Main steam safety/relief valves; vital dc power supply
2. Feed & bleed--condensate storage tanks and suppression chamber (BWR)	Decay heat removal	RHR and PHR service water systems
3. Feeding steam generators with the main feedwater system (PWR)	Decay heat removal	Auxiliary feedwater system
4. Feeding steam generators with the safety injection pumps (PWR)	Decay heat removal	Auxiliary feedwater system
5. Manual venting of steam generators (PWR)	Decay heat removal	Main steam generator safety relief valves
6. Reactor vessel makeup with HPCI system (BWR)	Reactor coolant inventory control/ decay heat removal	Reactor core isolation cooling system
7. Substitution--ESW system for RHR system (BWR)	Decay heat removal	RHR service water pumps
8. Fire main cross connection to RHR service water system (BWR)	Decay heat removal	RHR service water pumps
9. Series operation of SIS pumps for reactor high-pressure injection (PWR)	Reactor coolant inventory control	CVCS coolant charging pumps
10. Vessel makeup with the CRD pumps (BWR)	Reactor coolant inventory control	Reactor core isolation cooling system
11. Reactor vessel makeup with core spray or RHR systems (BWR) with automatic depressurization system	Reactor coolant inventory control	RCIC, HPCI, CRD systems
12. Reactor vessel makeup with main condensate system (BWR)	Reactor coolant inventory control	RCIC, HPCI, CRD, core spray and RHR systems
13. Substitution--plant service water for ESW system (BWR & PWR)	Auxiliary cooling	ESW pumps
14. Cross connection--main feedwater and ESW systems (PWR)	Auxiliary cooling	ESW pumps
15. Cross connection--fire main and ESW system (BWR & PWR)	Auxiliary cooling	ESW system
16. Substitution--ESW for CCW system (PWR)	Auxiliary cooling	Component cooling water pumps
17. Pressurizer and steam generator level indication local readout (PWR)	Decay heat removal/ primary plant inventory control	Instrumentation circuitry
18. Steam generator pressure indication--local (PWR)	Decay heat removal	Instrumentation circuitry
19. Class 1E backup power supply for non-Class 1E equipment (BWR & PWR)	Applies to several damage control options	Applies to several targets
20. Cross connection of Class 1E battery buses (BWR & PWR)	125-volt dc power source	125-volt dc power supply

Table 2.1. Summary of Damage Control Options Identified in NUREG/CR-1345 (Continued).

	Option	Function	Target (System Sabotaged or Affected)
21.	Cross connection of dc buses (Class 1E and non-Class 1E) (BWR & PWR)	125-volt dc power source	125-volt dc power supply
22.	Alternate dc power supply to designated equipment (BWR & PWR)	125-volt dc power source	125-volt dc power supply and distribution systems
23.	Backup water supplies (PWR)	Decay heat removal/ reactor plant inventory control	Various
24.	Backup water supplies (BWR)	Decay heat removal/ reactor plant inventory control	Various
25.	Manual operation of steam-driven pumps (BWR & PWR)	Decay heat removal/ reactor plant inventory control	Control power supply (ac or dc)

KEY

ESW = emergency service water
SIS = safety injection system
CRD = control rod drive
CVCS = chemical and volume control systems
RCIC = reactor core isolation cooling
HPCI = high-pressure coolant injection
CCW = component cooling water

- The systems and components that would normally be expected to perform these functions were identified.

- Auxiliaries and support systems required for each of the systems were identified.

- Alternative ways of performing the principal functions and providing needed support services, including procedural aspects of each method, were established.

- The procedural steps needed to initiate the alternative actions were defined.

- Hardware changes required for each action were defined and examined.

This report documents the results of work conducted under Phase II of the Sandia National Laboratories study to identify and evaluate nuclear power plant design concepts and damage control measures for sabotage protection. A detailed engineering evaluation of each of the damage control measures listed in Table 2.1, and associated design changes, is presented in this report. Additional complementary damage control measures and design changes are introduced and are also evaluated.

Section 2 References

1. Ericson, D. M. and Varnado, G. B. , "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

3. THE POTENTIAL SABOTAGE PROTECTION ROLE OF DAMAGE CONTROL MEASURES

3.1 DAMAGE CONTROL OVERVIEW

The basic objectives of damage control are to: (a) restore or maintain a functional capability required for safe shutdown, or (b) extend the time available to restore by other means those functional capabilities that have been lost due to sabotage actions. Unlike physical protection measures, damage control measures are only undertaken after sabotage actions cause a departure from normal plant operations and "traditional" reponse systems fail to provide the functional capabilities necessary to establish and maintain a safe shutdown condition. The key role for damage control therefore is in the response and recovery phase following attempted sabotage.

The types of damage control activities considered in this report emphasize the use of existing systems in normal or alternate modes of operation. This approach to damage control must be differentiated from conventional approaches which include activities such as: (a) making temporary repairs to vital equipment, and (b) jury-rigging systems and equipment to perform in alternate roles. Conventional damage control was considered in NUREG/CR-1345 (Ref. 1), but was found to have major shortcomings. As reported in NUREG/CR-1345, the significant concerns associated with conventional damage control activities at a nuclear power plant include the following:

- "This (damage control time line) analysis does not take into account the actions an adversary might take to interfere with repair crews. That is, if an adversary is intent upon damaging particular items of equipment, he could also take steps to prevent a repair crew from gaining access to the damaged equipment."
- "The time estimates for response and repair activities are highly subjective at this point and probably optimistic. To adequately support such an approach, a data base (which does not exist) is required which would provide response times to various control room alarms required to accomplish particular damage control tasks."

- "There is uncertainty regarding the reliability factors and time constraints involved in assembling a sufficient number of appropriately skilled personnel to conduct repairs or jury-rigging. Establishment of standby damage control teams for backshift response presents personnel management problems as well as additional costs. Given current requirements for fire brigades and security teams, a damage control team concept would likely meet firm resistance from utilities, who appear to believe they already have too many 'nonproductive' personnel."

- "With the large amount of repair and backfitting now going on during plant outages, maintaining 'emergency only' stocks of equipment and supplies could be a major administrative problem."

As a result of these concerns, the basic philosophy of damage control at nuclear power plants was reevaluated, and the concept of using existing systems in normal or alternate modes of operation was developed.

Many nuclear power plants have only limited capabilities to operate existing systems in alternate modes, therefore, design changes will likely be required to support the implementation of many damage control measures. Design changes may include, but are not limited to, the following:

- Adding the capability to crossconnect fluid systems or to establish unconventional system alignments.

- Adding the capability to crossconnect electrical buses or to transfer electrical loads.

- Adding the capability for local manual operation of equipment or systems that are not normally operated in this mode.

- Upgrading fluid system pumping capacity.

For timely implementation of damage control, all design changes should be permanent in nature, and damage control actions by operating personnel should be limited to valve, circuit breaker and switch manipulations to the extent practical.

An individual damage control measure provides a diverse system or an alternate operating mode to replace or restore the functional capability of a specific system or component (e.g., target) that has been disabled or adversely affected by sabotage actions. A set of damage control measures provides a variety of diverse systems and alternate operating capabilities to respond to the sabotage of a specific set of targets. If other systems or components are disabled, the available damage control measures may be of little benefit. The potential effectiveness of damage control is therefore strongly related to the analytical process by which "traditional" response systems (e.g., primary sabotage targets) and alternative response systems (e.g., candidates for use in damage control) are identified and prioritized.

An event solution (as opposed to a vital area solution) of the sabotage fault tree (Ref. 2) provides a structured, plant-specific approach for identifying the "traditional" systems required to establish and maintain a safe shutdown condition. A methodology has been developed to rank systems based on the time-sequenced order in which they are required for accident mitigation (Ref. 3). This methodology ranks front-line response systems (e.g., coolant inventory control systems, decay heat removal systems, etc.) as well as required auxiliary or support system (e.g., electric power, actuation, component cooling water, room ventilation, etc.). From the ranking information, it is evident that some systems will not be candidates for damage control because of the very short response time available. Such systems include the reactivity control system and the reactor protection system. Other systems may be potential candidates for damage control and their relative ranking provides the basis for prioritizing potential damage control activities.

Candidate systems for use in damage control can be identified through a systematic review of plant systems to compare the functional capabilities of each "traditional" response system with the capabilities of all potential alternate systems. Where a good match between "traditional" and alternate system capabilities exists, it may be possible to establish the interfaces required for damage control without significantly altering the operating characteristics of either system. Design changes may therefore be limited to the interface itself. In some cases, there may not be a good match between "traditional" and alternate system capabilities. If this occurs, two basic options exist. The first option is to use the alternate system in its present form to "buy time" to restore other more capable systems to operation. The second option is to significantly ugrade the capability of the alternate system to be functionally equivalent to the "traditional" system it will replace during damage control. Both options may require design changes to establish the necessary system interfaces. The second option requires major redesign of the alternate system; a factor that limits the practicality of this option.

3.2 INTEGRATION OF DAMAGE CONTROL AND PHYSICAL PROTECTION MEASURES

Having identified a set of damage control measures for a particular nuclear power plant, the question of how to integrate these capabilities with other sabotage protection measures must now be faced. The following are three basic approaches for treating damage control:

- Assume no credit for damage control in sabotage protection analysis. Physical protection is provided for a set of "traditional" response systems that are capable of establishing and maintaining a safe shutdown condition. Systems associated with damage control are not physically protected against sabotage, and any actual benefits from damage control will be considered as an "extra."
- Take credit for damage control capabilities, but only as a redundant backup to "traditional" response capabilities. Both "traditional" and alternate systems are physically protected, however, some reduction in physical protection requirements may be possible because of the redundant response capability.
- Take credit for selected damage control capabilities as primary means for establishing and maintaining a safe shutdown condition (e.g., in lieu of "traditional" response systems). Systems associated with damage control must be physically protected.

Current NRC philosophy regarding damage control is comparable to the first approach. The second approach uses damage control to provide some redundant capabilities for establishing and maintaining a safe shutdown condition, thereby justifying the reduction of physical protection requirements for the related set of "traditional" and alternate systems. The specific changes to physical protection philosophy that may be realized by implementing damage control are beyond the scope of this report. Such changes may include a reduction in the need for physical barriers and a modification of the monitoring and security force response requirements. These changes may lead to improvements in the operational flexibility of the integrated sabotage protection system. As an example, the existence of a functionally redundant, physically protected damage control capability may justify the simplification of physical protection procedures for maintenance that temporarily takes a vital piece of equipment out of service during plant operations. This redundant damage control capability may also provide a basis for reducing some requirements of the plant technical specifications dealing with safety-related equipment unavailability during power operation.

The third approach for treating damage control measures depends on the damage control capability in lieu of the "traditional" response system to establish and maintain safe shutdown conditions. It is doubtful that this approach would be an acceptable alternative in view of the fact that many nonsafety-related systems will likely be candidate systems for damage control.

Section 3 References

1. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

2. Varnado, G. B. and Ortiz, N. R., "Fault Tree Analysis for Vital Area Identification," NUREG/CR-0809, Sandia National Laboratories, June 1979.

3. Lobner, P., Goldman, L., Horton, W., and Finn, S., "Ranking of Light Water Reactor Systems for Sabotage Protection," SAND82-7053, Sandia National Laboratories, June 1982.

4. SUMMARY AND CONCLUSIONS REGARDING DAMAGE CONTROL MEASURES

4.1 SUMMARY OF THE EVALUATIONS OF INDIVIDUAL DAMAGE CONTROL MEASURES

The twenty-five damage control measures listed in Table 2.1 and the following two additional measures are evaluated in detail in Section 5:

- Alternate source of onsite Nonclass 1E AC power.
- Diesel generator startup and loading without DC power.

Potentially feasible approaches for all twenty-seven measures have been identified; however, the impact of their implementation varies greatly. To summarize the evaluation of each damage control measure, the following five ranking categories are used:

- Technical feasibility
- Effectiveness
- System or plant modifications required
- Operational impact
- Regulatory concerns

Tables 4.1 to 4.5 explain the subdivisions that are used within each ranking category.

The summary of the twenty-seven individual damage control measure evaluations is presented in Table 4.6. This table briefly describes the basic concept of each damage control measure, identifies the sabotage targets for which the damage control measure was developed, and describes the specific approaches that were considered to implement the basic concept. Each potentially feasible approach is evaluated using the five categories discussed previously. Approaches judged to be not technically feasible are included in Table 4.6 for information, but are only evaluated under the category "Technical Feasibility."

Table 4.1. Level of Technical Feasibility of Damage Control Measure or Design Change.

Code	Description
A	Existing design - (1) Examples of the proposed system design or operating mode exist in nuclear power plants and can be copied, or (2) the damage control measure uses the design capability of existing systems.
B	Feasible - It is judged that an adequate design and/or adequate operating procedures will result from the application of standard engineering practices and plant experience.
C	Questionable - Damage control measure is original or conceptual in nature and will likely require proof testing, or may operate outside the range of common experience.
D	Not feasible - Fundamental technical problems exist that would likely preclude implementing the measure.

Table 4.2. Level of Effectiveness of Damage Control Measure or Design Change.

Code	Description
A	A functional capability required for maintaining safe shutdown conditions is restored or maintained by the damage control measure following sabotage actions. The functional capabilities of concern are: • decay heat removal (DHR) • reactor coolant inventory control (INV) • overpressure protection (OPP) • a support function required for the operation of systems that perform any of the above functions (SUP)
B	The measure only extends the time available for other measures to restore functional capabilities that have been lost due to sabotage actions.

Note: "A" level effectiveness will be followed by the code "DHR", "INV", "OPP" or "SUP" in parentheses to indicate the related safety function(s).

Table 4.3. Level of System or Plant Modification Required To Implement Damage Control Measure.

Code	Descriptions
A	None - The proposed measure uses existing systems.
B	Low - Modifications are relatively minor in nature and can be accomplished at the component or subsystem level. Basic operational characteristics of existing systems are not altered.
C	Moderate - Modifications may entail (1) routing and installing new crossconnect piping systems, (2) redesigning and replacing a portion of a system, or (3) altering plant structures. Basic operational characteristics of existing systems are not significantly altered.
D	High - (1) Significant system-level or plant structural modifications require extensive redesign and replacement of equipment, with supporting detailed analysis and testing to verify adequate system operating capability, or (2) requires new system not commonly found at nuclear power plants.

Table 4.4. Level of Operational Impact Associated With Damage Control Measure.

Code	Description
A	None - The proposed measure utilizes existing systems in modes of operation for which plant personnel are already trained.
B	Low to moderate - Required operator actions and likely time constraints do not impose undue demands on operating personnel.
C	Moderate to high - (1) The number, variety or difficulty of operator actions may require additional operating personnel to provide timely response or to coordinate actions, or (2) the time available for operator actions may be marginal.
D	Very high - Operating personnel will most likely be unable to respond in the limited time available.

Table 4.5. Level of Regulatory Concern Associated With Damage Control Measure or Design Change.

Code	Description
A	None - (1) The proposed measures are existing features of approved nuclear plant design, or (2) the proposed measures are straightforward extrapolations of approved designs.
B	Low to moderate - Regulatory concerns may impose constraints on design, operation or training, but should not preclude implementing the proposed measure.
C	Moderate to high - Regulatory concerns may preclude the implementation of the proposed measure.

Table 4.6. Summary of Damage Control Measures and Design Changes.

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION						REMARKS
				TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	
1	Manually-operated capability to depressurize the reactor vessel (BWR)	Automatic depressurization system (ADS) and power-operated mode of safety/relief valve operation.	Add local manual operating capability to safety/relief valves.	B	A (DHR)	C	C	B	11, 12	
			Reestablish condenser vacuum and depressurize using turbine bypass system (TBS).	D*	--	--	--	--	--	*Inadequate response time available.
			Reestablish condenser vacuum and blowdown to condenser via reactor water cleanup (RWCU) system.	D*	--	--	--	--	--	*Inadequate blowdown capability.
			Vent reactor vessel to suppression pool via RCIC or HPCI pump steam lines.	D*	--	--	--	--	--	*Inadequate blowdown capability.
2	Feed-and-bleed suppression pool cooling (BWR)	Residual heat removal system (BWR/3 to BWR/6), separate containment cooling system (BWR/1 or BWR/2), and essential service water system.	Feed only. Makeup from upper containment pool.	A	B	B*	A	B	7, 8, 24	*Upper containment pool dump valve controls.
			Feed only. HPCI or HPCS pump provides suppression pool makeup via existing test line.	B*	B	A	A	B	-do-	*Effects of flooding on containment may limit volume of water that can be added.
			Feed only. Refueling water transfer pumps provide suppression pool makeup via upper containment pool.	B*	B	B**	B	B	-do-	*Effects of flooding on containment may limit volume of water that can be added. **Upper containment pool dump valve controls.

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION: TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	REMARKS
2 Con't	Feed-and-bleed supression pool cooling (BWR) (Continued)	Residual heat removal system (BWR/3 to BWR/6), separate containment cooling system (BWR/1 or BWR/2), and essential service water system. (Continued)	Feed-and-bleed. HPCI, HPCS or refueling water transfer pumps operated alternately in feed and then in bleed mode.	B	A (DHR)	C	C	C	24	
			Feed-and-bleed. HPCI or HPCS pumps and refueling water transfer pumps each operate in a fixed mode, one to feed, one to bleed.	B	A (DHR)	C	B	C	24	
3	Feed the steam generator with the main feedwater system (PWR).	Auxiliary feedwater system.	Power restored to components in a steam turbine-driven main feedwater pump train to re-establish makeup to the steam generators via existing piping.	B	A (DHR)	C	C	B	19, 26	Not applicable to PWR plants with only motor-driven main feedwater pumps.
4	Feed the steam generators with the high pressure safety injection pumps (PWR).	Auxiliary feedwater system.	SI pumps crossconnected to AFW system to reestablish makeup to the steam generators.	A	A (DHR)	C	B	B	--	
5	Alternate system to vent the steam generators (PWR).	Steam generator safety valve.	Redundant set of safety valves installed on main steam lines.	B	A (OPP)	C	B	B	--	
			Vent steam generators to main condenser via turbine bypass system.	D*	--	--	--	--	--	*Inadequate response time available.
6	Alternate high pressure reactor coolant makeup system (BWR)	Reactor core isolation cooling (RCIC) system.	High pressure coolant injection (HPCI) system provides reactor coolant makeup.	A	A (INV)	A	A	A	--	Applicable to BWR/3 and BWR/4 plants.

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION						REMARKS
				TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	
6 Con't	Alternate high pressure reactor coolant makeup system (BWR). (Continued)	Reactor core isolation cooling (RCIC) system. (Continued)	High pressure core spray (HPCS) system provides reactor coolant makeup.	A	A (INV)	A	A	A	--	Applicable to BWR/5 and BWR/6 plants.
7	Alternate service water system for RHR or suppression pool cooling heat exchangers (BWR).	Essential service water system.	Power restored to components in an alternate service water system and RHR service water flow reestablished via the crossconnect with the ESW system.	B	A (DHR)	C	B	B	7, 13, 19, 26	
8	Fire water system supplies ser ice water for RHR or suppression pool cooling heat exchanger (BWR).	Essential service water system.	All fire water pumps crossconnected to ESW system to reestablish RHR service water flow.	B	A (DHR)	C	B	C	7, 15, 19, 26	
			Fire water pumping capacity upgraded, part of system reserved for fire protection duties and part crossconnected to ESW system to reestablish RHR service water flow.	B	A (DHR)	D	B	B	-do-	
9	Series operation of safety injection (SI) pumps for coolant injection at design reactor coolant system pressure (PWR).	Charging pumps, auxiliary feedwater system.	SI system pressure boundary upgraded and piping added to permit tandem operation of two high pressure safety injection pumps.	C	A (INV)	D	B	C	--	
10	Reactor vessel makeup with the control rod drive pumps (BWR).	All other high pressure injection systems (HPCS, HPCI, RCIC and FWCI).	Control rod drive hydraulic system (CRDHS) provides reactor coolant makeup.	A	B*	A	A	A	19, 26	*Cannot match makeup capabilities of other high pressure injection systems.

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION: TECHNICAL FEASIBILITY	EVALUATION: EFFECTIVENESS	EVALUATION: SYSTEM OR PLANT MODIFICATIONS	EVALUATION: OPERATIONAL IMPACT	EVALUATION: REGULATORY CONCERNS	EVALUATION: RELATED DAMAGE CONTROL MEASURES	REMARKS
10 Con't	Reactor vessel makeup with the control rod drive pumps (BWR). (Continued)	All other high pressure injection systems (HPCS, HPCI, RCIC and FWCI). (Continued)	CRDHS modified to provide upgraded makeup capability.	C	A (INV)	D	*	C	19, 26	*Unknown.
11	Reactor vessel makeup with low pressure injection systems following depressurization (BWR).	All high pressure injection systems (HPCS, HPCI, RCIC, FWCI, and CRDHS).	LPCS system provides reactor coolant makeup following depressurization.	A	A (INV)	A	A	A	1	Applicable to BWR/2 to BWR/6 plants
			Separate LPCI system provides reactor coolant makeup following depressurization.	A	A (INV)	A	A	A	1	Applicable to BWR/1, BWR/2 and some BWR/3 plants.
			Multi-mode RHR system operates in LPCI mode to provide reactor coolant makeup following depressurization.	A	A (INV)	A	A	A	1	Applicable to BWR/3 to BWR/6 plants.
			Single-mode RHR system modified to provide reactor coolant makeup from the suppression pool following depressurization.	B	A (INV)	C	B	A	1	Applicable to BWR/1, BWR/2 and some BWR/3 plants.
			Single-mode containment cooling system modified to provide reactor coolant makeup from the suppression pool following depressurization.	B	A (INV)	C	B	A	1	Applicable to BWR/1 and BWR/2 plants.
12	Reactor coolant makeup with the main condensate system following depressurization (BWR).	All high pressure and low pressure injection systems (HPCS, HPCI, RCIC, FWCI, CRDHS, LPCS, LPCI, and RHR).	Power restored to condensate system components to reestablish low pressure makeup to the reactor vessel via existing piping.	B	A (INV)	B	B	B	1, 14, 19, 26	

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION: TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	REMARKS
13	Alternate service water system crossconnected to essential service water system (PWR and BWR).	Essential service water system.	Power restored to components in an alternate service water system and cooling to safety-related components reestablished via a crossconnection with the ESW system.	B	A (DHR, SUP)	C	D*	B	7, 19, 26	*If ESW provides diesel generator cooling, otherwise C
14	Feedwater system pumps crossconnected to essential service water system (PWR).	Essential service water system.	Power restored to condensate pumps and cooling to safety-related components reestablished via a crossconnection with the ESW system.	B	A (DHR, SUP)	C	D*	B	12, 19, 26	*If ESW provides diesel generator cooling, otherwise C.
			Auxiliary feedwater pumps crossconnected to ESW system to reestablish cooling for safety-related components.	D*	--	--	--	--	--	*Inadequate flow capability for ESW service.
15	Fire water system pumps crossconnected to essential service water system (PWR and BWR).	Essential service water system.	All fire water pumps crossconnected to ESW system to reestablish cooling for safety-related components.	B	B*	C	D**	C	8, 19, 26	*Cannot match ESW system flow requirements. **If ESW provides diesel generator cooling, otherwise C.
			Fire water pumping capacity upgraded, part of system reserved for fire protection duties and part crossconnected to ESW system to reestablish cooling for safety-related components.	B	A (DHR, SUP)	D	D**	B	-do-	**If ESW provides diesel generator cooling, otherwise C.
16	Essential service water system substituted for component cooling water system (PWR).	Component cooling water system.	ESW supply and return headers crossconnected directly to CCW system piping to provide direct cooling for components normally served by the CCW system.	B	A (DHR, SUP)	C	D*	B	--	*If CCW provides diesel generator cooling, otherwise C.

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION						REMARKS
				TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	
17	Pressurizer and steam generator level indication local readout (PWR).	Remote level instrumentation.	Permanently installed level gauges provided inside containment.	A	A (SUP)	B	A	A	--	
			Permanently installed level gauges provided outside containment.	A	A (SUP)	B	A	B	--	
			Portable, self-powered, calibrated level instrument package connected to existing signal terminals from level transmitters to measure level.	B	A (SUP)	B	B	A	--	
18	Steam generator pressure indication local readout (PWR).	Remote pressure intrumentation.	Existing pressure sensor/transmitter units replaced with units having a local indicator gauge.	A	A (SUP)	3	A	A	--	
			Portable, calibrated pressure gauge connected to existing sensing line.	A	A (SUP)	B	B	A	--	
			Portable, self-powered calibrated pressure instrument package connected to existing signal terminals from pressure transmitters to measure pressure.	B	A (SUP)	B	B	A	--	
			Local pressure gauge installed on main steam piping between containment and main steam isolation valves.	A	A (SUP)	B	A	A	--	

Table 4.6. Summary of Damage Control Measures and Design Changes (Cont nued).

				EVALUATION						
NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	REMARKS
19	Class 1E power supplied to Nonclass 1E equipment (PWR and BWR).	Nonclass 1E power system (and offsite power).	Run temporary three-phase cables to crossconnect selected Class 1E load centers and Nonclass 1E switchgear.	C	A (SUP)	A	C	B	3, 7, 8, 10, 12, 13, 14, 15	
			Provide permanent interconnections to align selected components to either the Nonclass 1E or the Class 1E electric power system.	B	A (SUP)	B	B	C	-do-	
			Permanently supply Nonclass 1E loads from the Class 1E system.	A	A (SUP)	C	B	B	-do-	
20	Crossconnect Class 1E DC load groups (PWR and BWR).	Class 1E battery and battery charger.	Manual bus tie capability provided between Class 1E load groups to reestablish power to safety-related DC loads.	A	A* (SUP)	B**	B	B	--	*Potentially limited by capacity of cross-connected DC source. **If bus ties do not already exist, otherwise A.
21	Crossconnect Class 1E DC load group with a Nonclass 1E DC system (PWR and BWR).	Class 1E battery and battery charger.	Manual bus tie capability provided between the Class 1E and Nonclass 1E DC systems to reestablish power to safety-related DC loads.	B	A* (SUP)	B	B	B	--	*Potentially limited by capa..ity of cross-connected DC source.
22	Alternate DC supply to designated equipment (PWR and BWR).	Class 1E DC load group (or division).	Selectable DC feeders provided to allow designated equipment to be manually aligned to an operable Class 1E DC load group.	A	A* (SUP)	B	B	B	--	*Potentially limited by capacity of alternate DC source.

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

NUMBER	BRIEF DESCRIPTION	SYSTEMS SABOTAGED OR AFFECTED	APPROACH TO DAMAGE CONTROL	EVALUATION: TECHNICAL FEASIBILITY	EFFECTIVENESS	SYSTEM OR PLANT MODIFICATIONS	OPERATIONAL IMPACT	REGULATORY CONCERNS	RELATED DAMAGE CONTROL MEASURES	REMARKS
23	Backup water supplies (PWR).	Normal decay heat removal or reactor coolant inventory control water sources (e.g., condensate and refueling water storage tanks).	Permanently installed cross-connections provided to supply water from alternate sources.	A	A (DHR, INV)	A*	B	A	--	*Adequate backup sources may exist.
24	Backup water supplies (BWR).	Normal decay heat removal or reactor coolant inventory control water sources (e.g., condensate and refueling water storage tanks).	Permanently installed cross-connections provided to supply water from alternate sources.	A	A (DHR)	A*	B	A	2	*Adequate backup sources may already exist. Note that suppression pool is assumed to be available for inventory control.
25	Manual operation of safety-related systems having steam turbine driven pumps (PWR and BWR).	AC power system and DC power for turbine-driven pump auxiliaries.	Auxiliary feedwater system modified for operation without AC or DC power (PWR).	B	A (DHR)	C	C	B	--	
			Reactor core isolation cooling system modified for operation without AC or DC power (BWR).	B	A (INV)	C	C	B	--	
			High pressure coolant injection system modified for operation without AC or DC power (BWR).	C	A (INV)	D	C	C	--	
26	Alternate onsite source of Nonclass 1E power (PWR and BWR).	Nonclass 1E AC power sources (offsite power and main turbine generator) and emergency Class 1E diesel generators.	Large Nonclass 1E combustion turbine generator unit permanently installed onsite and connected to startup bus to supply Class 1E or Nonclass 1E loads as necessary.	A	A (SUP)	D	C	A	3, 7, 8, 10, 12, 13, 14, 15	
27	Manual startup and loading of diesel generator (PWR and BWR).	DC power for diesel generator control system	Diesel generator auxiliary systems modified for startup and loading without AC or DC power.	C	A (SUP)	B	C	A	--	

Table 4.6. Summary of Damage Control Measures and Design Changes (Continued).

Notes:
1. AFW = auxiliary feedwater system
2. CCW = component cooling water system
3. CRDHS = control rod drive hydraulic system
4. ESW = essential service water system
5. FWCI = feedwater coolant injection system
6. HPCI = high pressure coolant injection system
7. HPCS = high pressure core spray system
8. LPCI = low pressure coolant injection system
9. LPCS = low pressure core spray system
10. RCIC = reactor core isolation cooling system
11. RCS = reactor coolant system
12. RHR = residual heat removal system
13. RWCU = reactor water cleanup system
14. SI = safety injection system
15. TBS = turbine bypass system

Damage control measures which may be implemented with relatively low technical risk and impact are those that are ranked as "A" or "B" in all categories except "Effectiveness." Damage control measures with higher technical risk or impact are ranked as "C" or "D" in one or more categories. This ranking was, of necessity, based on a review of the systems and design features of a limited set of nuclear power plants. Plant-specific considerations may have a very strong effect on the technical feasibility and impacts of each of the proposed damage control measures. Table 4.6 should therefore be considered only as a tool for performing a first-order screening of damage control measures as a prelude to further studies or plant-specific applications.

A summary of the damage control measures that may apply to PWR systems is presented in Table 4.7. Damage control measures potentially applicable to BWR systems are listed in Table 4.8. These tables were abstracted from Table 4.6. The individual evaluations in Section 5 provide additional information, when necessary, to identify the specific operating plants for which a damage control measure may be applicable. Note in Tables 4.7 and 4.8 that some systems are considered for use in more than one damage control measure. In actual practice, some alternate alignments for a given system are mutually exclusive, and a selection must be made regarding the damage control application of the system.

4.2 CONCLUSIONS

Damage control can make a useful contribution to sabotage protection in nuclear power plants, not as a stand-alone measure, but as an element in an integrated sabotage protection system. Through the use of damage control, diverse systems can be aligned and operated to restore functional capabilities that have been lost or degraded following sabotage of a specific set of safety-related systems or equipment. The range of damage control measures evaluated in this report provides insight into potential applications and into the engineering, operational and regulatory impacts that may be encountered when implementing these measures.

Table 4.7. Damage Control Measures and Design Changes Evaluated for PWR Systems.

System	Damage Control Measure	Description[1]
Auxiliary feedwater system	25	Modify system for operation without AC or DC power[2]
High pressure safety injection system	4	Crossconnect to substitute for AFW system[3]
	9	Modify for high pressure injection using tandem HPSI pumps[3]
Main steam overpressure protection system	5	Add redundant set of safety valves
Safety-related display instrumentation	17	Provide local indications of pressurizer and steam generator level
	18	Provide local indication of steam generator pressure
AC electric power system	19	Reenergize Nonclass 1E loads from the Class 1E AC system
	26	Add an alternate onsite source of Nonclass 1E power
	27	Modify diesel generators for startup and loading without AC or DC power[2]
DC electric power system	20	Add or utilize existing bus tie capability between Class 1E DC load groups[2]
	21	Reenergize Class 1E DC load group from a Nonclass 1E DC system[2]
	22	Provide load transfer capability for selected DC loads[2]

Table 4.7. Damage Control Measures and Design Changes Evaluated for PWR Systems. (Continued)

System	Damage Control Measure	Description(1)
Essential service water system	16	Crossconnect for direct cooling of components served by a CCW system
Plant (nonsafety) service water system	13	Modify to operate following loss of offsite power and crossconnect to substitute for ESW system
Fire water system	15	Modify to be fully operable following loss of offsite power and crossconnect to substitute for ESW system
Main feedwater system	3	Modify turbine-pump train to operate following loss of off-site power and use as substitute for AFW system
Condensate system	14	Modify to operate following loss of offsite power and crossconnect to substitute for ESW system
Backup water sources	23	Modify for rapid alignment of alternate sources of water for decay heat removal or coolant inventory control

Notes: (1) AFW = auxiliary feedwater system, HPSI = high pressure safety injection system, CCW = component cooling water system, ESW = essential service water system.

(2) DC system modifications (damage control measures #20, #21, or #22) may be an alternative to redesigning AFW system or diesel generator to operate without DC power (damage control measures #25 and #27 respectively).

(3) Damage control measures #4 and #9 are mutually exclusive.

Table 4.8. Damage Control Measures and Design Changes Evaluated for BWR Systems.

System	Damage Control Measure	Description[1]
High pressure coolant injection system	2	Modify for suppression pool feed-and-bleed cooling[2]
	6	Utilize existing capability as a high pressure coolant makeup system[2]
	25	Modify system to operate without AC or DC power[3]
High pressure core spray system	2	Modify for suppression pool feed-and-bleed cooling[2]
	6	Utilize existing capability as a high pressure coolant makeup system[2]
Reactor core isolation cooling system	25	Modify system to operate without AC or DC power[3]
Control rod drive hydraulic system	10	Utilize existing capability or modify for upgraded capability as a high pressure coolant makeup system
Automatic depressurization system	1	Modify system for local manual operation of safety/relief valves
Low pressure core spray system	11	Utilize existing capability as a low pressure coolant makeup system (with ADS)
Residual heat removal system (multi-mode)	11	Utilize existing capability as a low pressure coolant makeup system (LPCI mode with ADS)
Low pressure coolant injection system (separate system)	11	Utilize existing capability as a low pressure coolant makeup system (with ADS)

Table 4.8. Damage Control Measures and Design Changes Evaluated for BWR Systems. (Continued)

System	Damage Control Measure	Description[1]
Residual heat removal system (single-mode)	11	Modify system for low pressure coolant makeup capability
Containment cooling system (single-mode)	11	Modify system for low pressure coolant makeup capability
Suppression pool makeup system	2	Utilize existing capabilities for suppression pool feed
AC electric power system	19	Reenergize Nonclass 1E loads from the Class 1E AC system
	26	Add on alternate onsite source of Nonclass 1E power
	27	Modify diesel generators for startup and loading without AC or DC power[3]
DC electric power system	20	Add or utilize existing bus tie capability between Class 1E DC load groups[3]
	21	Reenergize Class 1E DC load group from a Nonclass 1E DC system[3]
	22	Provide load transfer capability for selected DC loads[3]
Plant (nonsafety) service water system	7	Modify to operate following loss of offsite power and crossconnect to supply RHR heat exchangers (e.g., substitute for ESW system)
	13	Modify to operate following loss of offsite power and cross-connect to substitute for entire ESW system

Table 4.8. Damage Control Measures and Design Changes Evaluated for BWR Systems. (Continued)

System	Damage Control Measure	Description(1)
Fire water system	8	Modify to be fully operable following loss of offsite power and crossconnect to supply RHR heat exchangers (e.g., substitute for ESW system)
	15	Modify to be fully operable following loss of offsite power and crossconnect to substitute for entire ESW system
Condensate system	16	Modify to operate following loss of offsite power and use as substitute low pressure coolant makeup system
Refueling water transfer system	2	Modify to operate following loss of offsite power and for suppression pool feed-and-bleed cooling
Backup water sources	23	Modify for rapid alignment of alternate water sources of water for decay heat removal or coolant inventory control

Notes: (1) ADS = automatic depressurization system, LPCI = low pressure coolant injection, RHR = residual heat removal system, ESW = essential service water system.

(2) Damage control measures #2 and #6 are mutually exclusive.

(3) DC system modifications (damage control measures #20, #21 or #22) may be an alternative to redesigning HPCI system, RCIC system or diesel generators to operate without DC power (damage control measures #25 and #27).

Many of the design features necessary to implement damage control measures are not commonly found in current nuclear power plant designs. Therefore, damage control opportunities with currently available resources may be somewhat limited.

For damage control to be effective, the design features necessary to establish crossconnections or to operate systems in alternate modes must be permanently installed and available on short notice to operating personnel. Design features such as fluid system crossconnections and electrical system bus ties must be carefully engineered to ensure that the separation, independence and reliability of safety-related systems are not adversely affected by damage control measures. Requirements for separation and independence have been considered in the design changes proposed in this report. Effects of these design changes on the reliability of safety-related systems and on nuclear power plant risk have not been evaluated.

5. EVALUATION OF INDIVIDUAL DAMAGE CONTROL MEASURES

Engineering evaluations of twenty-seven damage control measures are presented in this section. Each evaluation is presented as an individual subsection, using the following standard format.

- Title and brief description of the basic damage control concept.
- Sabotage scenario - a description of the postulated sabotage events which the damage control measure is intended to mitigate.
- System descriptions - description of the functional capabilities of systems associated with the postulated sabotage scenario.
- Plant conditions during sabotage scenario - description of the plant response to the postulated sabotage scenario.
- System alignment or design changes necessary to implement the damage control measure.
- Technical and regulatory impediments to implementing the damage control measure.
- Summary and conclusions regarding the damage control measure.
- References

To the extent practical, each evaluation discusses the potential applicability of the damage control measure to specific nuclear power plants.

5.1 DAMAGE CONTROL MEASURE #1 - BWR

The purpose of damage control measure #1 is to provide manually operated relief valves for depressurizing the reactor vessel. This capability would allow operation of the low pressure injection or residual heat removal (RHR) systems in the event that automatic or remote-manual operation of the automatic depressurization system (ADS) is prevented by sabotage action.

5.1.1 Sabotage Scenario

Loss of offsite power is assumed to occur coincidentally with the successful sabotage of the ADS. The main turbine generator trips on loss of load. The emergency diesel generators operate to supply AC power to the Class 1E buses. The systems not dependent upon offsite power are assumed to operate normally, with the exception of the high pressure injection systems which will include one or more of the following; Reactor Core Isolation Cooling (RCIC) System, High Pressure Core Spray (HPCS) System, High Pressure Coolant Injection (HPCI) System, the Feedwater Coolant Injection (FWCI) System and the Control Rod Drive Hydraulic System (CRDHS). The unavailability of the high pressure injection systems creates the need for ADS actuation and operation of the low pressure injection systems, such as the Low Pressure Core Spray (LPCS) System, Low Pressure Coolant Injection (LPCI) System or the Residual Heat Removal (RHR) System.

5.1.2 Normal Operation of Pressure Relief Valves for Reactor Coolant System Depressurization (based on descriptions in NUREG 0625)

All light water reactors are required to have some means of relieving reactor primary system pressure in order to prevent overpressurization. This protection takes the form of pressure relief valves which are set to open when the primary system pressure reaches predetermined setpoints. Early BWR plants use two separate types of valves for overpressure protection -- relief valves and safety valves. The relief valves are power-actuated at a pressure below the mechanical safety valve setpoint. Pressure relief systems in later BWR plants use one type of valve, a safety/relief valve (SRV). The SRVs are power-actuated when operating as relief valves and are mechanically opened by primary system pressure when operating as safety valves. Table 5.1.1 summarizes the pressure relief valve complement of BWRs.

In addition to the overpressure protection function, relief valves and SRVs are required to perform another function; i.e., automatic depressurization. Automatic depressurization of the primary system is required in the event of a small-break LOCA where the system pressure remains high and the plant has no high pressure emergency core cooling system (ECCS) capable of injecting water into the system to cool the core, either as a result of high pressure ECCS failure or because the plant has no system available. Automatic ADS actuation typically requires a coincidence of low reactor water level and high drywell pressure (e.g., conditions typical of a LOCA). The ADS logic has two independent channels, "A" and "B", either of which can cause ADS valve operation. Remote manual ADS actuation can be accomplished via remote manual switches in the channel A and B logic, or by individual control switches for each ADS valve. For plants with high pressure ECCS, the ADS operates only in the event of failure of the high pressure ECCS. For plants without a high pressure ECCS, the ADS system actuates to reduce primary system pressure to allow core cooling by means of low pressure cooling systems. Generally, in the older plants, the ADS system uses "electromatic" relief valves while the newer plants use a number of the SRVs for the ADS function.

The separate relief valves used in the earlier plants noted above were power-actuated valves manufactured by the Dresser Company, commonly known as "electromatic" valves (shown in Figure 5.1.1, from Ref. 1). These valves should actually be termed solenoid-operated, power-actuated relief valves since they operate as follows: System steam at pressure is applied to the main valve disk at the valve inlet (Chamber A), passing upward around the disc guide in Chamber B, also entering Chamber C through a clearance space between the main valve disc and disc guide. The main valve disc is held against the seat, in the closed position, by the steam pressure in Chamber C. Actuation is accomplished by energizing the solenoid assembly which then moves the pilot operating lever, moving the pilot valve disc and allowing steam from Chamber C to escape, reducing the pressure in Chamber C. Resulting differential pressure on the main valve disc causes it to open, allowing steam to escape from Chamber B to the outlet of

Table 5.1.1. BWR Plant Pressure Relief Valve Complements.[1]

BWR Type	Facility	Safety/Relief Valves[2]	Safety Valves	Power-Actuated Relief Valves[2]
2	Nine Mile Point	-	16	6
2	Oyster Creek	-	16	5
3	Dresden 2 & 3	1	8	4
3	Millstone 1	6	-	-
3	Monticello	7	-	-
3	Pilgrim 1	4	2	-
3	Quad Cities 1 & 2	1	8	4
4	Browns Ferry 1, 2, & 3	11	2	-
4	Brunswick 1 & 2	11	-	-
4	Cooper	8	3	-
4	Duane Arnold	6	2	-
4	Fitzpatrick	11	-	-
4	Hatch 1 & 2	11	-	-
4	Peach Bottom 2 & 3	11	2	-
4	Vermont Yankee	4	2	-
5,6	Grand Gulf (typical)	19 (typical)	-	-

Notes: [1]Based on Table B-1 in NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant-Accidents in GE-Designed Operating Plants and Near-Term Operating Liceense Applications."

[2]Valves capable of providing ADS function.

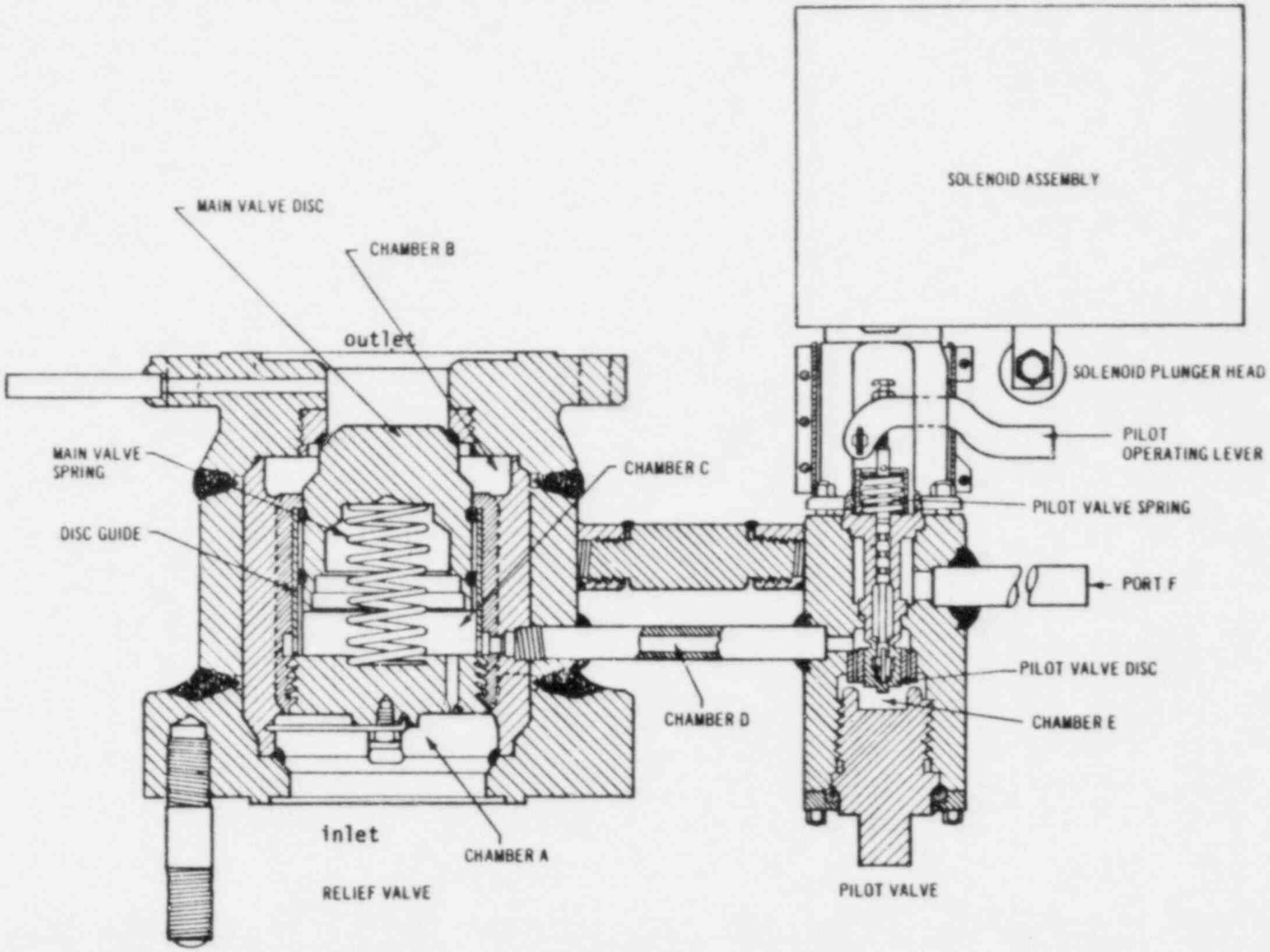


Figure 5.1.1. Power-Actuated Relief Valve (from NUREG 0626).

the valve. Typical capacity of each relief valve of this type is in the range from 400 to 600 Klb/hr at the lowest relief setpoint (Ref. 1).

SRVs in the operating plants are usually three-stage Target Rock valves (Figure 5.1.2, from Ref. 1). In either the ADS mode or relief mode, air or nitrogen is admitted to the chamber above the air actuator at the top of the valve. This differential pressure drives the actuator downward, moving the second stage piston spring and disc downward, thereby unseating the second stage disc. This action relieves the pressure from above the main valve piston with system pressure acting both to force the main valve disc down against the seat and to force the main valve piston upward. Since the diameter of the piston is greater than that of the disc, the net force is upward, opening the valve. Self-actuation occurs when sufficient system pressure enters the pilot sensing port to cause the bellows to expand. This eliminates the abutment gap, pulling the pilot disc from its seat and allowing system pressure to enter the volume above the second stage piston forcing the second stage piston down. This action unseats the second stage disc thereby relieving system pressure above the main valve piston and opening the valve. Typical capacity of each SRV of this type is in the range from 800 to 900 Klb/hr at the lowest relief setpoint (Ref. 1).

SRVs in more recent plants (e.g., BWR/5 and BWR/6 plants, not yet licensed), use direct system pressure against a spring-loaded valve disc for safety actuation. An exterior cylinder, actuated pneumatically (usually air or nitrogen) opens the valve mechanically in the relief mode or ADS mode by means of a lever connected to the main valve disc (Figure 5.1.3; from Ref. 2). Typical capacity of each SRV of this type is also in the range from 800 to 900 Klb/hr at the lowest relief setpoint (Ref. 1).

A typical pneumatic supply system for an SRV with an ADS capability is illustrated in Figure 5.1.4. Remote actuation of each SRV is controlled by three normally deenergized solenoid valves. Energizing any solenoid valve will admit high pressure air or nitrogen to the SRV remote air actuator (see Figures 5.1.2 and 5.1.3) to actuate the SRV. Solenoid A is actuated automatically by the "A" channel of the ADS or pressure relief logic, and is powered from 125 VDC Division 1. Solenoid B is actuated by the "B" channel of the ADS or pressure relief logic, and is powered by 125 VDC Division 2. Solenoid C is manaully actuated via

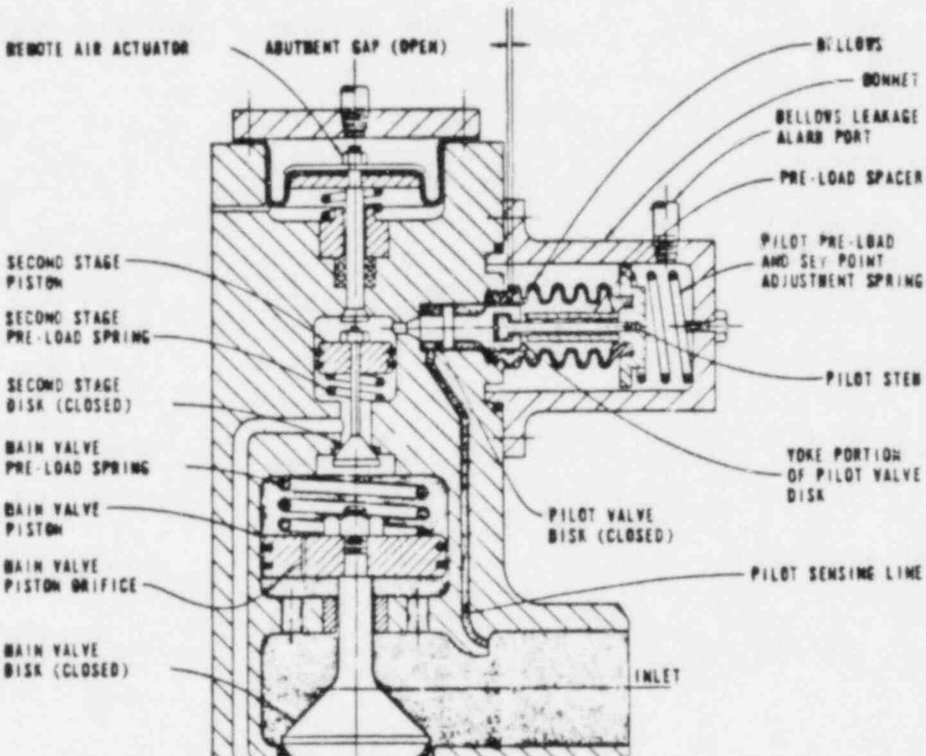


Figure 5.1.2. Three-Stage Pilot-Operated Pressure Relief Valve (from NUREG 0626).

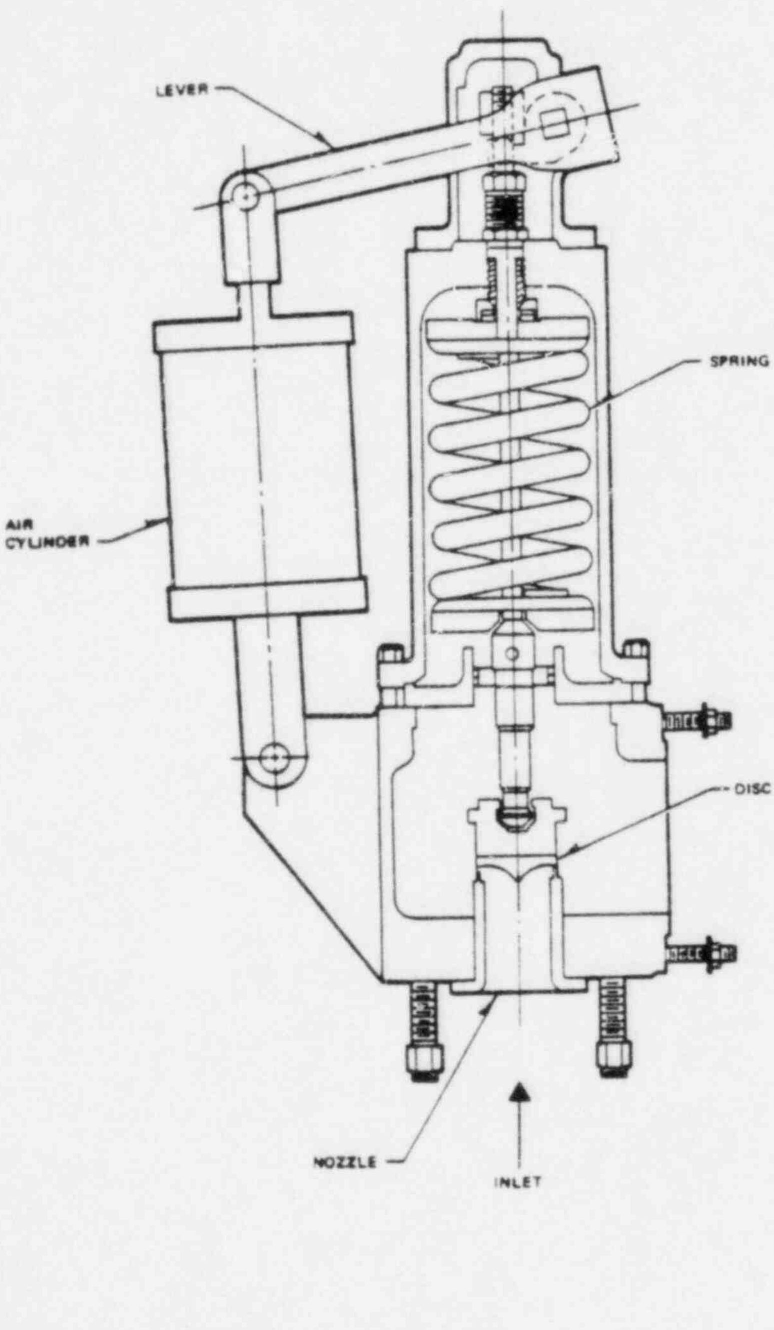


Figure 5.1.3. Safety/Relief Valve with External
Actuating Device (from 238 GESSAR).

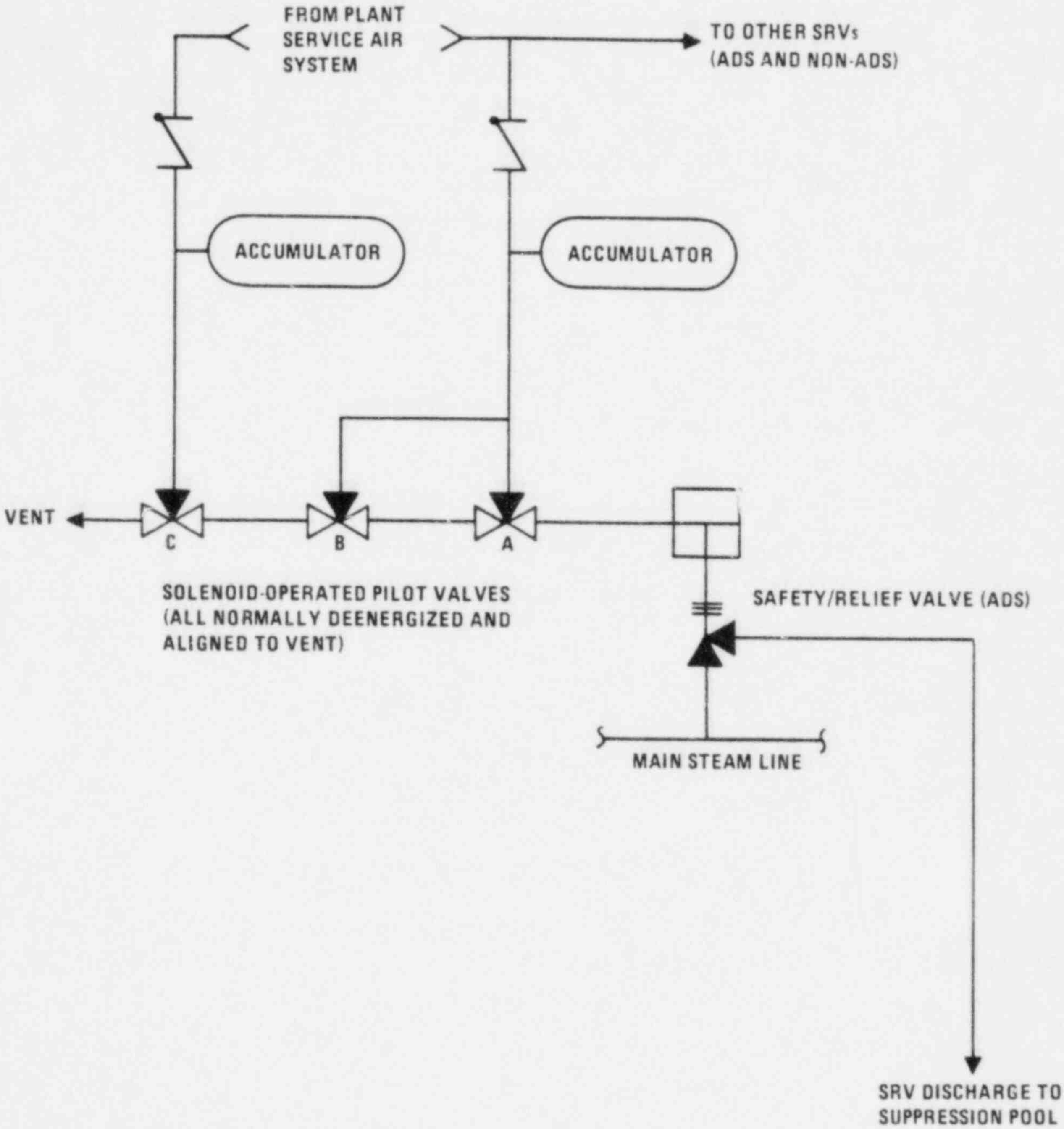


Figure 5.1.4. Typical Pneumatic Supply System For an ADS Valve.

multiple control room switches and is powered by 125 VDC Division 1. An accumulator is provided in the air supply line for each SRV. The accumulator permits one or two actuations of the SRV in the event that the normal high pressure air system is unavailable.

5.1.3 Plant Conditions During Sabotage Scenario

Loss of offsite power causes a loss of the normal feedwater system. The high pressure injection systems (RCIC, FWCI, HPCS, HPCI, CRDHS) are unavailable, thereby creating the need to depressurize the reactor and use the low pressure injection systems to maintain reactor coolant inventory. The ADS has been sabotaged to prevent automatic and remote-manual opening of the SRVs. The reactor coolant system will likely remain at high pressure (e.g., at or near the SRV mechanical relief setpoints which typically range from approximately 1165 psig to 1250 psig). Coolant inventory will be lost via SRV blowdown to the suppression pool.

NUREG-0626 (Ref. 1) describes BWR plant response to a variety of feed water transients and loss-of-coolant accidents (LOCAs). The accident scenario most comparable to the sabotage scenario postulated in this section is a loss of feed water transient coincident with the loss of high pressure emergency core cooling systems. The reactor coolant system initially pressurizes to the SRV setpoint and then stabilizes at high pressure (e.g., at or below the SRV setpoint). With manual ADS actuation 19 minutes into the transient, it was calculated that only the top 0.8 feet of the core would be uncovered for approximately 10 seconds.

Based on BWR operating history discussed in NUREG-0626 (Ref. 1), a relief valve failure to close has been recorded 30 times in 187 cases of relief valve challenges over a three year period (e.g., probability of 0.16 per challenge). With this relatively high probability of occurrence, it is possible that, without further sabotage actions, the feedwater transient described above could develop into a feed water transient plus LOCA (e.g., due to a stuck open relief valve). With failure of the high pressure emergency core cooling systems, it has been calculated (Ref. 1) that the time available to actuate the ADS in order to prevent the onset of core uncovery could be as short as 3 minutes under these circumstances.

It has been estimated that the reactor core will be uncovered to its midplane in 1.4 hours following a total station blackout and loss of makeup to the reactor vessel (Ref. 3). This scenario approximates the sabotage scenario postulated in this section, and suggests that an hour or more may be available for operator action before the onset of core melting. WASH-1400, Appendix VIII (Ref. 4) describes BWR core melt processes and estimates core melt times for a variety of boiloff and LOCA conditions, none of which are directly comparable to the scenario postulated in this section. Detailed quantification of the time available for local manual operator actuation of the ADS to prevent core melt is therefore not possible without further analysis.

5.1.4 ADS Valve Design Features To Facilitate Operation In A Manual Mode

Manual handwheel actuators can be added to operate any of the SRVs described in this section. The Target Rock SRV (Figure 5.1.2) is available with a handwheel actuator, but typically for applications where remote actuation is not required. A possible modification of this type of valve to facilitate local manual actuation of the ADS is illustrated in Figure 5.1.5. The lead screw is normally retracted, and does not interfere with normal SRV operation. During local manual operation, the lead screw is inserted into the SRV by operating the handwheel. Contact is made with the valve actuator which is driven downward by the lead screw, moving the second stage piston spring and disc downward and causing the SRV to open as described previously. A similar type of modification could be made to manually operate the power-actuated relief valve in Figure 5.1.1 (e.g., a manually operated lead screw acting directly on the pilot valve stem).

Manual operation of the SRV in Figure 5.1.3 could be accomplished by extending the top of the valve stem, adding a second dog and connecting the dog shaft to a reach rod and handwheel using a set of bevel gears as shown in Figure 5.1.6. Operation of the handwheel would rotate the dog shaft, causing the manually operated dog to lift the valve stem and open the SRV.

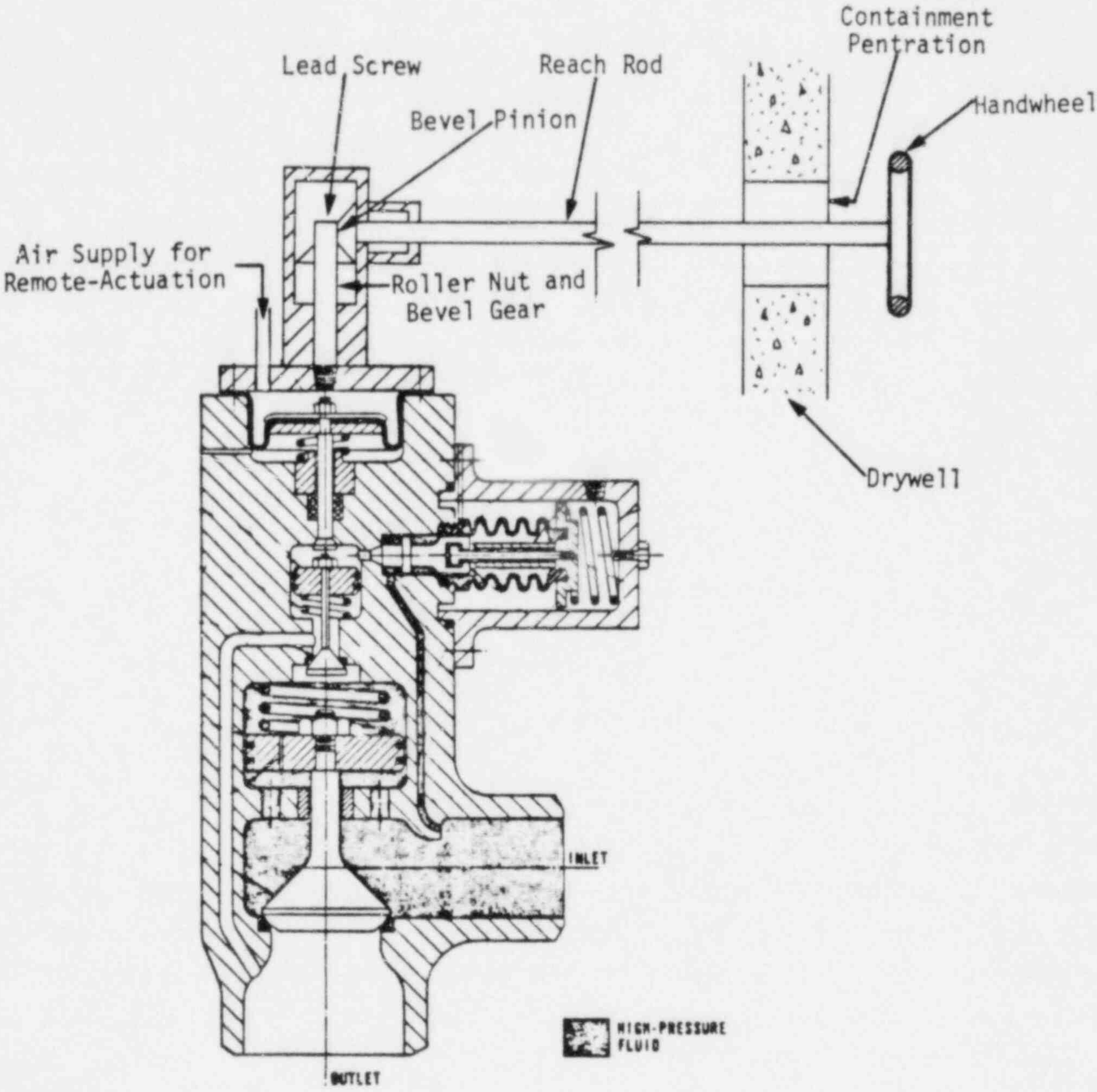


Figure 5.1.5. Three-Stage Pilot -Operated Pressure Relief Valve Modified for Local Manual Operation.

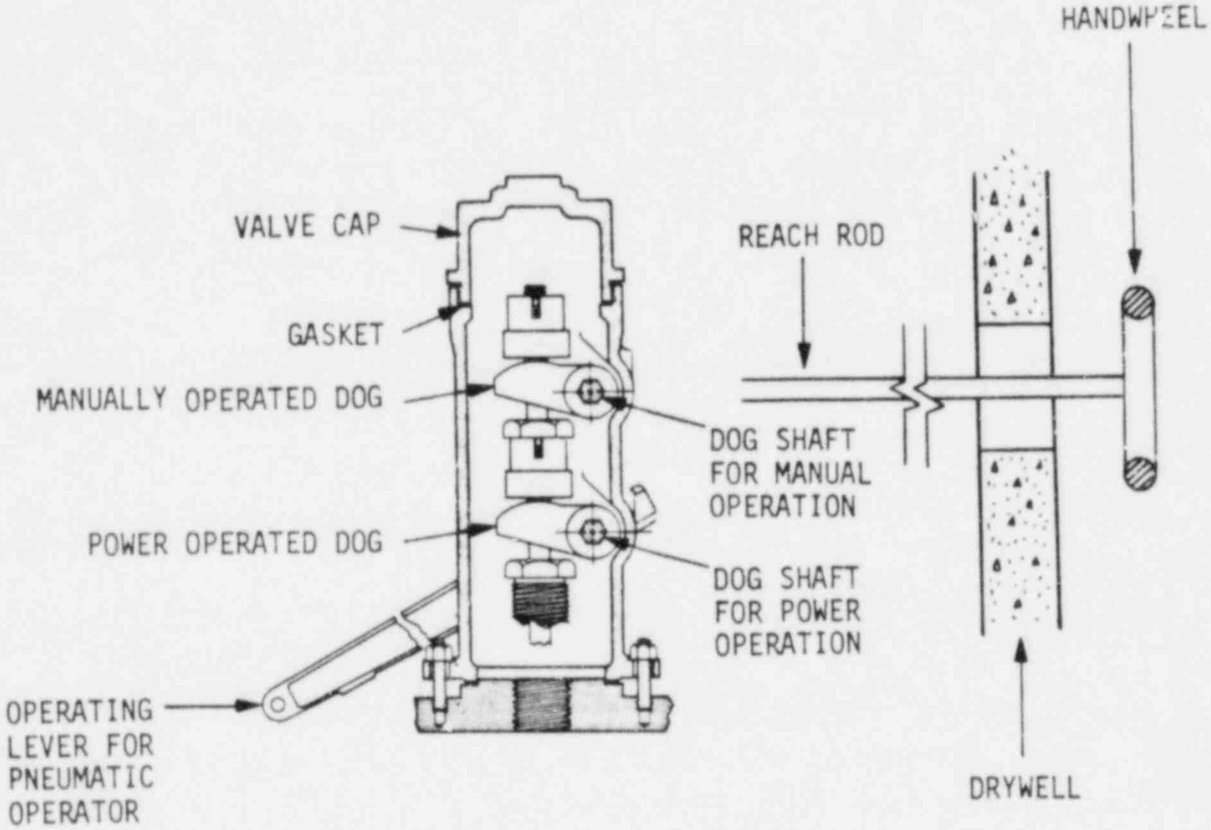


Figure 5.1.6. Safety Relief Valve With External Actuating Device, Modification of Valve Bonnet for Local Manual Operation.

The SRVs are located in the drywell, as illustrated in Figure 5.1.7. In a typical BWR/6, only 8 (2 per steam line) of 19 SRVs are actuated by the ADS. A comparable number may require the local manual actuation capability. With the relief valve and SRV capacities discussed previously, this adds up to a very large initial blowdown. The specific valves could be selected to simplify the installation of the reach rods for valve operation from outside the drywell and to minimize the requirements for angle gears to get around other equipment. Flexible shafts may be a possible alternative to rigid reach rods, thereby eliminating the need for angle gears. It may also be necessary to select SRVs to maintain a symmetrical blowdown to the suppression pool. If this is necessary, manual operation of the SRVs could not be accomplished from a single location. At least two valve stations in the reactor building (one on each side of the drywell) would be required. During normal operation the valves at these stations require physical protection because of the possibility of initiating a LOCA by opening these valves when reactor coolant system depressurization is not desired.

It may be possible to design the containment penetrations for each SRV reach rod in a manner comparable to the rotating shaft penetrations commonly used in containment airlocks. Typically, shafts penetrating airlocks are sealed by multiple seals as illustrated in Figure 5.1.8.

5.1.5 Other Approaches for Depressurizing the Reactor Coolant System

Other potential methods for depressurizing a BWR following failure of the high pressure injection systems and the ADS are described in NUREG/CR-2100 (Ref. 5). These methods are discussed below.

5.1.5.1 Dump Steam to the Main Condenser

The main steam isolation valves (MSIVs) close automatically on low reactor vessel water level. To dump steam to the main condenser in this condition, it would be necessary to override containment isolation and reopen the MSIV bypass valves and then the MSIVs. Also, it would be necessary to reestablish condenser vacuum using an electric hogging pump and/or the steam jet air ejectors. With vacuum restored, and a portion of the main circulating water system operating, the turbine bypass system could then be used to dump steam to

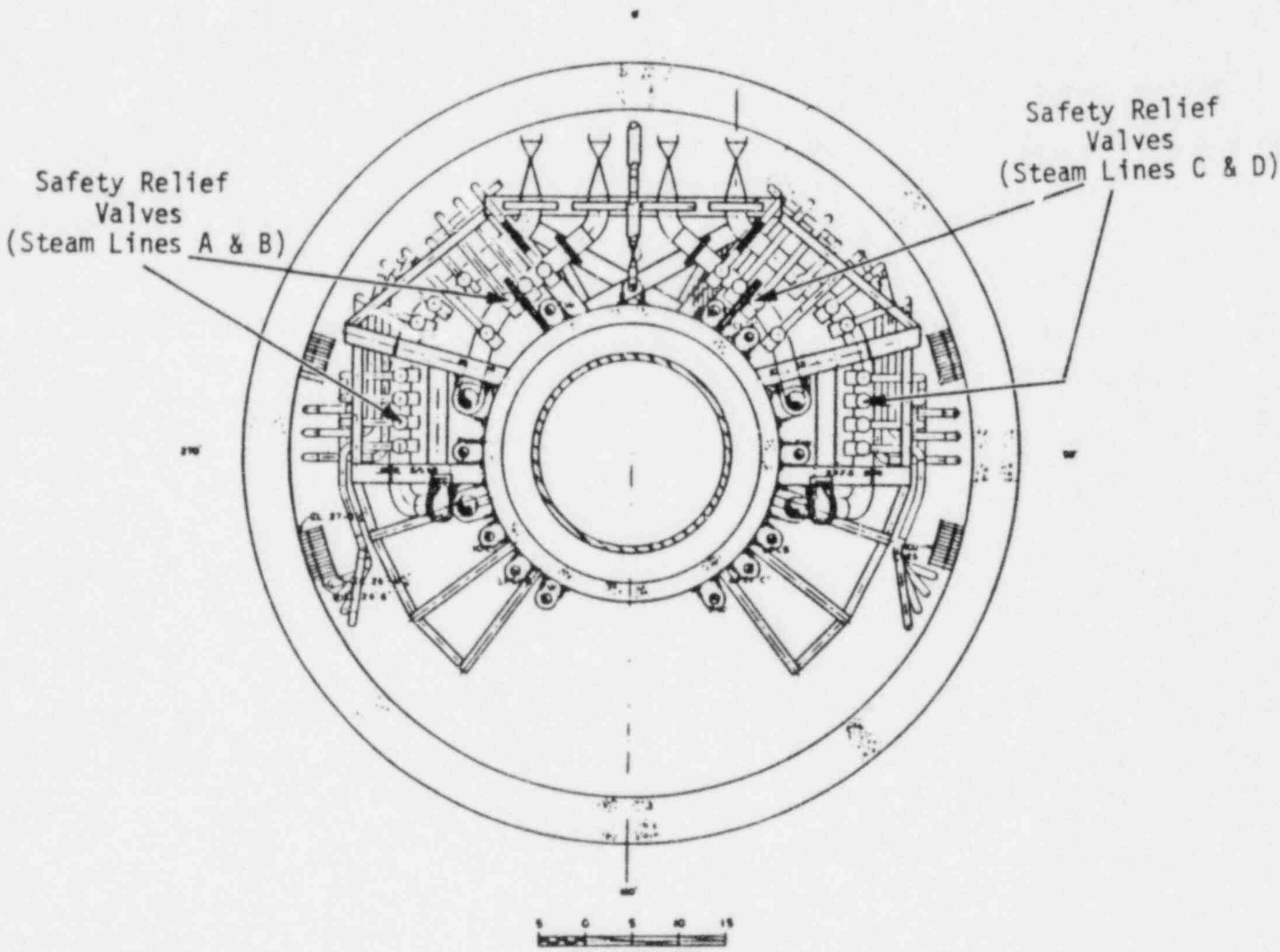


Figure 5.1.7. Typical SRV Location in the Drywell.

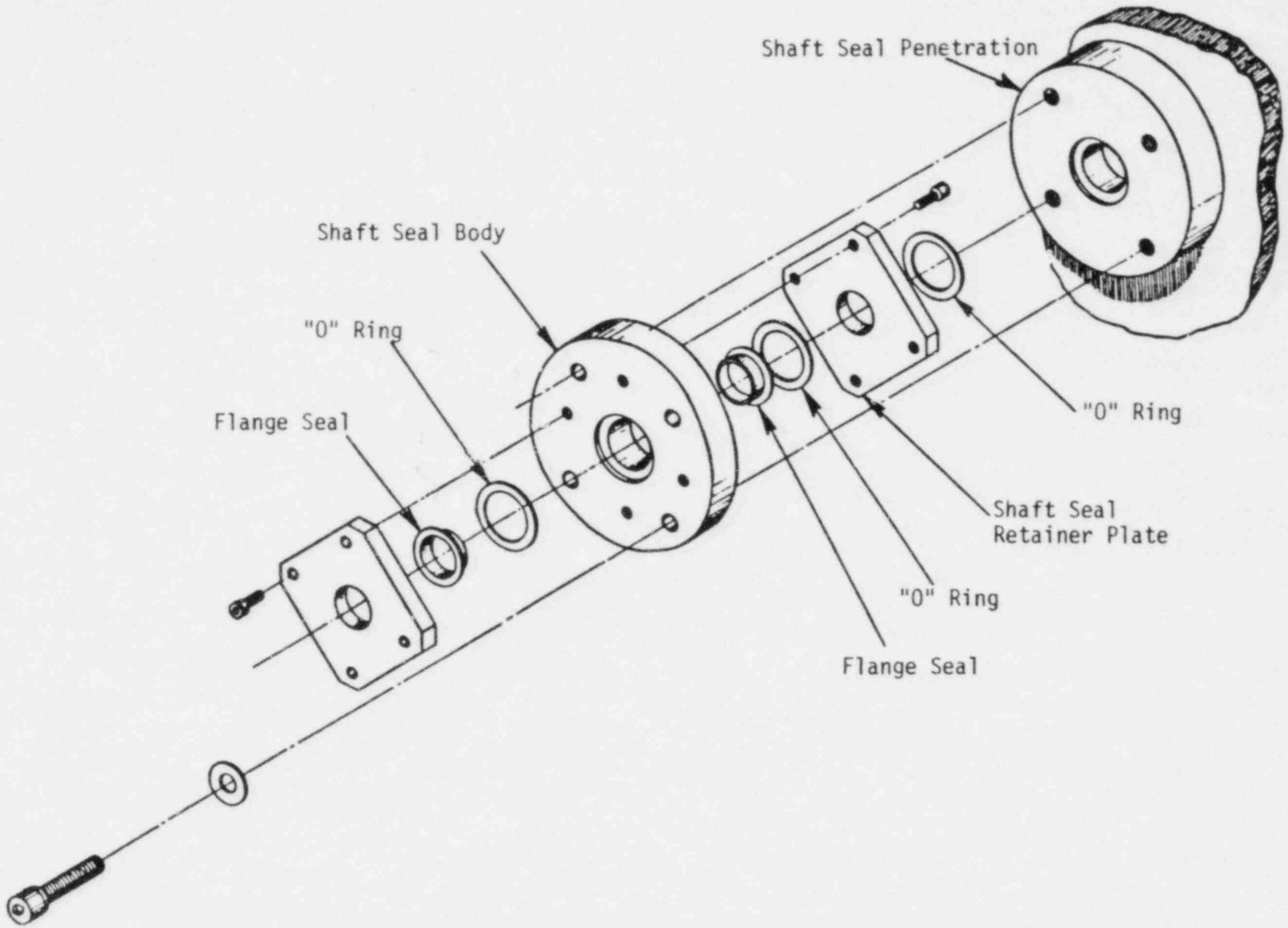


Figure 5.1.8. Containment (Airlock) Penetration Design for a Rotating Shaft.

the main condenser and thereby depressurize the reactor coolant system at a rate comparable to the ADS. A significant number of Nonclass IE components are required to implement this damage control measure. It is unlikely that all of these components could be supplied from the diesel generators. If offsite power cannot be restored it may be possible to supply necessary components from an onsite nonclass IE source such as a standby gas turbine generator (see damage control measure #26). It is unlikely that this approach could provide the timely response required.

5.1.5.2 Blowdown the Reactor Coolant System to the Main Condenser Via the Reactor Water Cleanup (RWCU) System

The RWCU system can be aligned to blowdown reactor coolant from the suction side of the reactor coolant recirculation lines to the main condenser (see Figure 5.1.9). Piping sizes in the RWCU system vary, but nominally are 4 inches in diameter. To maximize blowdown flowrate, a bypass line could be installed from the suction of the RWCU pumps to the blowdown line to the main condenser (see Figure 5.1.9). Even with this bypass line, blowdown rate would not exceed that of a 4 inch break (0.087 ft^2 break) at the interface of the RWCU with the recirculation suction line.

NUREG-0626 (Ref. 1) analyzed the case of a 0.1 ft^2 break in the recirculation suction line. With this size break, the reactor coolant system remained at high pressure and ADS operation was required to permit coolant injection by low pressure systems. Blowdown of reactor coolant via the RWCU system would therefore not be a viable alternative for depressurizing the reactor following high pressure injection system and ADS failure.

5.1.5.3 Discharge Steam to the Suppression Pool Via The HPCI and/or RCIC Pump Turbines

The HPCI and/or RCIC systems are assumed to be sabotaged so that makeup water can not be delivered to the reactor coolant system at high pressure. If the turbines can still be operated following the sabotage event, reactor-generated steam could be exhausted to the suppression pool via the turbine drives. An RCIC turbine is typically rated at 460 to 925 horsepower. Maximum RCIC turbine steam flow rate is in the 30 to 40 Klb/hr range (Ref. 2). A

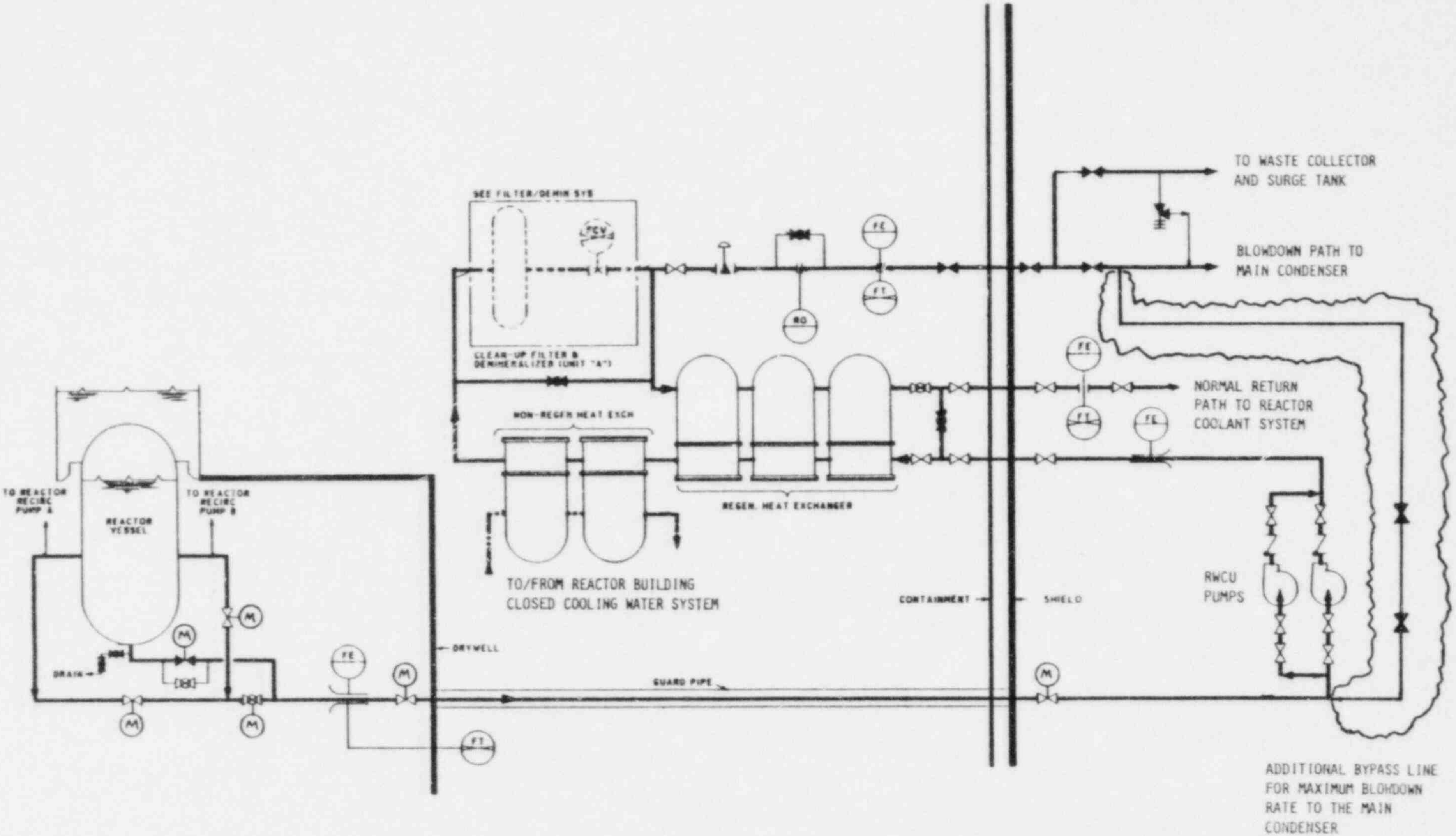


Figure 5.1.9. Reactor Water Cleanup System, Process Diagram.

HPCI turbine may be rated between 2675 to 4600 horsepower. The maximum HPCI turbine steam flow would likely be in the 120 to 150 Klb/hr range. For BWR plants with both HPCI and RCIC pumps, the combined maximum steam flow through the turbines would be 22 to 47 percent of the relief capacity of a single relief valve. The turbine governor valves would limit actual steam flow through the turbines to much less than this value for many sabotage modes of the HPCI and RCIC system (e.g., if the pump is operating at shutoff head with no flow in the system).

As noted, NUREG-0626 (Ref. 1) equated a stuck-open relief valve to a 0.1 ft^2 steam line break. Without high pressure injection systems operating, ADS actuation was required. Discharge of steam through the HPCI and/or RCIC turbines would equate to a much smaller steam line break and therefore the reactor coolant system would remain at high pressure.

5.1.6 Technical And Regulatory Impediments to Implementing Damage Control Measure #1

The technical aspects of incorporating a local manual operating capability into SRV design appears to be compatible with the requirements of the ASME Boiler and Pressure Vessel Code, Section III, Division 1, Article NB-7000, "Overpressure Protection." Installing this capability on BWR SRVs does, however, create a significant new physical protection problem by providing the insider saboteur with another means for initiating a LOCA without the need for explosives. The manual handwheels provide a very simple means for initiating a broad spectrum of LOCAs, depending on the number of valves that are opened by the saboteur. Physical protection of the SRV manual handwheels will, therefore, be an important consideration.

Other than valves associated with airlocks, manual valves operated with reach rods penetrating the containment are not commonly found in nuclear power plants. Regulatory concerns associated with the integrity of the new containment penetrations under accident conditions are certain to arise. In particular, it will be necessary to demonstrate that the new containment penetrations do not: (a) reduce the failure limits of the containment structure, or (b) increase the leak rate of the containment.

5.1.7 Conclusions and Recommendations Regarding Damage Control Measure #1

There appears to be at least one technically feasible approach for manually depressurizing the reactor vessel to permit operation of low pressure coolant injection systems. Moderate plant modifications are required to implement this damage control measure. The time available for operator response is judged to be marginal, and the reactor core will probably be partially uncovered before or during manual depressurization.

5.1.8 Section 5.1 References

1. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January, 1980.

2. "238 Nuclear Steam Supply System-GESSAR," Docket STN-50550, General Electric Company.

3. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

4. WASH-1400, "Reactor Safety Study," Appendix VIII, "Physical Processes in Reactor Meltdown Accidents," U. S. Nuclear Regulatory Commission, October 1975.

5. Brown, R. G. and vonHerrmann, J., "Boiling Water Reactor Status Monitoring During Accident Conditions," NUREG/CR-2100, Science Applications, Inc., April 1981.

5.2 DAMAGE CONTROL MEASURE #2 - BWR

The purpose of damage control measure #2 is to supply cooling to the suppression pool using a feed-and-bleed technique in the event that suppression pool cooling systems are disabled through sabotage action.

5.2.1 Sabotage Scenario

Loss of offsite power occurs and the main turbine generator trips on loss of load. The emergency diesel generators operate to supply AC power to the Class 1E buses. Suppression pool cooling systems have been sabotaged, but other safety-related systems operate normally.

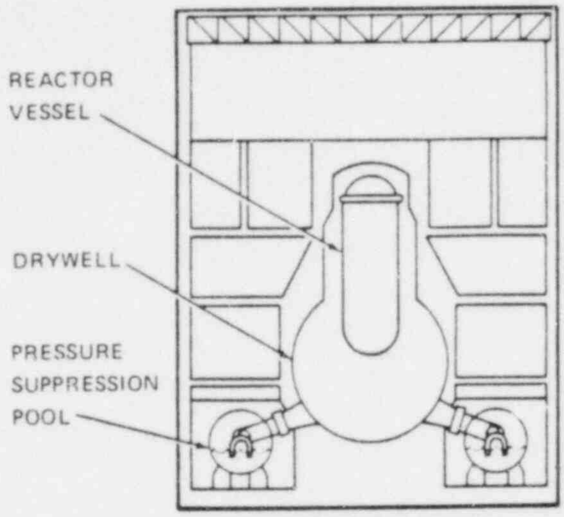
5.2.2 System Descriptions

5.2.2.1 BWR Pressure Suppression Containment

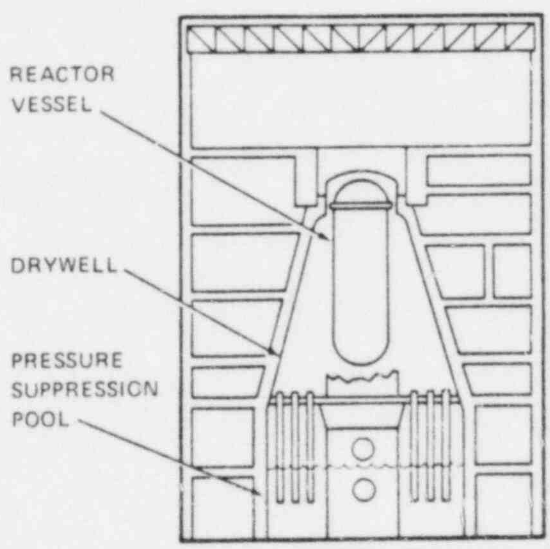
The three major BWR containment designs are designated Mark I, Mark II, and Mark III. These containment designs are illustrated in Figure 5.2.1 and selected parameters related to suppression chamber design are compared in Table 5.2.1.

The pressure suppression pool is a standby passive heat sink which maintains a large water volume to absorb heat and quench steam from the following major sources:

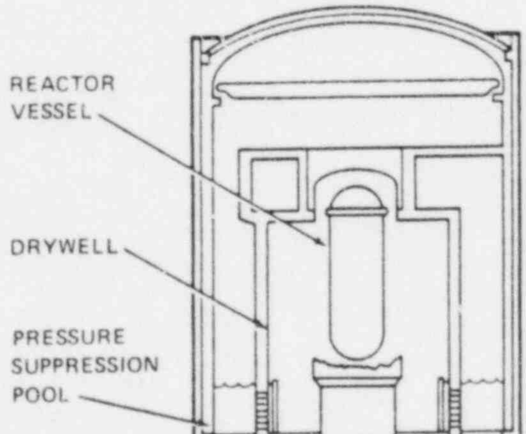
- Loss of coolant accident (LOCA) inside the drywell
- Safety/relief valve operation
  - for overpressure protection
  - for reactor coolant system (RCS) depressurization following Automatic Depressurization System (ADS) actuation
- Safety-related steam turbine-driven pump operation
  - High Pressure Coolant Injection (HPCI) pump



MARK I



MARK II



MARK III

Figure 5.2.1. BWR Pressure Suppression Containment

Table 5.2.1. Comparison of Selected BWR Containment Design Parameters.

	BWR CONTAINMENT TYPES		
	Mark I[1]	Mark II[2]	Mark III[3]
Description of Containment Design	Light bulb-shaped steel drywell, torus-shaped steel pressure suppression chamber	Frustrum-of-cone shaped drywell above cylindrical wetwell, all steel-lined concrete	Cylindrical concrete drywell surrounded by cylindrical steel suppression pool
Design Temperature of Pressure Suppression Chamber (^oF)	220 to 281 (most are 281)	215 to 275	185 to 200
Design Pressure of Pressure Suppression Chamber (psig)	56 to 62	45 to 56 (most are 45)	15
Water Volume in Pressure Suppression Chamber			
(ft^3)	58,900 to 135,000 (91,000 typ)	87,000 to 125,000 (110,000 typ)	152,600 to 164,000 (158,000 typ)
(gallons)	(681,000 typ)	(823,000 typ)	(1,182,000 typ)
Free (air) Volume in Pressure Suppression Chamber (ft^3)	91,670 to 130,900 (119,000 typ)	93,000 to 164,500 (138,000 typ)	>1,100,000[4]

Notes: (1) Sampling of 12 plants, including Peach Bottom, Arnold, Vermont Yankee, Hatch, Browns Ferry, Cooper, Fermi II, Brunswick, Pilgrim, Dresden II, Monticello and Millstone 1

(2) Sampling of 4 plants, including Zimmer, Shoreham, LaSalle, and Limerick

(3) Sampling of 2 plants, including Perry and Grand Gulf

(4) Total containment free air volume

- Reactor Core Isolation Cooling (RCIC) pump

Water temperature and level limits and plant operating limitations are imposed to ensure that the suppression pool remains an effective standby heat sink (Refs. 1 and 2). Following an event that causes suppression pool heatup, systems are normally placed in operation to cool the suppression pool by completing the heat transfer path to the ultimate heat sink.

LOCAs, events requiring RCS depressurization and events causing sustained overpressure protection system response can be characterized by a significant blowdown of reactor coolant to the suppression pool and rapid suppression pool heatup. From full power operating conditions, a LOCA or ADS blowdown to a suppression pool initially at 90°F results in a water temperature of approximately 135°F immediately following blowdown (Ref. 1). Subsequent heatup of the suppression pool progresses at a slower rate, governed primarily by the decay heat generation rate of the reactor core.

5.2.2.2 Suppression Pool Cooling Systems

In some early-vintage BWRs, suppression pool cooling is accomplished by a dedicated containment spray system. Figure 5.2.2 illustrates a BWR/2 containment spray system which consists of two 100 percent capacity, independent loops. In later-vintage BWRs, suppression pool cooling is performed by an operating mode of the residual heat removal (RHR) system. The RHR system generally consists of two 100 percent capacity, independent loops that can be aligned to draw a suction on the suppression pool, and return the water either directly to the suppression pool or to the containment spray headers. Either return path will provide for heat removal from the suppression pool water. A typical BWR/3 or BWR/4 multi-mode RHR system aligned for suppression pool cooling is shown in Figure 5.2.3. A BWR/5 or BWR/6 RHR system in a similar alignment is shown in Figure 5.2.4. BWR suppression pool cooling capabilities are summarized in Table 5.2.2.

All suppression pool cooling heat exchangers transfer heat to component cooling and/or service water systems that complete the heat transfer path to the ultimate heat sink. There is considerable variety in the design of these cooling

Table 5.2.2. Summary of BWR Suppression Pool Cooling Capabilities.

Plant	BWR Type	Systems for Containment Spray and Suppression Pool Cooling(1)	
		CS-S	CS-M
Dresden 1	1	X	-
Humboldt Bay	1	X	-
Big Rock Point	1	-	(2)
Oyster Creek	2	X	-
Nine Mile Point	2	X	-
Millstone 1	3	-	(3)
Dresden 2 & 3	3	-	(3)
Pilgrim	3	-	(4)
Monticello	3	-	(4)
Quad Cities 1 & 2	3	-	(4)
Hatch 1 & 2	4	-	(4)
Browns Ferry 1, 2 & 3	4	-	(4)
Vermont Yankee	4	-	(4)
Peach Bottom 2 & 3	4	-	(4)
Cooper	4	-	(4)
Duane Arnold	4	-	(4)
Fitzpatrick	4	-	(4)
Brunswick 1 & 2	4	-	(4)
Shoreham	4	-	(4)
Fermi 2	4	-	(4)
Susquehanna 1 & 2	4	-	(4)
LaSalle 1 & 2	5	-	(4)
Zimmer	5	-	(4)
Hanford 2	5	-	(4)
Grand Gulf 1 & 2	6	-	(4)
Other BWR/5 & /6		-	(4)

Notes: (1) CS-M = containment spray or suppression pool cooling, which is an operating mode of some other multi-mode system

CS-S = single-mode containment spray system

(2) Containment/suppression pool cooling is an operating mode of the Low Pressure Core Spray (LPCS) system

(3) Containment/suppression pool cooling is an operating mode of the Low Pressure Coolant Injection (LPCI) system

(4) Containment/suppression pool cooling is an operating mode of the multi-mode Residual Heat Removal (RHR) system.

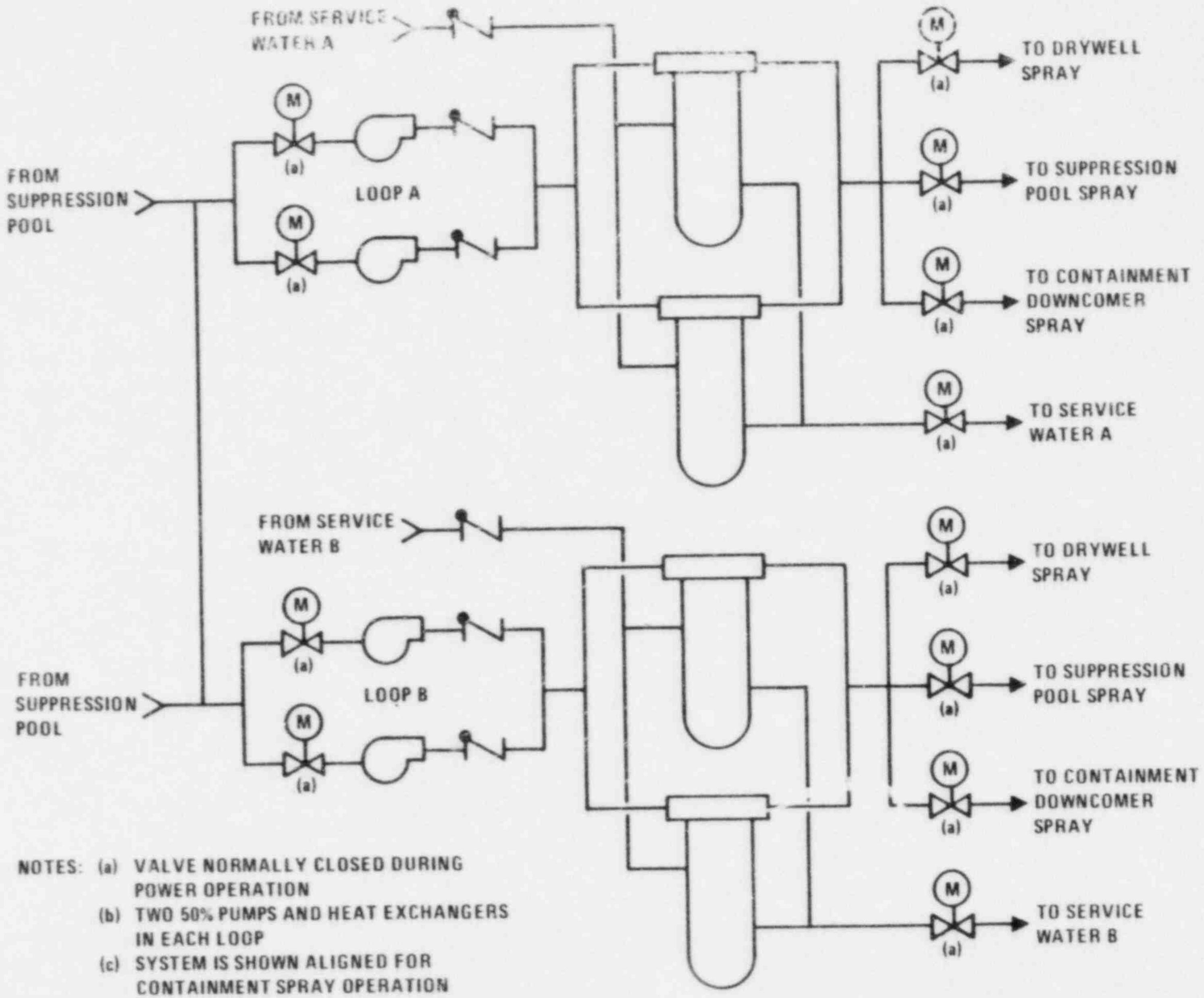


Figure 5.2.2 Typical BWR/2 Containment Spray System.

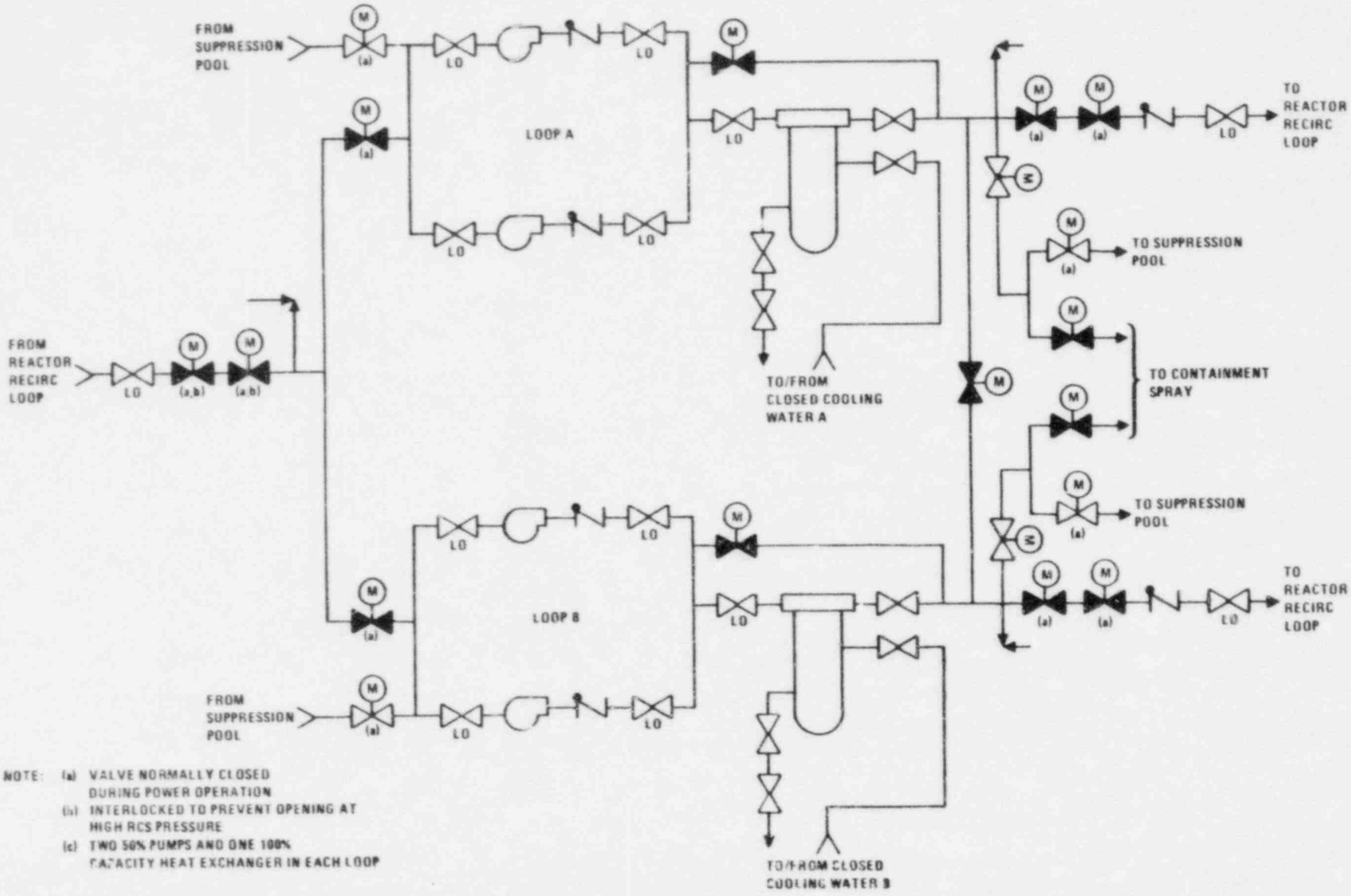


Figure 5.2.2. Typical BWR/3 or BWR/4 Multi-Mode Residual Heat Removal System Aligned for Suppression Pool Cooling.

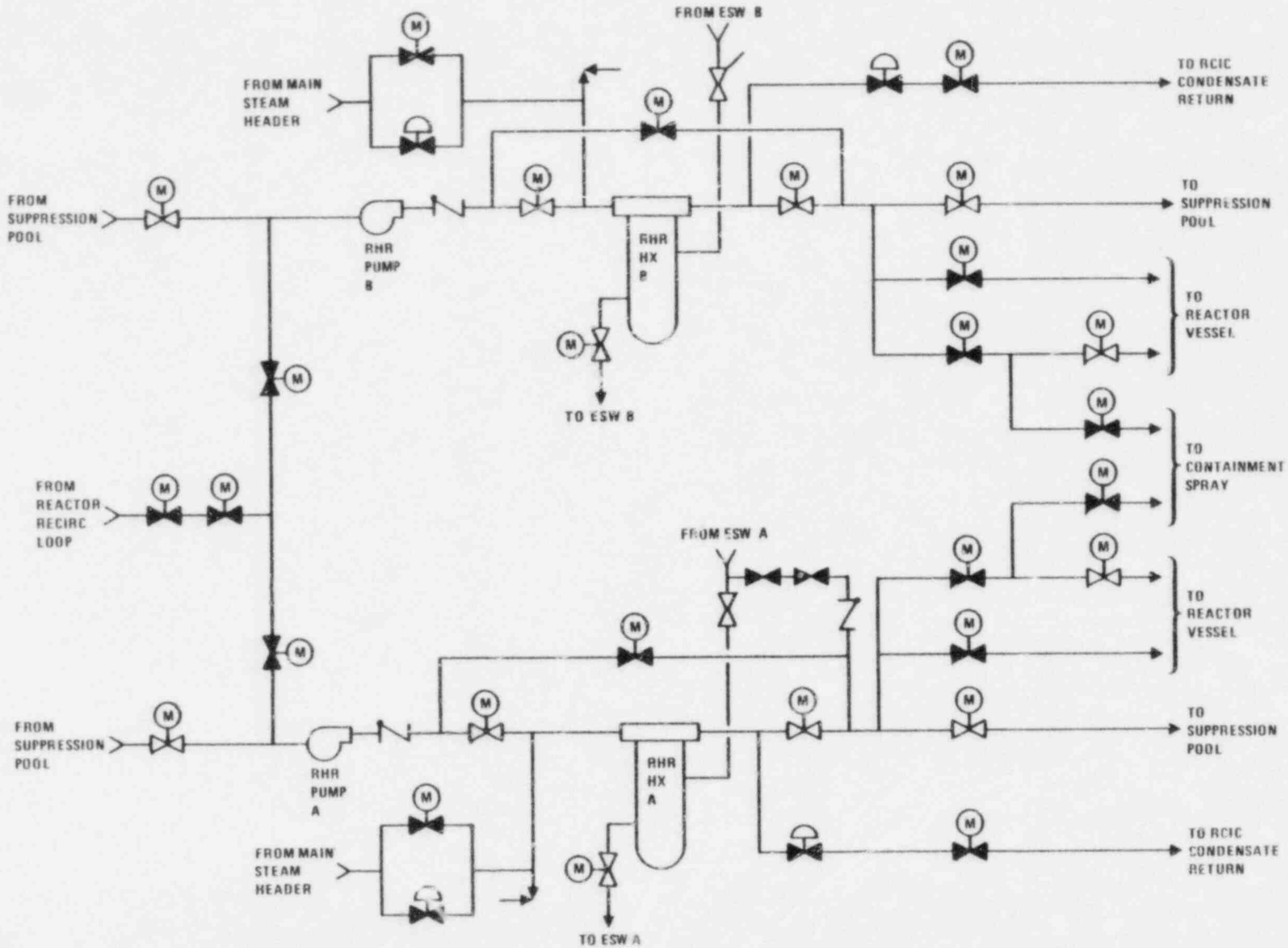


Figure 5.2.4. Typical BWR/5 or BWR/6 Multi-Mode Residual Heat Removal System Aligned for Suppression Pool Cooling.

water systems. A BWR/6 essential service water (ESW) system which provides cooling for the RHR heat exchangers is discussed in Section 5.13.

5.2.3 Plant Conditions During Sabotage Scenario

Following loss of offsite power and main turbine trip, the primary coolant system safety/relief valves will open, as necessary, to provide overpressure protection for the RCS. The turbine bypass system (TBS) is not available to dump steam to the main condenser because the main circulating water system is not operating and main condenser vacuum is rapidly being lost.

As RCS blowdown via the safety/relief valves continues, reactor vessel water level decreases. When level drops to approximately ten feet above the top of the core (Level 2), the main steam isolation valves (MSIVs) are automatically closed and makeup water is provided to the RCS by the RCIC and HPCI or High Pressure Core Spray (HPCS) systems. These inventory control systems initially draw water from the condensate storage tank (CST) which reserves a minimum volume (e.g., 75,000 to 170,000 gallons) specifically for reactor coolant makeup. This reserve volume is usually sized to provide for about eight hours of RCIC and HPCI (or HPCS) system operation following reactor scram from rated power (Ref. 3). When the CST water inventory is exhausted, the RCIC and HPCI (or HPCS) systems are realigned to take a suction on the suppression pool.

After the initial blowdown to the suppression pool, core decay heat will be transferred to the suppression pool by intermittent safety/relief valve operation and by operation of the turbine-driven RCIC and/or HPCI pumps which exhaust to the suppression pool. It has been estimated that the suppression pool of a Mark I BWR containment will reach 150^{o}F approximately 3.1 hours following loss of offsite power with no suppression pool cooling (Ref. 4).

5.2.4 Techniques for Maintaining Suppression Pool Temperature Within Design Limits Without Active Heat Removal Systems

5.2.4.1 Increasing the Mass of Water in the Suppression Pool

To ensure that the suppression pool remains an effective heat sink, the BWR Owner's Group has developed generic guidelines for a heat capacity temperature limit curve (Ref. 2). A plant-specific application of these guidelines produced the limit curve in Figure 5.2.5. Continued heatup of the suppression pool above the heat capacity temperature limit may result in insufficient suppression pool heat capacity to assure stable condensation of steam discharged through the safety/relief valves at some point following an ADS actuation. If the RCS remains at high pressure following the sabotage scenario described in Section 5.2.3, the operator would be required to initiate suppression pool cooling before bulk temperature reached approximately 160^{o}F (see Figure 5.2.5). Alternatively, the operator could initiate RCS depressurization. The heat capacity temperature limit curve is defined by a straightforward energy balance so that ADS actuation initiated below the curve will not cause pool temperature to exceed the curve during the depressurization. Following depressurization, suppression pool temperature is limited by the design temperature listed in Table 5.2.1. (Note that a heat capacity temperature limit curve for a BWR/6 plant with a Mark III containment would be considerably more restrictive than the curve in Figure 5.2.5.)

If the suppression pool cooling systems are not operable, existing design features may allow the operator to expand the heat sink capacity of the suppression pool by supplying water from the upper containment pool as shown in Figure 5.2.6 (from Ref. 3). Approximately 30,000 to 40,000 ft^3 (225,000 to 300,000 gallons) of water at 100 to 125^{o}F may be available for suppression pool makeup from this source.

There are upper limits on allowable suppression pool level when the reactor coolant system is pressurized (Ref. 2). These limits ensure that the dynamic loads resulting from safety/relief valve actuation do not exceed the yield stress on the limiting submerged structural component in the suppression pool. Because of these limits and permissive actuation logic restrictions, makeup water from the upper containment pool would not be supplied before

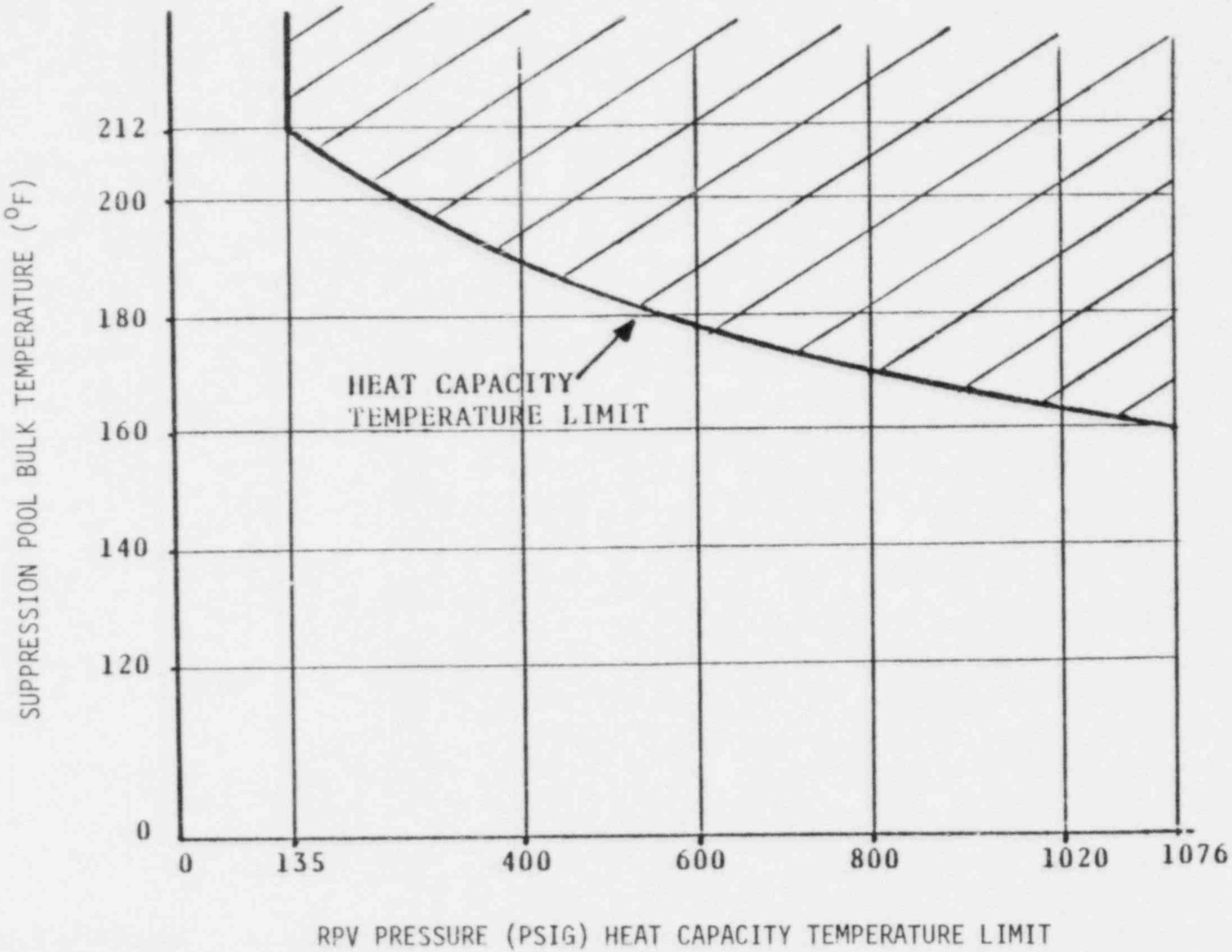


Figure 5.2.5. Suppression Pool Heat Capacity Temperature Limit Curve (from BWR Emergency Procedure Guidelines).

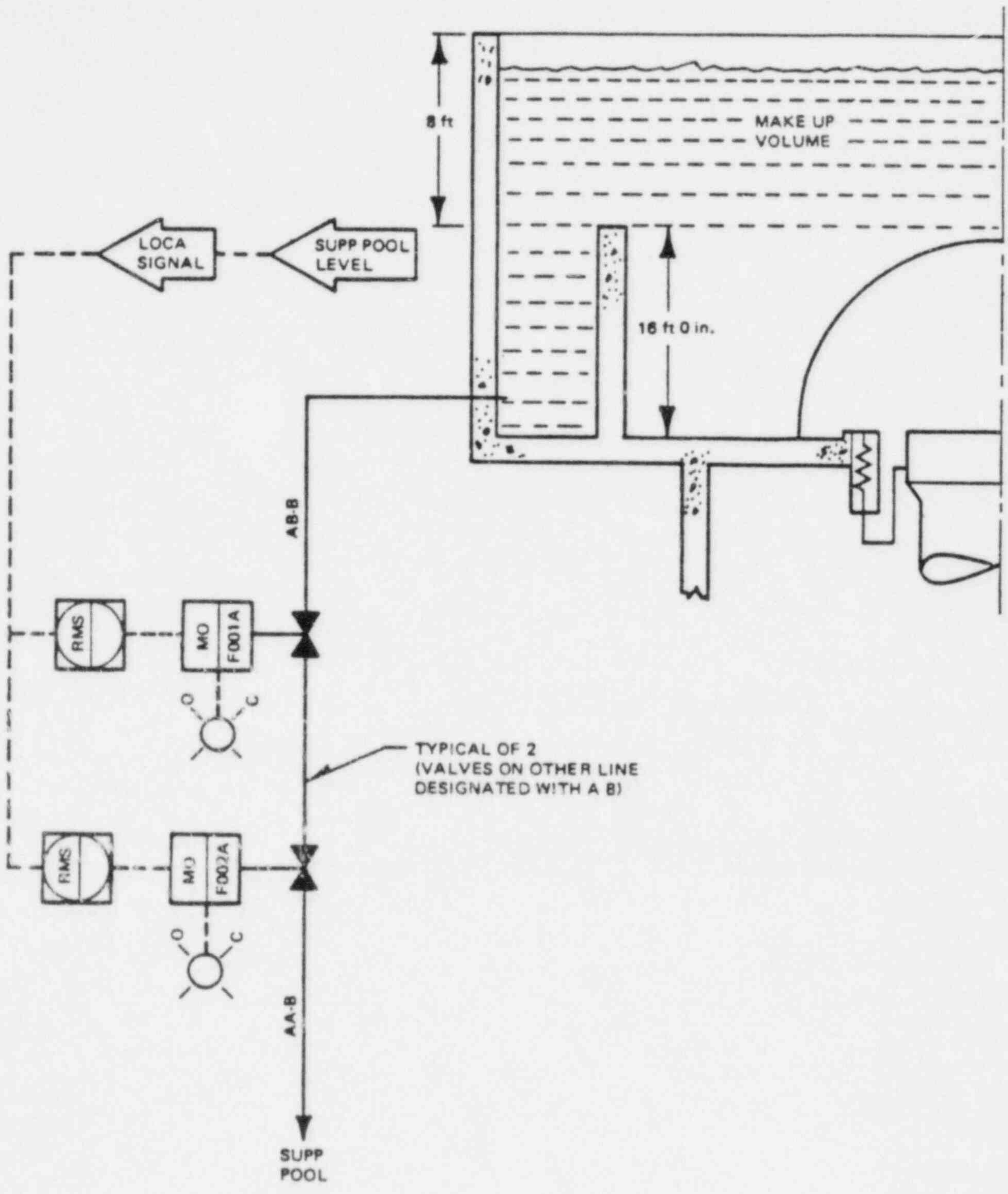


Figure 5.2.6. Suppression Pool Makeup System
(from 238 GESSAR).

depressurization of the RCS. From Figure 5.2.5, it can be estimated that suppression pool temperature would be approximately 200^{o}F following depressurization (assuming depressurization was initiated 3.1 hours after loss of offsite power when the suppression pool reached 150^{o}F).

As illustrated schematically in Figure 5.2.6, initiation of makeup from the upper containment pool requires the coincidence of low suppression pool level <u>and</u> a LOCA signal (e.g., high drywell pressure and low reactor vessel water level). These coincident conditions would not exist following ADS actuation (e.g., there is no blowdown to the drywell). The permissive logic also blocks remote-manual initiation of makeup from the upper containment pool. To make this source of water available, it would be necessary to bypass the permissive interlocks in the dump valve control circuits. This could likely be accomplished by jumpering the appropriate contacts in the valve control circuits. Alternatively, the dump valve actuation logic and control circuits could be redesigned to provide series keylocked switches (e.g., "arm" and "dump") in the control room to open the valves independently of the interlocked actuation system. Administrative control of the keys would be required to ensure that the upper containment pool could not be inadvertently dumped.

The makeup water from the upper containment pool has the capacity to absorb 140 to 250 x 10^{6} BTU by being heated to 200^{o}F. At 3.1 hours after reactor scram, the decay heat rate is approximately one percent of the initial operating power level (Ref. 5). Assuming an initial power level of 3000 MWt (10,240 x 10^{6} BTU/hr), the decay heat rate at 3.1 hours is approximately 102 x 10^{6} BTU/hr. The added heat capacity of the makeup water from the upper containment pool would therefore provide an additional 1.4 to 2.5 hours before suppression pool temperature exceeded 200^{o}F (assuming a constant decay heat rate).

Following addition of water from the upper containment pool, suppression chamber free volume has been reduced to 80,000 to 100,000 ft^{3} (see Table 5.2.1). It should be possible to use some of the remaining free volume and add more water to the suppression pool from other sources (e.g., fire water system, demineralized water, etc.) if suitable makeup connections can be established (see damage control measure #24). At five hours after reactor scram, the decay heat rate will be approximately 82 x 10^{6} BTU/hr. This decay heat rate can be absorbed if 75,000 gallons/hour (1250 gpm) of makeup water at 70^{o}F can be supplied to the suppression pool which is assumed to be at 200^{o}F. The containment free volume would be reduced by approximately 10,000 ft^{3}/hr at this makeup rate and the suppression chamber will be slowly pressurized.

By increasing the thermal mass of the suppression pool, it may be possible to maintain the pool at 200^{o}F for several additional hours. Limiting factors to be considered include: (a) the static load (from static head of water and from gas pressure) on the suppression chamber, (2) instrument flood-out in the suppression chamber, and for BWR/6 plants, (c) overflowing the weir wall and flooding the drywell.

This damage control measure only serves to delay the time at which an active heat transfer path must be established between the suppression pool and an ultimate heat sink. The added time provided by this damage control measure may be helpful when considered in conjunction with other measures to restore active cooling for the suppression pool (see damage control measures #7 and #8). Several other methods of providing makeup to the suppression pool are described below.

A. Suppression Pool Makeup Using HPCI or HPCS System

The containment cooling systems illustrated in Figures 5.2.2 to 5.2.4 could provide more than the required 1250 gpm makeup rate if a suction-side connection to a suitable onsite reservoir could be established (assuming that the sabotage actions discussed in Section 5.2.1 have only disabled the heat transfer capability of the suppression pool cooling system heat exchangers). Assuming that these systems are unavailable, the HPCI or HPCS system (or marginally, the RCIC system) could be removed from duty as a reactor coolant inventory control system and aligned to supply water from the CST to the suppression pool via the test line illustrated in Figure 5.2.7. In some plants, this test line may not be designed as a full-flow test line and may have to be increased in size to accommodate at least 1250 gpm. The CST would be rapidly depleted at the high makeup rate required by the suppression pool. An alternate suction for the HPCI or HPCS pumps could be provided as illustrated in Figure 5.2.7. Other onsite sources of water might include: (1) refueling water storage tank, (2) fire water storage tanks, (3) service or potable water systems.

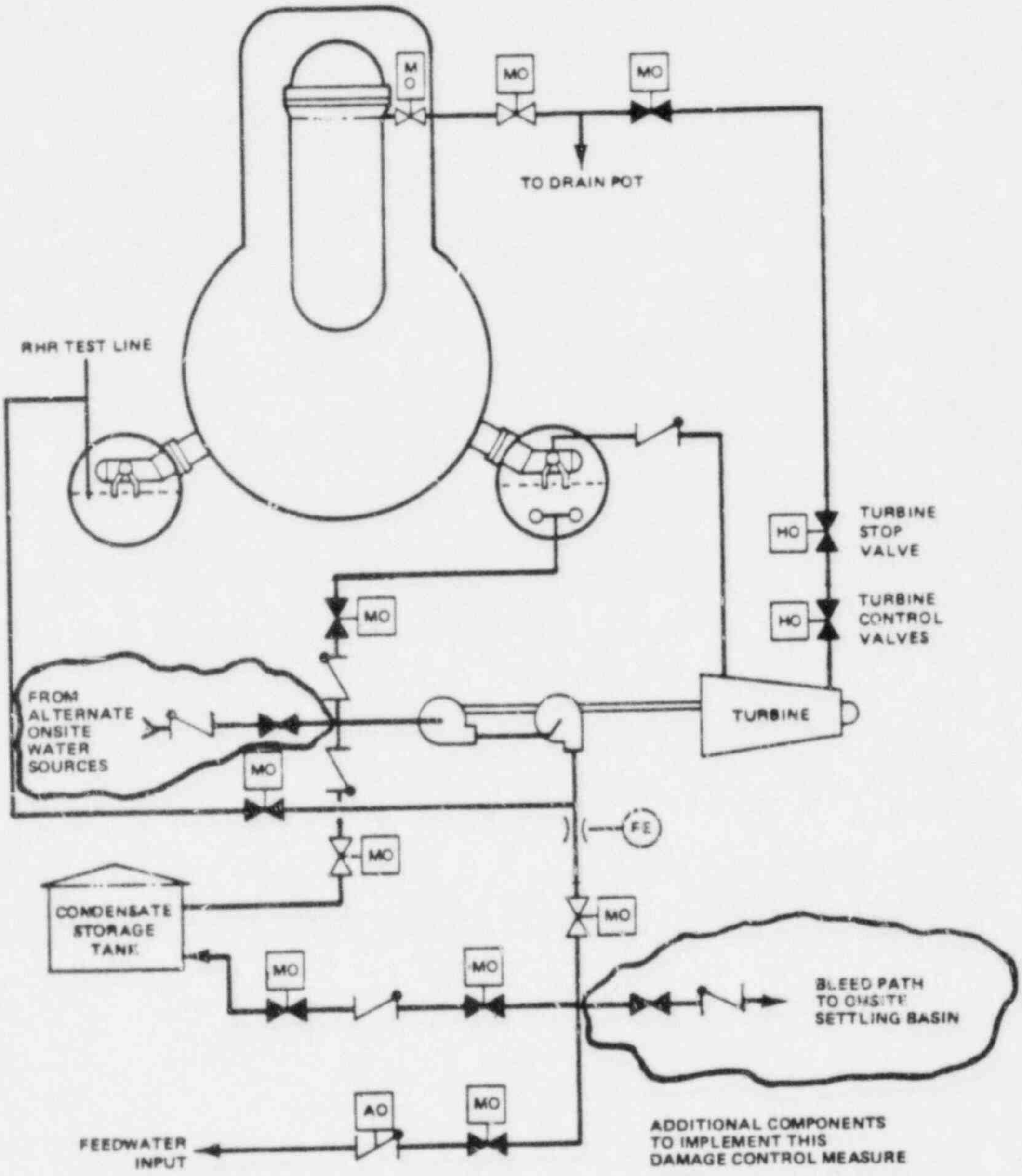


Figure 5.2.7. High Pressure Coolant Injection (HPCI) System Modifications for Emergency Suppression Pool Cooling.

B. Suppression Pool Makeup Using Refueling Water Transfer System

An indirect means for supplying water to the suppression pool is to use the refueling water transfer system to supply makeup water from the refueling water storage tank (RWST) to the upper containment pool (see Figure 5.2.8). Water from the upper containment pool can be supplied to the suppression pool as described previously. Capacity of each transfer pump may be as high as 1250 gpm at 95 psid. The RWST contains 150,000 to 300,000 gallons which would be an adequate source for several hours of suppression pool makeup. The transfer pumps are usually supplied by Nonclass 1E power and would be unavailable following loss of offsite power. These pumps could be supplied with Class 1E power (see damage control measure #19) or from an alternate onsite source of Nonclass 1E power (see damage control measure #26). The condensate transfer pumps do not (and should not) have access to the 75,000 to 170,000 gallons of water reserved in the condensate storage tank for reactor coolant inventory control (e.g., for the RCIC, HPCI and HPCS systems). These pumps would, therefore, not be likely candidates for suppression pool makeup.

C. Suppression Pool Makeup Using Service Water System Crossconnect to RHR System

A crossconnect may exist between the RHR service water system and the RHR system, such that the service water system can be aligned as a makeup source for the suppression pool. This crossconnect path, shown in Figure 5.2.4, is normally isolated by two manual valves. When this makeup path is established, water can be supplied to the suppression pool using the service water pumps. Service water quality must be considered, however, when determining the acceptibility of this approach.

5.2.4.2 Feed-and-Bleed Cooling of the Suppression Pool

An alternative approach to suppression pool cooling would be to supply "cold" makeup water by any of the techniques described in Section 5.2.4.1 and drain an equivalent amount of "hot" water from the suppression pool. This method could be continued indefinitely without restrictions imposed by flooding the suppression chamber. Assuming that a sufficient reservoir of "cold" water exists the major concern associated with feed-and-bleed cooling of the suppression pool is where to put the 75,000 gallons/hour (approximately) that would be removed from the suppression pool.

The suppression pool water will likely be contaminated with radionuclides, and therefore, release directly to the environment would not be feasible. Surface release to a large clay-lined settling basin may be possible, however, environmental effects should be calculated on an individual case basis.

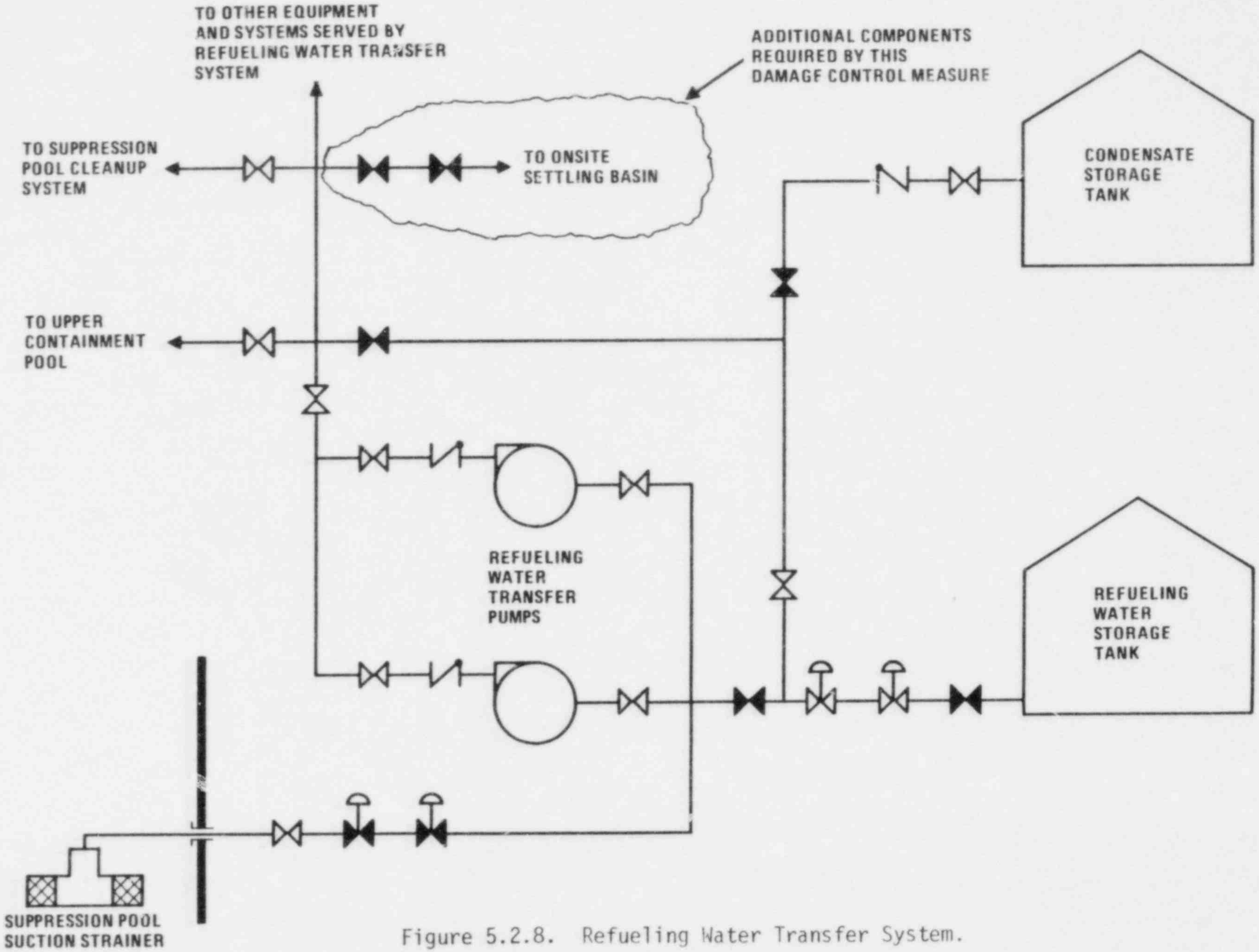


Figure 5.2.8. Refueling Water Transfer System.

The HPCI or HPCS system flow rates exceed the suppression pool makeup requirements, therefore these systems could be operated alternately in a "feed" mode and then in a "bleed" mode. In the "feed" mode, water is supplied from an onsite reservoir to the suppression pool via new suction-side piping and the HPCI or HPCS test line (see Figure 5.2.7). In the "bleed" mode, the pump suction is realigned to the suppression pool using existing piping, and the pump discharge is aligned to new piping that directs flow to the onsite settling basin. It would be necessary to maintain RCS pressure above 150 psig to permit continued operation of the turbine-driven HPCI pump. The electric motor-driven HPCS pump is not subject to these restrictions.

The refueling water transfer pumps could also be operated alternately in a feed-and-bleed mode (or in a single mode in conjunction with the HPCI or HPCS pump). The "feed" path has been described previously. The "bleed" path would utilize an existing suppression pool suction line (normally used for suppression pool cleanup) and new piping on the discharge side of the transfer pumps to direct flow to an onsite settling basin. The operator may have to override containment isolation valves to make this "bleed" path available during some emergency conditions. As an alternative to the settling basin, existing crossconnect piping could be used to pump water back to the CST and RWST until these tanks have been filled (see Figure 5.2.8). If initially empty, these tanks could provide a storage volume for several hours of suppression pool feed-and-bleed operations.

5.2.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #2

The primary technical and regulatory concerns are: (1) containment integrity under static loading conditions imposed by a flooded suppression chamber, and (2) potential radionuclide release to the environment resulting from feed-and-bleed operations. These concerns should be addressed on an individual case basis.

5.2.6 Conclusions and Recommendations Regarding Damage Control Measure #2

Increasing the thermal mass of the suppression pool provides a means for extending the time available to restore active suppression pool cooling systems to operation, and would be useful in this context. Existing design features can provide significant makeup to the suppression pool from several sources. Relatively minor modifications could make the makeup water sources more readily available during emergencies. The feasibility of long-term suppression chamber feed operations (e.g., flooding without draining any water) should be evaluated on an individual case basis.

Feed-and-bleed cooling of the suppression pool could provide an effective long-term heat sink without the need to restore conventional suppression pool cooling systems to operation. The potential impact of radionuclide releases to the environment, and therefore the acceptability of this approach, should be evaluated on an individual case basis.

5.2.7 Section 5.2 References

1. NUREG-0123 (Rev. 3), "Standard Technical Specifications for General Electric Boiling Water Reactors (BWR/5)," U. S. Nuclear Regulatory Commission, Fall 1980.

2. "Emergency Procedure Guidelines, BWR/1 through BWR/6, Revision 1," BWR Owner's Group, January 1981.

3. "238 Nuclear Steam Supply System - GESSAR," Docket STN-50550, General Electric Company.

4. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

5. ANSI/ANS 5.1-1979, "Decay Heat Power In Light Water Reactors."

5.3 DAMAGE CONTROL MEASURE #3 - PWR

The purpose of damage control measure #3 is to use a steam turbine-driven main feedwater pump to supply feedwater to the steam generators in PWR plants in the event that the auxiliary feedwater system has been disabled by sabotage.

5.3.1 Sabotage Scenario

It is assumed that offsite power is lost coincidentally with successful sabotage actions that have made the steam turbine-driven and motor-driven trains of the auxiliary feedwater system inoperable. The main turbine generator trips on loss of load. The power conversion system (main steam, feedwater and condensate and circulating water system) is unavailable due to loss of Nonclass 1E power. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.3.2 System Descriptions

5.3.2.1 Auxiliary Feedwater System

See Section 5.4

5.3.2.2 Main Feedwater (MFW) System

The main feedwater system is used to supply feedwater to the steam generators during normal operations. PWR feedwater and condensate system configurations are summarized in Table 5.3.1. Approximately 55 percent of the plants listed in this table have steam turbine-driven feedwater pumps. Basic elements of a typical main feedwater system are illustrated in Figure 5.3.1

During power operation, the main feedwater pump drive turbines are typically supplied with steam from extraction nozzles at an intermediate point on the main turbine. The feedwater pump turbine can also be driven by high pressure main steam taken upstream of the main turbine. This latter mode of operation is

Table 5.3.1. Summary of PWR Feedwater and Condensate System Configurations

Plant	Type(1)	Feedwater Pumps Number	Feedwater Pumps Drive(2)	Booster Pumps (3)	Condensate Pumps (4)
San Onofre 1	W	2	E	-	4
Yankee-Rowe	W	3	E	-	3
Prairie Island 1&2	W	2	E	-	3
Trojan	W	2	S	-	2
Salem 1	W	2	S	-	3
Ginna	W	2	E	3	3
North Anna 1&2	W	3	E	-	3
Point Beach 1&2	W	2	E	-	2
Kewaunee	W	2	E	-	2
D.C. Cook 1&2	W	2	S	3	3
Farley 1&2	W	2	S	-	3
H.B. Robinson	W	2	E	-	2
Zion 1&2	W	2	S	4	4
		1	E		
Haddam Neck	W	2	E	-	2
Indian Point 2&3	W	2	S	-	3
Beaver Valley	W	2	E	-	2
Turkey Point 3&4	W	2	E	3	2
Surrey 1&2	W	2	E	-	3
Arkansas Nuclear One-2	C-E	2	S	-	4
Calvert Cliffs 1&2	C-E	2	S	3	3
Fort Calhoun	C-E	3	E	-	3
Maine Yankee	C-E	2	E	-	3
Millstone 2	C-E	2	S	-	3
Palisades	C-E	2	S	-	2
Saint Lucie 1	C-E	2	E	-	2
Three Mile Island 1&2	B&W	2	S	3	3
Crystal River	B&W	2	S	2	2
Oconee 1,2&3	B&W	2	S	3	3
Rancho Seco	B&W	2	S	-	3
Davis Besse	B&W	2	S	2(5)	3
Arkansas Nuclear One-1	B&W	2	S	-	3
		1	E		

Notes:

(1) W = Westinghouse, C-E = Combustion Engineering, B&W = Babcock & Wilcox
(2) E = electric motor-driven, S = steam turbine driven.
(3) All electric motor-driven, except as noted below.
(4) All electric motor-driven.
(5) Gear-driven off main feedwater pump shaft.

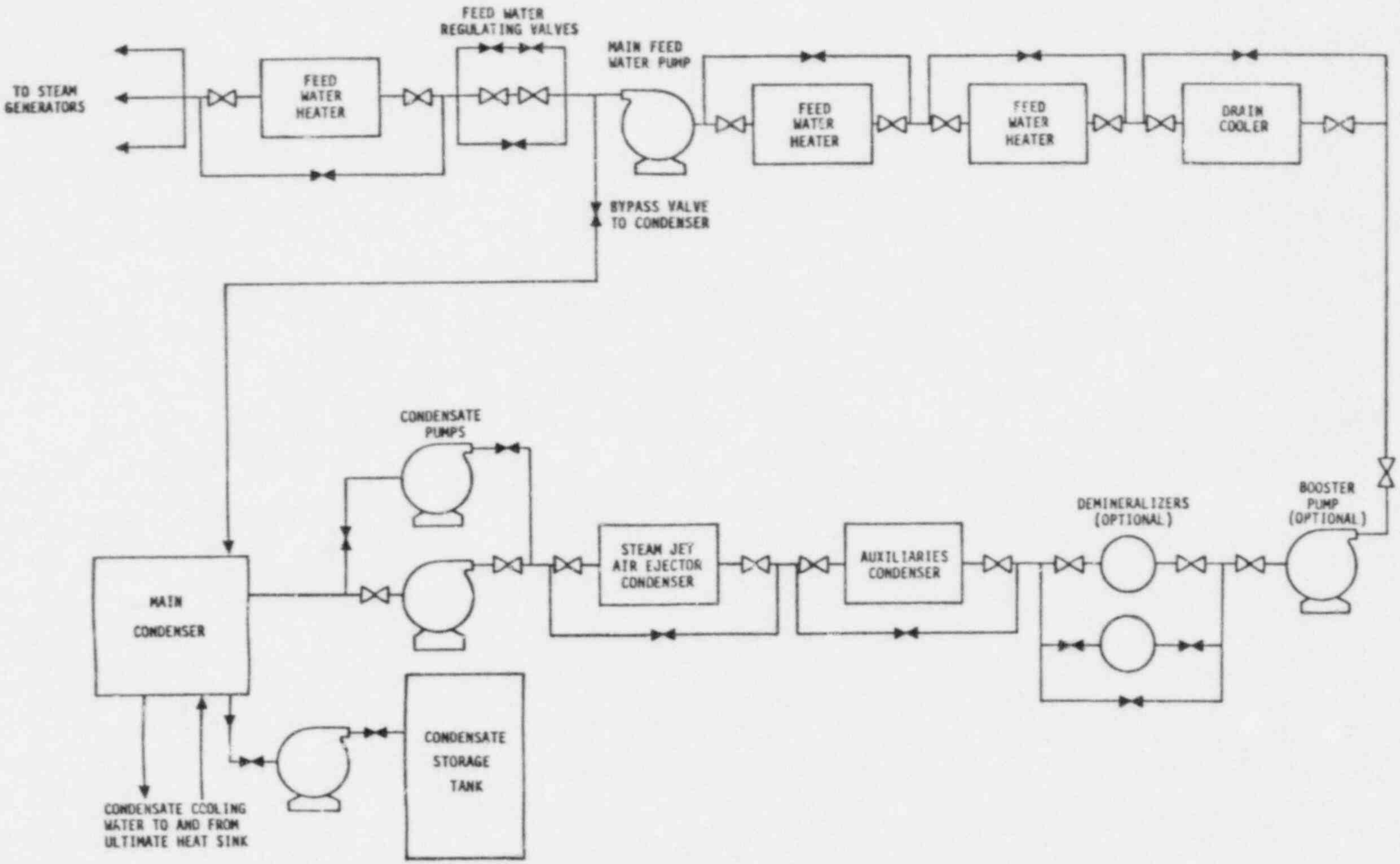


Figure 5.3.1. Representative Main Feed Water System, One of Two Trains.

used during plant startup when the main turbine is not operating. The feed pump turbine exhaust is routed to the main condenser with permissible exhaust pressures between 1 and 10 inches mercury absolute. Typically, a three-element feedwater flow control system maintains programmed water level in the steam generator by modulating feedwater pump turbine drive speed and feedwater control valve position. The programming of valve position and feedwater pump speed is such that valve control of feedwater flow rate predominates at low-power conditions, while pump speed control is the primary mechanism for feedwater flow adjustment at high power levels (e.g., with the control valves fully open to minimize pressure drop across the valves).

A main feedwater pump drive turbine can be characterized as a multi-stage condensing turbine. This is in contrast to an auxiliary feedwater pump drive turbine which is typically a single-stage noncondensing turbine. Conditions that will typically cause a trip of a steam turbine-driven MFW pump are summarized in Table 5.3.2.

5.3.3 System Conditions During Sabotage Scenario

The electrically-powered condensate and booster pumps in the main feedwater system would be inoperable because of the loss of Nonclass 1E AC power. Loss of these pumps makes the condenser unavailable as a water source for the main feedwater pumps. In addition, loss of the circulating water system, the steam jet air ejectors and the trip of the main turbine would cause a rapid loss of main condenser vacuum. The main feedwater pumps would therefore trip for a variety of reasons (e.g., low suction pressure, low condenser vacuum, low lube oil pressure).

The steam supply for the main feedwater pump steam turbine drive would be interrupted when the main turbine tripped following loss of offsite power. Main steam could be made available to the feedwater pump drive turbine directly from the main steam header as described previously. Operation of a main feedwater pump would require the restoration of AC power to the feedwater pump lube oil system, feedwater control system, the condensate and booster pumps, and the control air system (for feedwater regulating valve control).

Table 5.3.2. Trip Conditions Typically Associated With Turbine-Driven Main Feedwater Pumps

Low Condenser Vacuum (high turbine exhaust pressure)
Low Pump Suction Pressure
High Pump Discharge Pressure
Low Bearing Lube Oil Pressure (pump and turbine)
High Turbine Speed
High Turbine Vibration Level
Thrust Bearing Wear
High Steam Generator Water Level[1]
Safety-Injection Signal[1]
Manual

Notes: [1]Some Westinghouse Plants.

Steam generator level is rapidly decreasing following loss of all feedwater. The steam generators are expected to boil dry in 14 to 43 minutes if feedwater flow is not restored (Refs. 1 and 2).

5.3.4 System Alignment Necessary To Use The Main Feedwater System As a Substitute For The Auxiliary Feedwater System

The main feedwater system modifications necessary to implement this damage control measure are shown in Figure 5.3.2, and are discussed below. Only limited time is available to restore feedwater flow, therefore operational requirements associated with reestablishing feedwater flow must also be limited.

- A piping system interconnection would be needed between the condensate storage tank and the condensate pump inlet such that the storage tank could be used as an alternate water supply source for the main feedwater system.

- Unused condensate and booster pumps would be isolated by shutting their respective suction valves.

- Bypasses would need to be installed around auxiliary system condensers, feedwater heaters, demineralizers and booster pumps normally connected in series between the condensate and main feedwater pumps. In several plants these equipment bypasses are provided in order to achieve flexibility in plant operations. In those plants, it would be necessary to assure that the proper bypass valves could be aligned within the time constraints available. Remote-manual actuation of these valves would likely be required.

- Electric power must be restored to the following feedwater system components:

  - Feedwater pump lube oil system for one FW pump.
  - Feedwater control system
  - Control air system
  - One condensate pump
  - One booster pump (if provided)

  This can be accomplished by supplying these components with Class 1E power (see damage control measure #19) or with an alternate onsite source of Nonclass 1E power (see damage control measure #26).

- A control valve would be needed in a manifold between the high and low pressure steam inlets to the main feedwater pump drive turbine to permit continued turbine operation on low pressure steam as steam conditions deteriorate in the long-term following the initiating event.

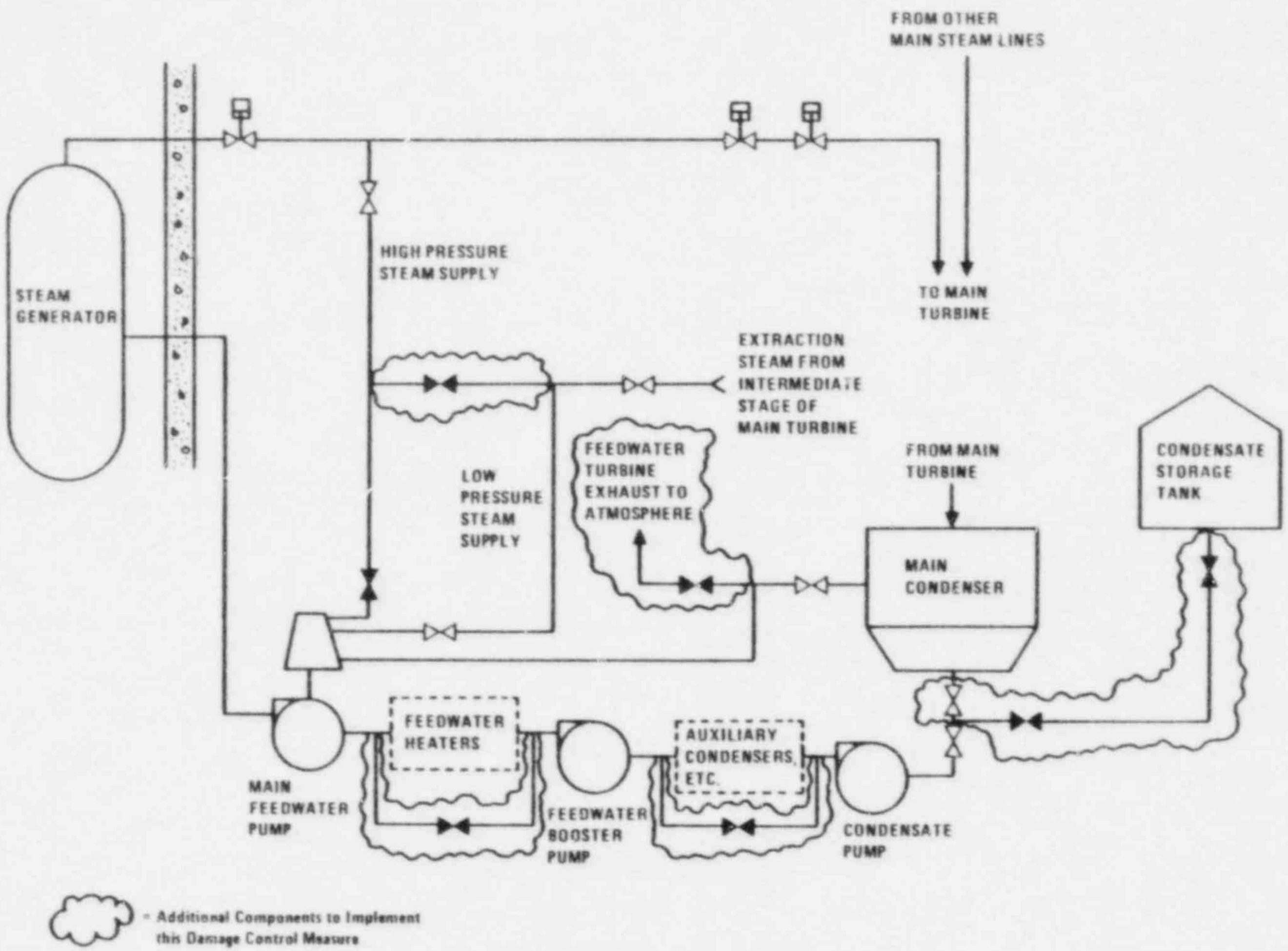


Figure 5.3.2. Modifications Necessary to Implement Damage Control Measure #3.

- An alternate line to discharge exhaust steam from the feed water pump drive turbine directly to atmosphere would be required. Atmospheric discharge of steam is necessary because the time constraints for restoring feedwater flow would likely preclude restoring main condenser vacuum and utilizing the normal exhaust path for the turbine drive.

  The main feedwater pump turbine drive is designed for condensing operation, with the exhaust discharged to the main condenser under vacuum conditions. When exhausting to atmosphere, the turbine drive would be operating in a noncondensing mode. Problems associated with operating the turbine in this mode include overheating the final stages of the turbine drive.

  The turbine modifications that would be necessary to permit the turbine to operate under the steam inlet and exhaust conditions resulting from the postulated incident have not been defined in this study. It is likely that existing drive turbines could not be readily modified. Replacement drive turbines may be required to implement this damage control measure.

- The feedwater control system will likely require modification to provide feedwater at rates comparable to the auxiliary feedwater system. A comparison of a main feedwater and an auxiliary feedwater pump is provided in Table 5.3.3. A typical MFW pump provides more than twenty times the flow provided by a typical AFW pump. Following the initial response to an accident, AFW flow is further reduced to prevent overcooling the shutdown reactor plant and overfilling the steam generators.

  Additional control system modifications would be required to provide a bypass for the low condenser vacuum (high turbine exhaust pressure), and high MFW pump discharge pressure trips. To protect the main condenser, an interlock may also be required to ensure that the MFW pump turbine exhaust is aligned to the atmosphere before the high main condenser vacuum trip can be bypassed.

5.3.5 Technical and Regulatory Impediments To Implementing Damage Control Measure #3

It appears to be technically feasible to install properly sized piping interconnections between the main feedwater and main steam systems to implement damage control measure #3. Appropriately sized lines, together with the necessary block and backflow prevention valves could be installed and could be capable of providing an additional source of feedwater to the steam generators during emergencies. The primary technical impediments to this damage control measure are: (1) the inability of the feedwater pump to operate for an extended period of time with atmospheric pressure exhaust conditions, and (2) the ability of the feedwater control system to provide the required modulation of the

Table 5.3.3. Comparison of Main and Auxiliary Feedwater Pump Characteristics

	Main Feedwater Pump	Auxiliary Feedwater Pump
Type	Multi-Stage Centrifugal	Multi-Stage Centrifugal
Flowrate	8,000 to 20,000 gpm (14,000 gpm typical)	260 to 1050 gpm (600 gpm typical)
Design Head	2000 to 3200' (2600' typical)	2500 to 3000' (2700' typical)
Horsepower	8000 to 12000	600 to 1000

feedwater pump turbine speed and the feedwater regulating valves for the low feedwater flow conditions required following plant shutdown.

The potential regulatory impediments to implementing this damage control measure include the following:

- The condensate storage tank is the normal water source for the auxiliary feedwater system. Aligning the main feedwater system to this tank during an emergency in which steam generator cooling is required would not degrade this system for emergency use. If, however, the main feedwater system were inadvertently connected to the condensate storage tank during normal power operations, the availability of this emergency source of feedwater could be placed in jeopardy. Normally closed and locked series valves with suitable physical protection may provide adequate assurances against inadvertent alignment of the condensate pump suction to the condensate storage tank. Physical protection requirements for these valves may hamper rapid realignment of the main feedwater system when required in an emergency.

- Any electrical interconnections between the Nonclass 1E and the Class 1E AC distribution systems would require particular attention to assure that the Class 1E system was not degraded because of the interconnection. See Section 5.19 for additional information.

- The potential impact of this damage control measure on the likelihood of an overcooling transient or other damage due to overfilling the steam generators should be assessed. In addition to modification of the feedwater control system, emergency operating procedures and operator training may be adequate to minimize this concern.

5.3.6 Conclusions and Recommendations Regarding Damage Control Measure #3

This damage control measure appears to be technically feasible, however, there are significant operational constraints that may limit its practicality. If the feedwater system can be rapidly restored to operation, core decay heat removal via the steam generators can be reestablished.

5.3.7 Section 5.3 References

1. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

2. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5.4 DAMAGE CONTROL MEASURE #4 - PWR

The purpose of damage control measure #4 is to supply water to the steam generators using the safety injection pumps in the event that the auxiliary feedwater (AFW) system is disabled through sabotage action.

5.4.1 Sabotage Scenario

Offsite power is lost coincidentally with the successful sabotage of the auxiliary feedwater system. The main turbine generator trips on loss of load and main feedwater is interrupted because of the loss of normal AC power. The auxiliary feedwater system is disabled through sabotage action. The emergency diesel generators operate to supply AC power to the Class 1E buses.

5.4.2 System Descriptions

5.4.2.1 Safety Injection System

The safety injection (SI) system is an element of the emergency core cooling system (ECCS). During normal power operation, the system is in standby. Following a loss of coolant accident (LOCA), the safety injection pumps are started automatically, and supply borated water to the reactor coolant system (RCS) from the refueling water storage tank (RWST). When RWST water has been exhausted, the suction of the safety injection pumps can be shifted to the containment sump. Post-LOCA core cooling is continued by recirculating water from the sump back to the reactor vessel. Safety injection system operation may also be required to maintain adequate core coolant inventory following some transients. There is a wide variety of safety injection system designs. A safety injection system for a typical Combustion Engineering PWR is illustrated in Figure 5.4.1 (from Ref. 1).

There are two basic safety injection subsystems, providing high pressure safety injection (HPSI) and low pressure safety injection (LPSI) functions. In many plants, the HPSI function is performed by positive displacement or centrifugal charging pumps that are capable of providing makeup

NOTE: System is shown in lineup for ECCS injection. During normal power operation, this system is in standby.

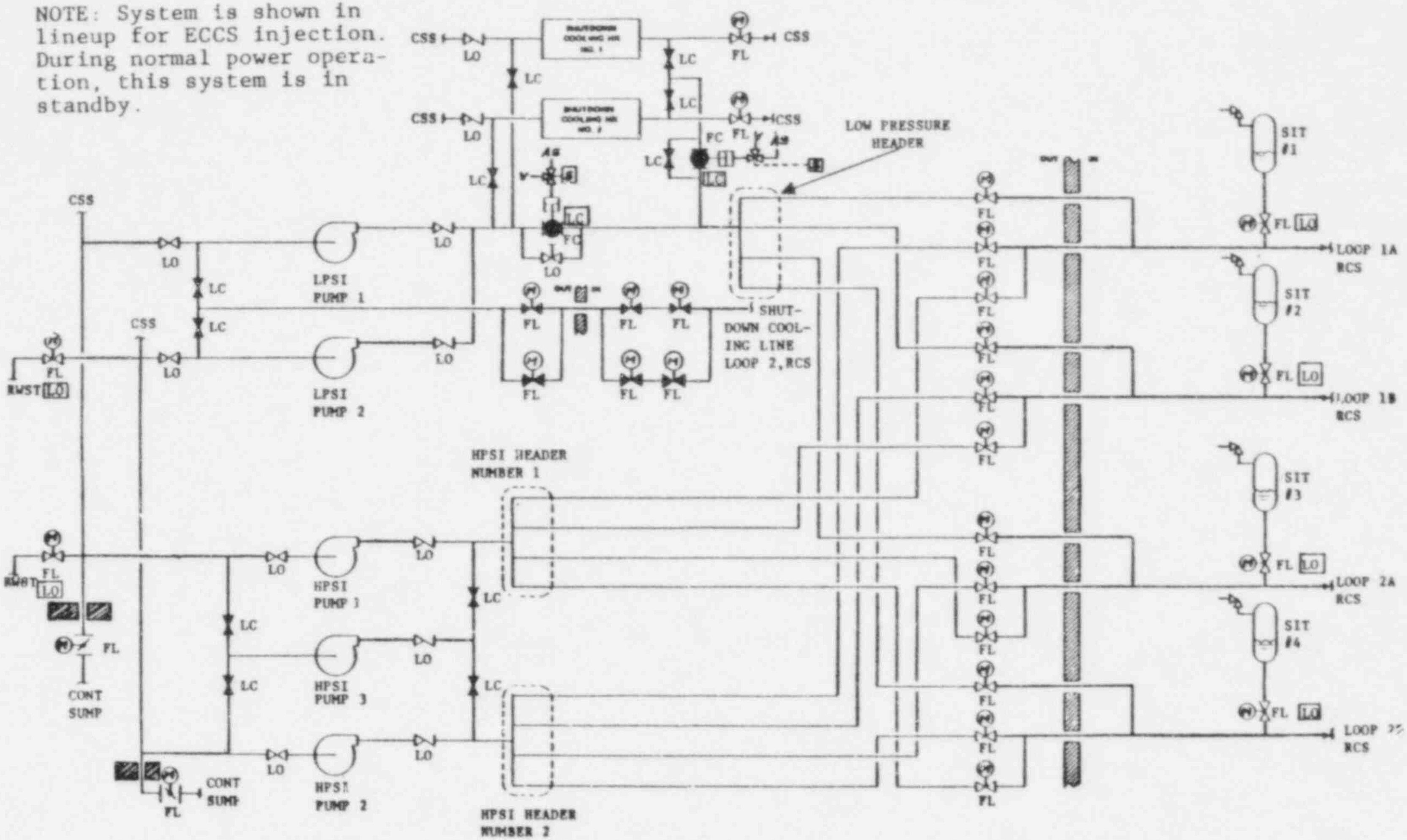


Figure 5.4.1. Typical Combustion Engineering Emergency Core Cooling System (from SAI01379-626LJ)

to the RCS against full system pressure. Typical capacity of a centrifugal charging pump that doubles as a HPSI pump is in the 140 to 370 gpm range at 2500 psig (5760 feet). Three charging pumps are usually provided, and total high pressure injection flow rate is in the 355 to 810 gpm range (one of the three charging pumps may be a lower capacity positive displacement pump providing 50 to 98 gpm flow). A typical performance curve for a centrifugal charging pump is illustrated in Figure 5.4.2 (from Ref. 2).

Many plants have separate pumps for the HPSI and normal charging functions. In these plants, the HPSI pumps usually cannot provide makeup against full RCS pressure. These HPSI pumps have a design flow rate of 375 to 425 gpm at a head of 1150 to 1225 psid (2650 to 2822 feet). Two or three HPSI pumps are usually provided, yielding a design HPSI system flow rate of 750 to 1275 gpm. A typical performance curve for a centrifugal HPSI pump is illustrated in Figure 5.4.3 (from Ref. 2). The separate charging pumps are usually positive displacement and are rated at 33 to 98 gpm. Three charging pumps are usually provided, and total charging system flow rate is in the range from 100 to 260 gpm.

Low pressure safety injection pumps typically have a design flow rate of 2500 to 4200 gpm at a head of 140 to 170 psid (320 to 390 feet). Two or three LPSI pumps are usually provided, yielding a design LPSI system flow rate of 7500 to 12,600 gpm. A typical performance curve for a LPSI pump is illustrated in Figure 5.4.4 (from Ref. 2). LPSI pumps generally serve a dual role, and are also used in the residual heat removal (RHR) system to provide for normal shutdown cooling of the RCS following cooldown to approximately 35^{o}F and 350 psig by another system (e.g., auxiliary feedwater or main turbine bypass system).

5.4.2.2 Auxiliary Feedwater System

The AFW system provides for heat removal from the primary system via the steam generators when the main feedwater system is not available. It is capable of maintaining the plant in a hot shutdown condition or of cooling the RCS to the point where the RHR system can be placed in operation. The AFW system can also be used to provide feedwater to the steam generators during normal plant startup and shutdown conditions.

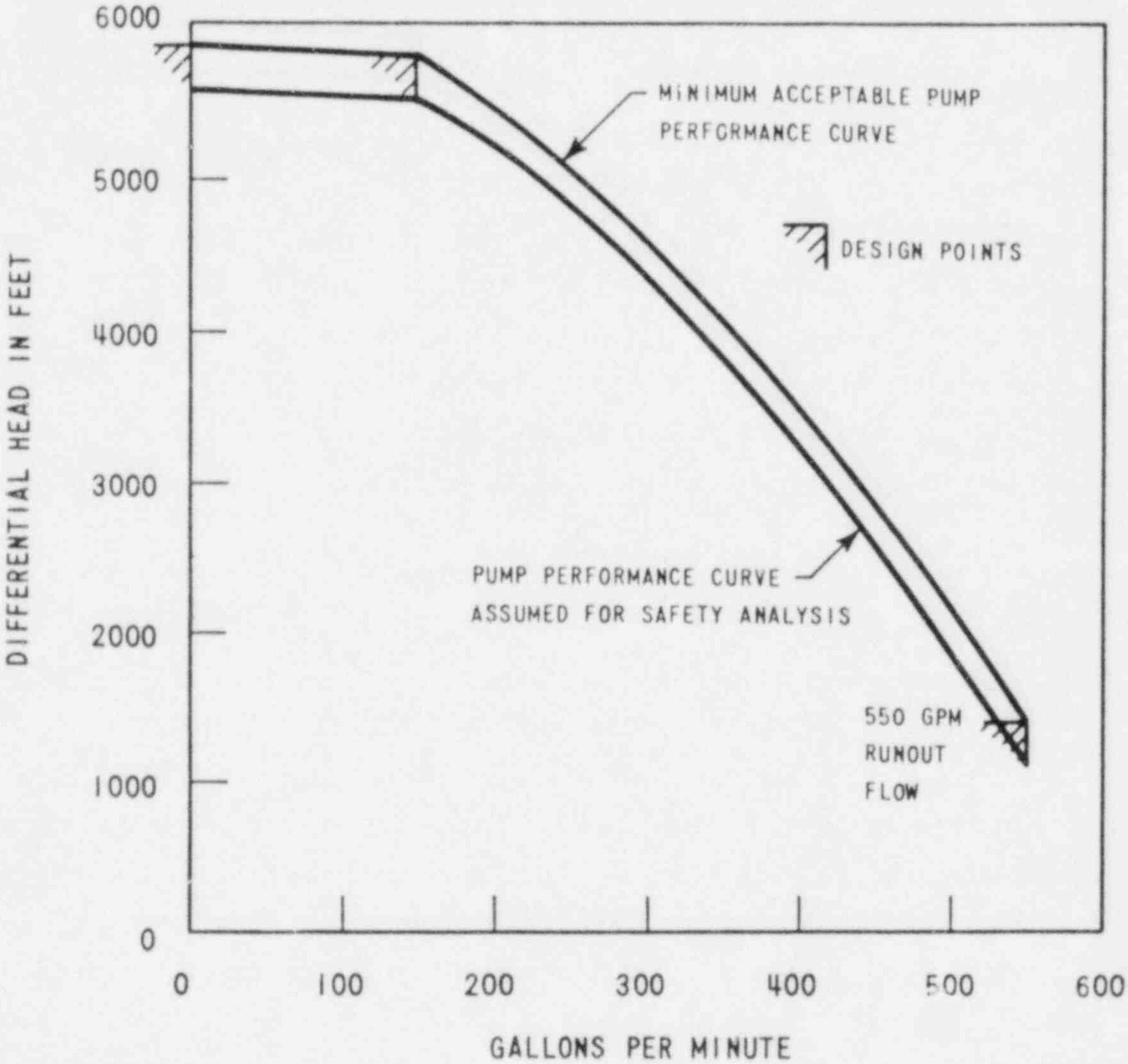


Figure 5.4.2. Typical Centrifugal Charging Pump Design Performance Curves (from RESAR-3S)

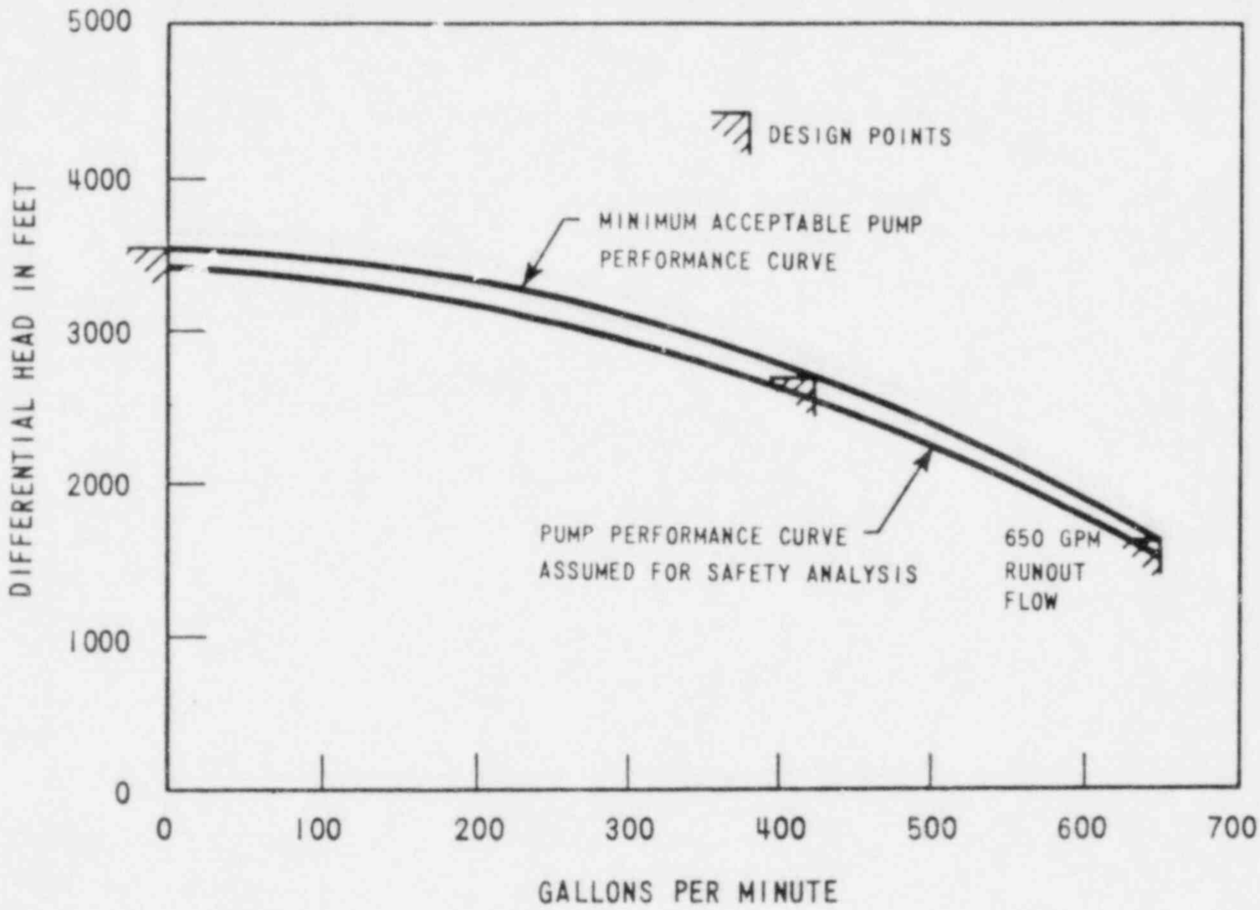


Figure 5.4.3. Typical HPSI Pump Design Performance Curves (from RESAR-3S).

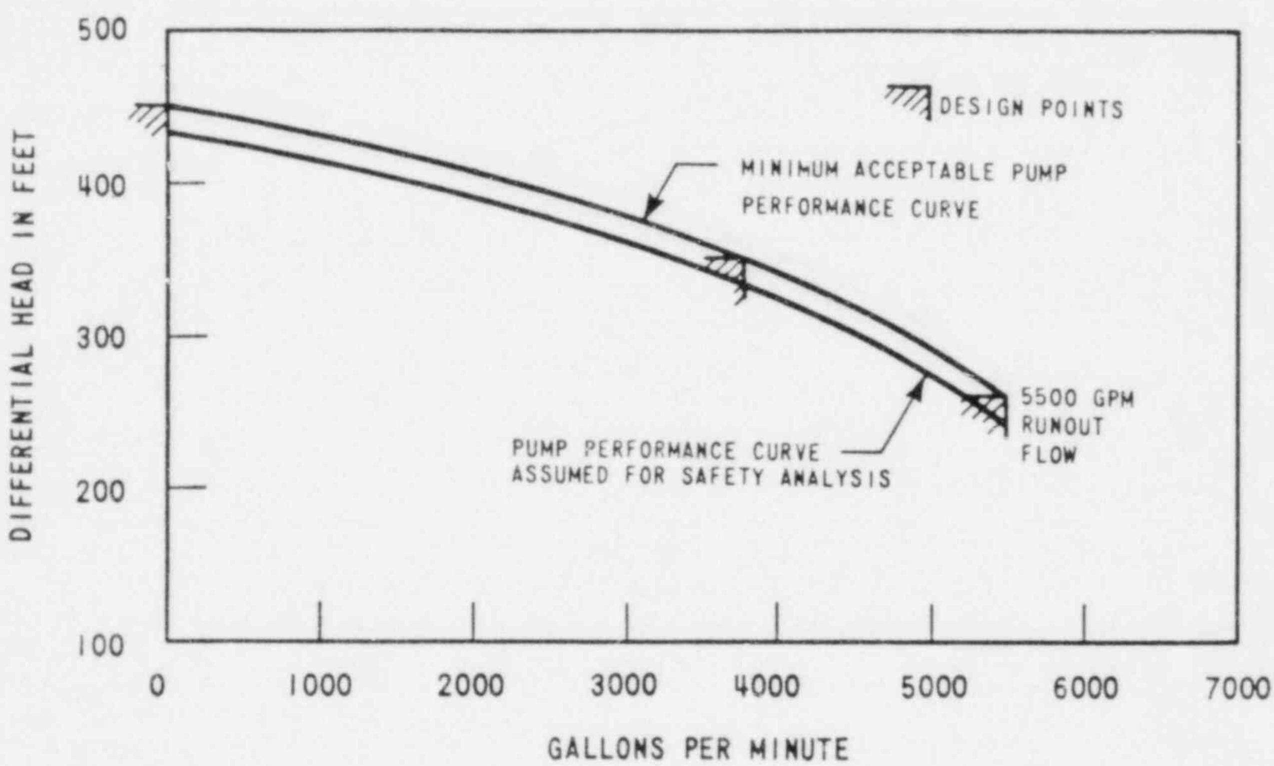


Figure 5.4.4. Typical LPSI Pump Design Performance Curves (from RESAR-3S)

The AFW system also plays an important role in mitigating some small break loss-of-coolant accidents (LOCAs). Small break LOCAs traditionally are considered to include breaks with an equivalent diameter up to six inches. Within this class of LOCAs, there are two distinctly different plant responses. Analysis predicts that PWR LOCA sizes greater than approximately two inches in diameter have the capacity to remove energy from the primary system at a rate greater than that introduced by the core decay heat source, independent of heat removal from the steam generators (Refs. 3, 4, and 5). As a result, RCS depressurization occurs, and coolant makeup can be provided by the HPSI portion of the ECCS or by the ECCS accumulators. Breaks smaller than two inches equivalent diameter are dependent for a portion of the heat removal function on the steam generators to depressurize the RCS. Without heat removal via the steam generators, the RCS will remain at high pressure. In this condition, many plants will be unable to provide coolant makeup with the ECCS system because reactor pressure exceeds the shutoff head of the high pressure safety injection pumps.

There is a wide variety of AFW system designs. Many of these designs are described in References 3, 4, and 6. The pump complement found in AFW systems is summarized in Section 5.25 and a AFW system is illustrated in Figure 5.4.5 (from Ref. 3). A representative performance curve for an AFW pump is illustrated in Figure 5.4.6.

5.4.3 Plant Conditions During Sabotage Scenario

A total loss of feedwater has occurred following loss of the main and auxiliary feedwater systems. The pressurizer safety or power-operated relief valve (PORV) will initially open and then reclose. Initially, RCS pressure and temperature will drop following valve closure because for a limited period of time, there may be more energy removed by the steam generators than is being put into the system by the stored and decay heat of the core. As the steam generators boil off their secondary-side water inventory, this imbalance will shift so that more heat is being added to the RCS than is being removed through the steam generators. RCS temperature and pressure will rise again to the PORV and/or safety valve setpoint (Ref. 6). The steam generators are expected to boil dry in 14 to 43 minutes (Refs. 3 and 4).

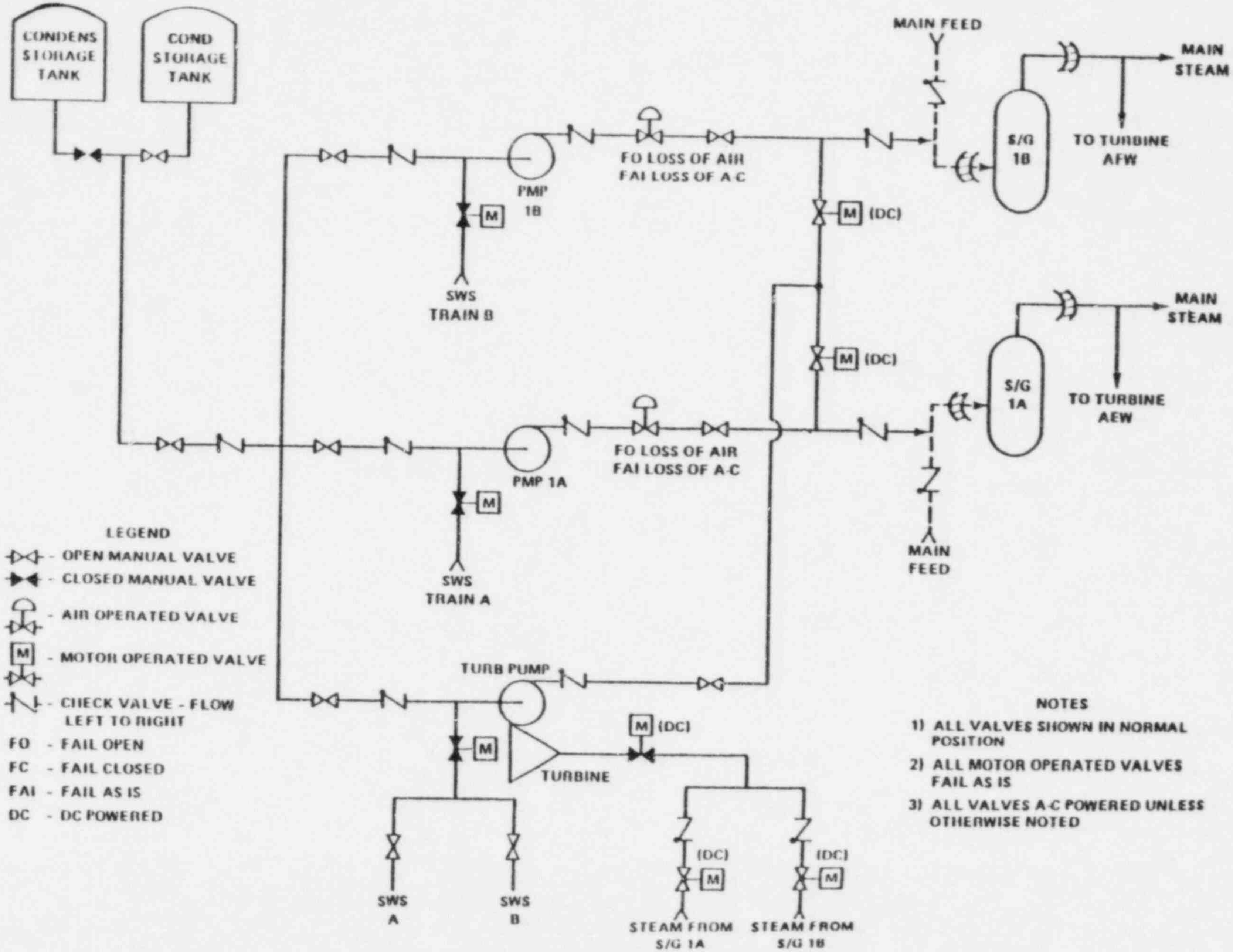


Figure 5.4.5. Auxiliary Feedwater System, Kewaunee Nuclear Plant (from NUREG-0611).

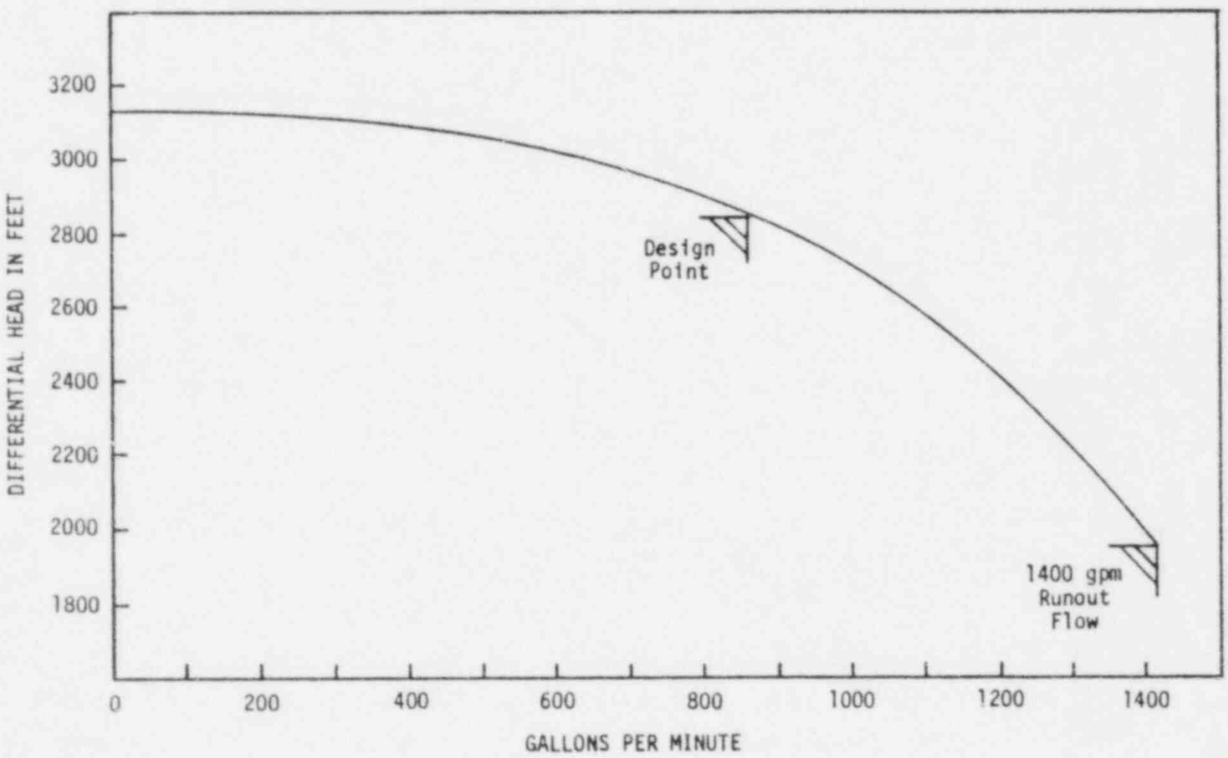


Figure 5.4.6. Typical AFW Pump Design Performance Curve.

Following steam generator dryout, blowdown through the pressurizer safety valves is the only significant heat removal path from the RCS. The primary system will likely remain at high pressure.

Plants with safety injection systems capable of pumping against full RCS pressure will be able to maintain adequate core coolant inventory. It should be possible to maintain these plants in a safe condition for an extended period of time, essentially by using a feed-and-bleed method of core cooling. The pressurizer safety valves and power-operated relief valve (if provided), discharge to a quench tank that is not sized to accomodate extended blowdowns. Overpressure protection for the quench tank is typically provided by rupture discs that fail at a predetermined pressure. The open quench tank then vents into the containment. Although not a particularly desirable situation, safety systems are available to perform the key safety functions of core cooling (inventory control), and containment cooling.

Plants without safety injection systems capable of pumping against full RCS pressure would probably not be able to maintain adequate core coolant inventory with the low capacity charging system alone. Under station blackout conditions (e.g., with no makeup to the RCS), it has been estimated that the core will be uncovered to its midplane in approximately two hours (Ref. 7).

5.4.4 System Alignment Necessary to Substitute the Safety Injection System for the Auxiliary Feedwater System

The Yankee Rowe nuclear plant has the capability to use the charging and safety injection systems as a backup to a single steam turbine-driven AFW pump. This system is illustrated in Figure 5.4.7 (from Ref. 3). As described in Ref. 3, the operation of this backup AFW capability is as follows:

> "A backup method of supplying feedwater to the steam generators in the event of failure in the AFWS is the plant's primary coolant system charging pumps with total capacity of approximately 100 gpm (33 gpm/pump). Two of the pumps have variable speed motors. The system is connected permanently by a spool piece that connects to the main feedwater header. The operation of ten manual valves (two drains and eight isolation) is required to initiate flow from this source. The water supply to the charging pumps is the 135,000 gallon Primary Water Storage Tank.

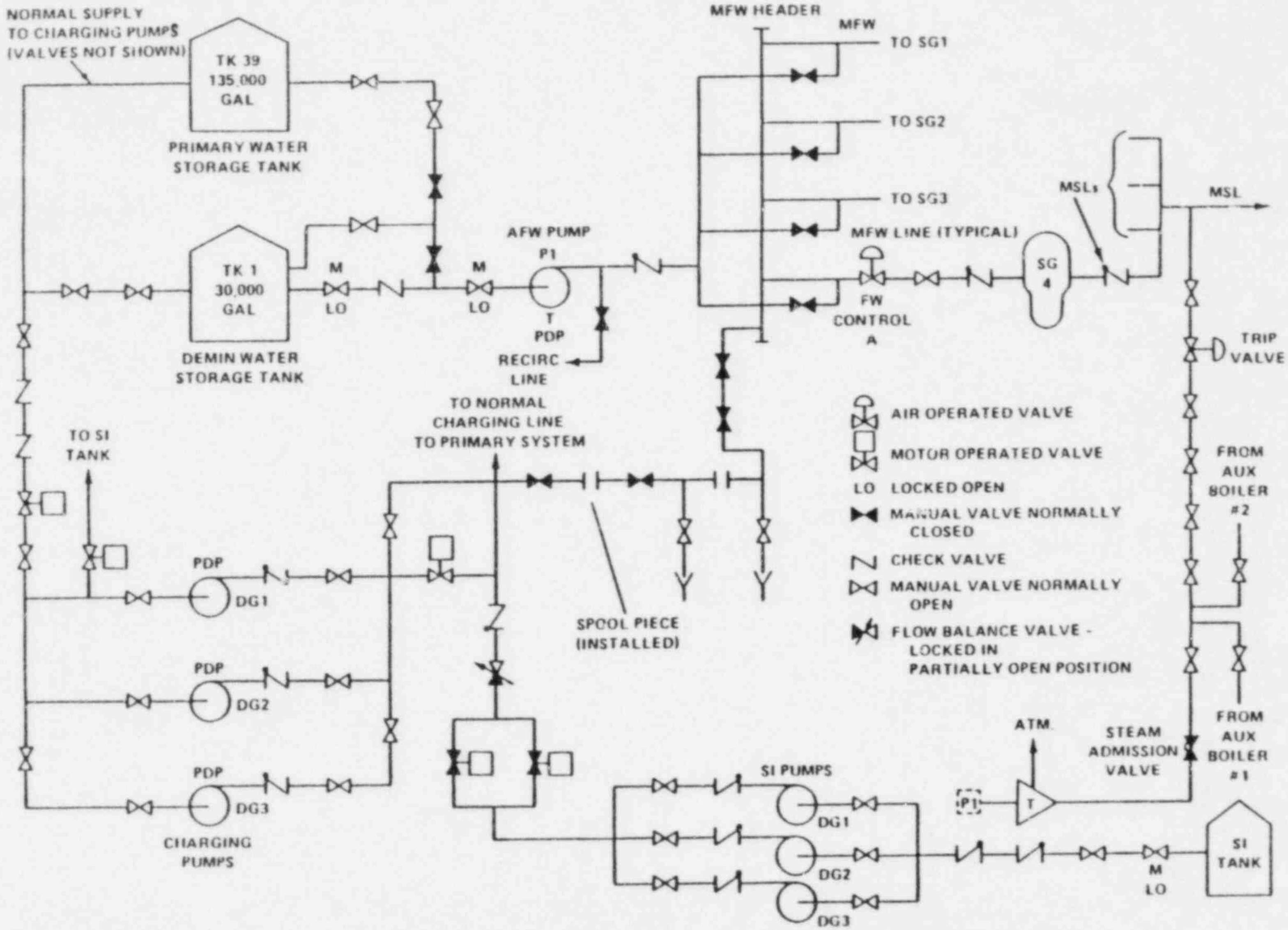


Figure 5.4.7. Auxiliary Feedwater System, Yankee Rowe Nuclear Plant
(from NUREG-0611)

The high pressure safety injection and low pressure safety injection pumps provide another backup method of supplying feedwater to the steam generators. Flow from this source is obtained by the operation of the same manual valves used when the charging system is the source, plus the operation of one of two redundant motor-operated valves (MOV). Flow is then directed to the steam generators through the same permanently connected spool piece used for the charging pump path as described above. The flow available from this source is 200 gpm per train (three trains available)."

Yankee Rowe is an early vintage PWR, and this system interconnection capability is not typical of other PWR plants.

A comparison of AFW, centrifugal charging and HPSI pumps is provided in Table 5.4.1. As is evident from this table, the three types of pumps provide somewhat comparable flow at 2700 feet head (e.g., comparable to the steam generator safety valve setpoints). At a given plant, a centrifugal charging pump and a HPSI pump are generally capable of providing between 50 to 70 percent of the flow of a 100 percent capacity AFW pump. It would therefore be likely that, in most plants, two centrifugal charging or HPSI pumps could provide adequate flow to the steam generators if they could be realigned for this purpose. Remaining charging or HPSI pumps should be left aligned for core coolant inventory control.

Because of the wide variety of AFW and safety injection system designs, an approach for making the system interconnections will be outlined in general terms. Basic features would include the following:

- Valving is provided to align individual safety injection (SI) pump discharges to the RCS or the steam generator, as required. Initially, realignment of two SI pumps to the steam generators would likely be required. Any remaining SI pump(s) could perform its normal reactor coolant inventory control function. As AFW coolant demands decrease, an additional SI pump could be returned to its normal alignment.

- Valving is provided to align individual SI pump suctions to the RWST or to the condensate storage tank, as required. SI pumps performing a reactor coolant inventory control function would be aligned to the RWST and would provide borated water to the RCS. This would be the normal system alignment. When providing coolant to the steam generators, the corresponding pump suctions would be aligned to the condensate storage tank (CST), which is the normal water supply for the AFW system. This will preserve the inventory of borated water in the RWST for primary coolant inventory control.

Table 5.4.1. Comparison of AFW, Centrifugal Charging and HPSI Pump Characteristics

	AUXILIARY FEEDWATER PUMP	CENTRIFUGAL CHARGING PUMP	HIGH PRESSURE SAFETY INJECTION PUMP
TYPE	Multi-stage centrifugal	Multi-stage centrifugal	Multi-stage centrifugal
DESIGN FLOWRATE	260 to 1050 gpm (600 gpm typical)	140 to 306 gpm	375 to 425 gpm
DESIGN HEAD	2500 to 3000 ft. (2700 ft. typical)	5760 to 6500 ft.	2650 to 2822 ft. (2700 ft. typical)
FLOWRATE @ 2700 ft. HEAD (1170 psid)	260 to 1050 gpm	440 to 700 gpm	375 to 500 gpm
HORSEPOWER	600 to 1000	600 to 900	400 to 600

- Interlocks would be provided to match suction and discharge valve alignment if power-operated valves are used. This would prevent the inadvertent introduction of unborated water from the CST into the RCS. If manual valves are used, operating procedures must be developed to ensure proper valve alignment.

- Interlocks are provided to prevent realignment of SI pump dishcarges to the steam generators during large LOCA conditions. Heat removal via the steam generators is not required during large LOCAs. Suitable logic, such as the coincidence of low RCS pressure and high containment pressure, could provide the required interlocks.

- The physical connection between the SI system and the AFW system should be selected on a plant-specific basis. A possible location would be immediately upstream of the containment isolation valves in the AFW supply lines to each steam generator. No new containment penetrations or containment isolation valves would be required, and the impact of faults in the AFW system on the new backup AFW capability would be minimized. The interconnection should also be upstream of any valves operated by the AFW loop selection logic (if provided) which identifies and isolates a failed steam generator. This logic ensures that AFW flow is only provided to an intact steam generator.

- Electrical separation and independence of the SI trains must be maintained throughout the interconnection with the AFW system.

An example of an SI system with such modifications is illustrated in Figure 5.4.8. Plant-specific designs and supporting analysis would be required for real-plant applications of this damage control measure.

5.4.5 Technical and Regulatory Impediments to Damage Control Measure #4

Use of the SI system as a backup to the AFW system is technically feasible. As discussed previously, the Yankee Rowe plant has the AFW and SI systems interconnected. In their review of the AFW system for the Yankee Rowe plant, the NRC had no comments that reflected concern over the use of the SI and charging systems in the alternate role as a backup to the AFW system (Ref. 3).

Analysis would be required to determine the full impact of the interconnections on SI and AFW system reliability. Operating procedures would also be required to ensure that adequate core coolant inventory was being maintained when a portion of the SI system was serving in an AFW capacity.

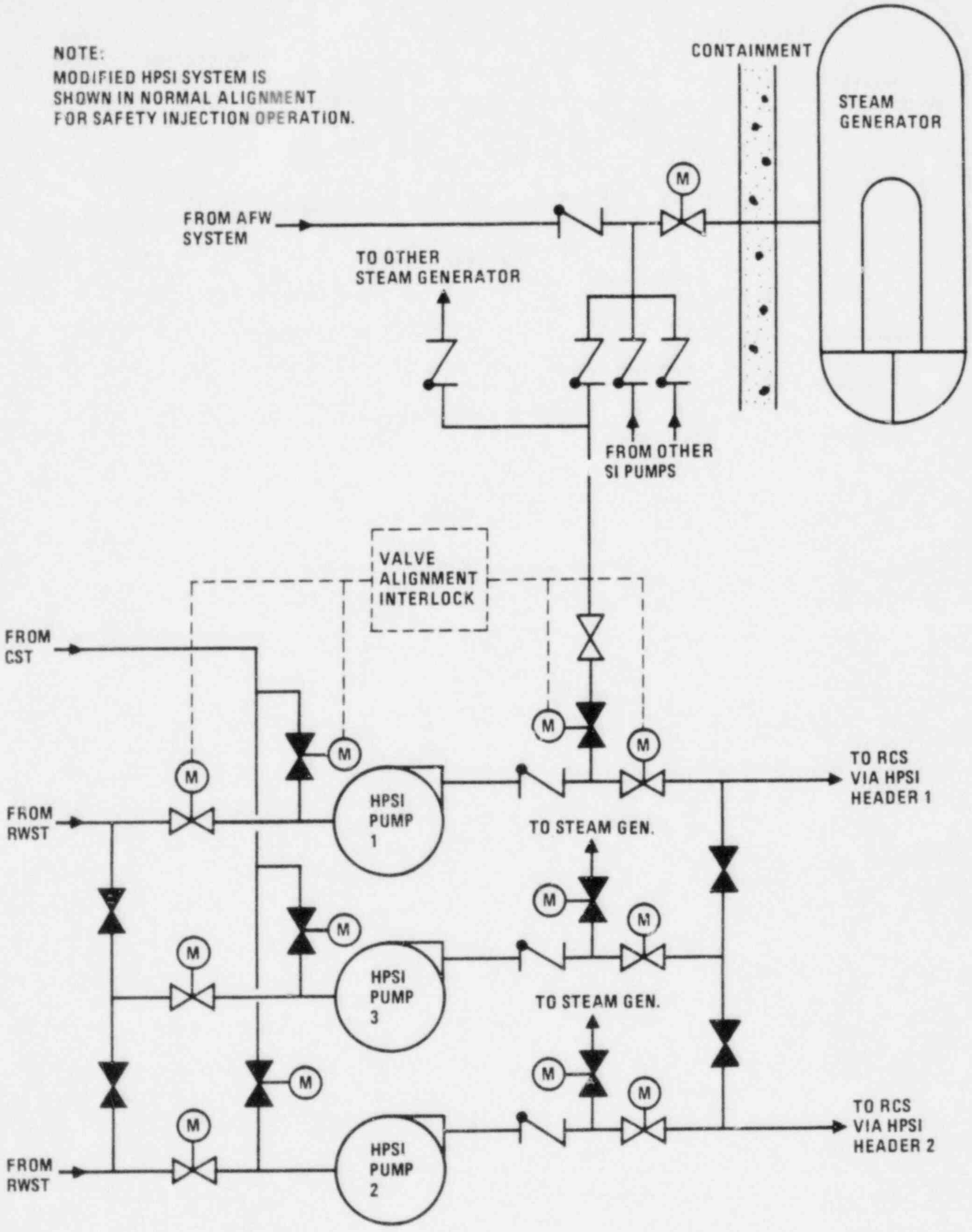


Figure 5.4.8. Modifications to HPSI System To Provide Backup AFW Capability.

5.4.6 Conclusions and Recommendations Regarding Damage Control Measure #4

The importance of the AFW system in mitigating transients and small break LOCAs has been evaluated in detail in recent analyses (Refs. 3 to 6). This damage control measure is technically feasible and may add significantly to the AFW capabilities of PWR plants. The need for AFW cooling must, however, be balanced against the need for a high pressure reactor coolant inventory control capability. This damage control measure would be of most importance in PWR plants that do not have a HPSI system capable of providing makeup against design RCS pressure (see Section 5.9 for a listing of the safety injection capabilities of PWR plants). This damage control measure may be of less importance in PWR plants that have an adequate core coolant makeup capability at design RCS pressure.

5.4.7 Section 5.4 References

1. Lobner, P., et al., "The Pressurized Water Reactor - A Review of a Typical Combustion Engineering PWR Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

2. "Reference Safety Analysis Report-RESAR 3S," Docket STN-50545, Westinghouse Nuclear Energy Systems.

3. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Westinghouse-Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

4. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5. NUREG-0565, "Generic Evaluation of Small Break Loss of Coolant Accident Behavior in Babcock and Wilcox Designed 177-FA Operating Plant," U. S. Nuclear Regulatory Commission, January 1980.

6. NUREG-0560, "Staff Report on Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock and Wilcox Company," U. S. Nuclear Regulatory Commission, May 1979.

7. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

5.5 DAMAGE CONTROL MEASURE #5 - PWR

The purpose of damage control measure #5 is to provide an emergency decay heat removal capability by manually venting the steam generators to the atmosphere via the main condensers in the event that the main steam safety valves and the power-operated atmospheric steam dump valves are disabled by sabotage action.

5.5.1 Sabotage Scenario

Loss of offsite power occurs and the main turbine generator trips on loss of load. The steam generator secondary-side pressure relief valves are inoperable.

5.5.2 System Descriptions

5.5.2.1 Main Steam Pressure Relief Systems

A. Main Steam Safety Valves

The spring-loaded main steam safety valves provide overpressure protection for the secondary-side of the steam generators and the main steam piping. In a four-loop Westinghouse PWR, there are four or five safety valves mounted between the steam generator and the main steam isolation valves in each of four main steam lines. In a two-loop Combustion Engineering or Babcock and Wilcox PWR, there may be as many as nine or ten safety valves on each main steam line. Main steam safety valve setpoints are staggered so that all valves do not cycle at the same time. The lowest main steam safety valve setpoint is usually equal to the steam generator design pressure (about 1085 psig). The highest setpoint is usually 105 percent of the steam generator design pressure (about 1140 psig). The set of safety valves on each steam generator must be capable of limiting maximum transient pressure to 110 percent of design pressure (Ref. 1).

As summarized in Table 5.5.1, total main steam relief valve capacity is in the range from 106 to 185 percent of rated main steam flow (data abstracted from Ref. 2). Individual relief valve capacity is in the range from 750 to 1050 Klb/hr. An upper limit may be set on the capacity of an individual safety valve to limit the potential consequences of an accidental depressurization of the main steam system due to an inadvertent opening of a single safety valve.

Table 5.5.1. Summary of PWR Main Steam Safety Valve and Turbine Bypass Capacities(a).

Plant	Type(b)	Main Steam Safety Valve Capacity(c)	Turbine Bypass Capacity(c)
San Onofre 1	W	(?)	10
Prairie Island 1 & 2	W	129	10
Trojan	W	145	40
Salem 1	W	110	40
Ginna	W	128	40
North Anna 1 & 2	W	118	40
Point Beach 1 & 2	W	111	40
Kewaunee	W	155	40
D.C. Cook 1 & 2	W	141	85
Farley 1 & 2	W	116	40
H. B. Robinson	W	160	40
Zion 1 & 2	W	139	40
Haddam Neck	W	122	40
Indian Point 2	W	121	40
Indian Point 3	W	124	45
Beaver Valley	W	185	85
Turkey Point 3 & 4	W	110	40
Surry 1 & 2	W	(?)	40
Arkansas Nuclear One-2	C-E	170	32
Calvert Cliffs 1 & 2	C-E	(?)	40
Maine Yankee	C-E	(?)	45
Millstone 2	C-E	121	43
Palisades	C-E	152	5
Saint Lucie 1	C-E	146	5
Three Mile Island 1	B&W	120	15
Three Mile Island 2	B&W	106	21
Crystal River	B&W	131	15
Oconee 1, 2 & 3	B&W	117	25
Rancho Seco	B&W	(?)	15
Davis Besse	B&W	126	25
Arkansas Nuclear One-1	B&W	121	15

Notes: (a) Data abstracted from NUREG/CR-2069, "Summary Report on a Survey of Light Water Reactor Safety Systems"

(b) W = Westinghouse, C-E = Combustion Engineering, B&W = Babcock & Wilcox

(c) Capacity is listed as a percent of design main steam flow rate. Data that was not available is indicated by a "(?)".

B. Power-Operated Atmospheric Steam Dump Valves

A power-operated atmospheric dump valve is installed between the steam generator and the main steam isolation valves in each main steam line. These valves provide for controlled removal of reactor decay heat when the main condenser is not in service and are used in conjunction with the auxiliary feedwater (AFW) system when the main feedwater system is also not in service (e.g., following loss of offsite power). The power-operated atmospheric steam dump valves are each rated at about five percent of the total rated main steam flow (e.g., up to about 400 Klb/hr per valve).

The atmospheric steam dump valves are operated by a pneumatic system (e.g., instrument air system with backup accumulators). A remote-manual operating capability from the control room is provided in addition to a local manual operating capability. The valves fail closed on loss of pneumatic pressure or electrical control power.

C. Main Turbine Bypass System

The turbine bypass system is an automatically actuated system that is designed to limit main steam pressure following a variety of transient conditions (e.g., partial load rejection) without requiring operation of the main steam safety valves or reactor scram. The TBS is also used for decay heat removal during normal plant cooldown when the main condenser is available as a heat sink. The TBS takes steam from the main steam lines upstream of the main turbine stop valves and discharges directly to the main condenser, as illustrated in Figure 5.5.1. As summarized in Table 5.5.1, turbine bypass capacity in PWR plants is in the range from 15 to 85 percent of rated main steam flow (data abstracted from Ref. 2).

A representative steam bypass control system is shown in Figure 5.5.2 (from Ref. 3). The steam bypass control system compares the measured steam header pressure with a calculated pressure setpoint. A master controller modulates the operation of the pneumatic turbine bypass valves in a sequential manner to establish the required bypass flow rate. A quick opening demand signal is generated whenever the size of the load rejection is such that it cannot be accommodated with the normal valve modulation speed. The number of valves to which the quick opening signal is applied is a function of the magnitude of the load rejection.

A bypass valve permissive signal is generated when main condenser vacuum is greater than a specified setpoint (e.g., about 18 inches Hg absolute). The TBS cannot be operated when main condenser vaccum is less than the setpoint value. Such low vacuum conditions would likely exist following loss of the main circulating water system, loss of steam jet air ejectors and loss of offsite power.

The bypass valves fail closed on loss of pneumatic system pressure or electrical power to the control system or solenoid pilot valves.

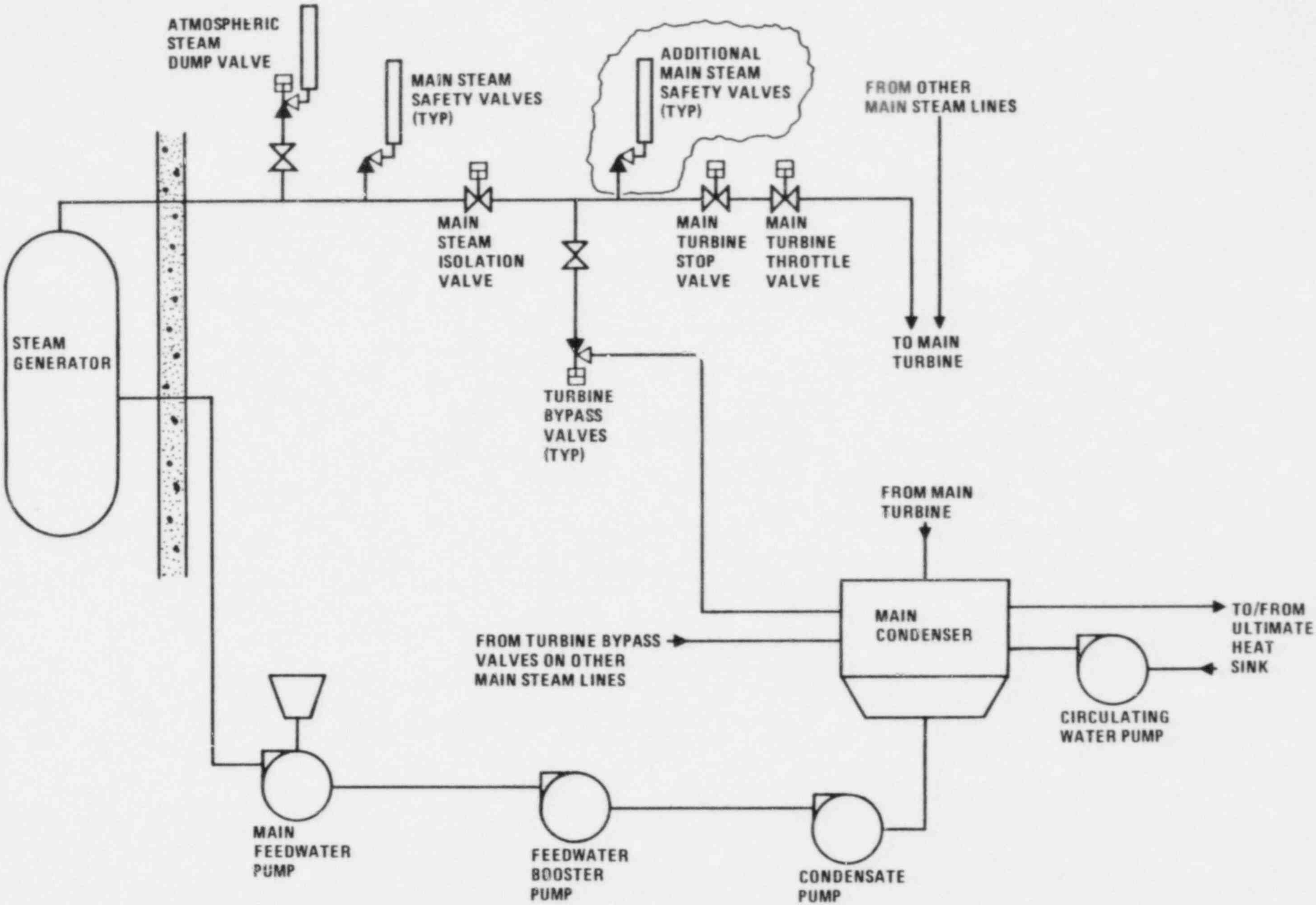


Figure 5.5.1. Simplified Main Turbine Bypass System Diagram.

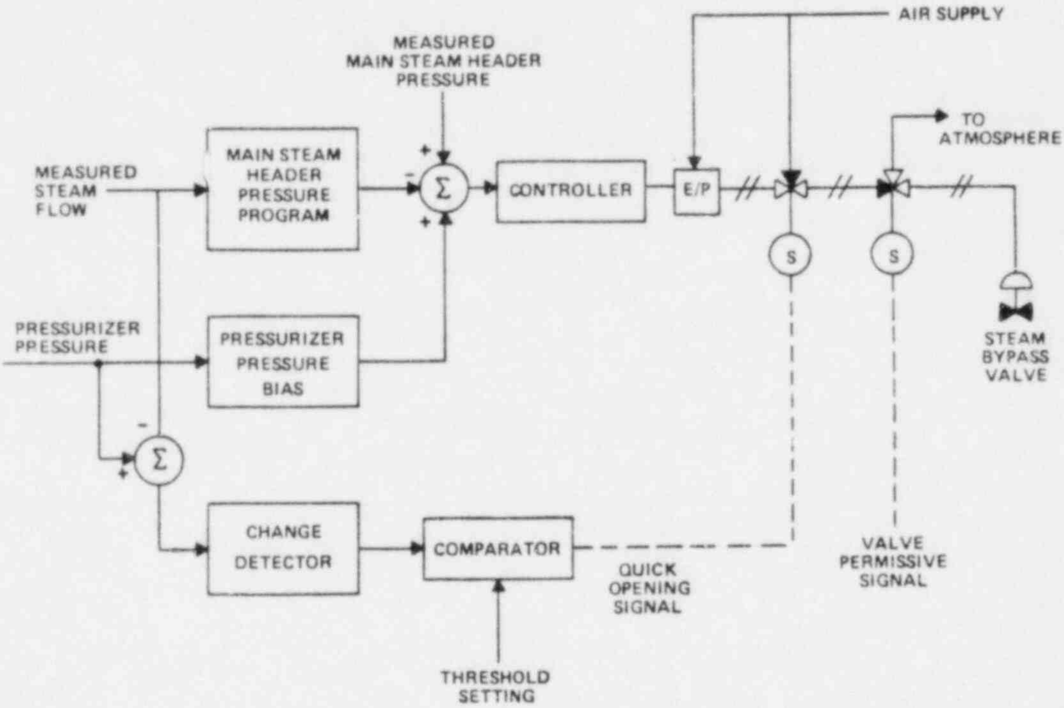


Figure 5.5.2. Main Turbine Bypass Control System Simplified Block Diagram (from Ref. 3).

5.5.2.2 Main Tubine and Condenser Overpressure Protection Systems

To protect the low pressure (LP) turbines from overpressure as a result of turbine bypass system operation, the bypass control system is provided with a low vacuum trip that blocks operation of the TBS. The LP turbine casings are additionally protected against overpressurization by multiple atmospheric relief diaphragms on each LP turbine. These atmospheric relief diaphragms rupture at a pressure usually in the range from 18 to 22 psia. Separate rupture diaphragms may also be provided to protect the main condenser and the flexible turbine exhaust hood against overpressurization.

5.5.2.3 Main Steam Isolation Valves

Each main steam line has a single hydraulically-operated main steam isolation valve (MSIV) that is normally open during power operation. The MSIVs are located upstream of the turbine bypass system, and therefore must remain open during bypass operations. To ensure MSIV closure when required, redundant solenoid-operated pilot valves powered from separate Class 1E power sources open and dump hydraulic oil from the bottom of the MSIV actuator piston. The MSIV is shut by nitrogen pressure on the top of the actuator piston. The valves fail closed on loss of hydraulic system pressure or loss of electric power to the MSIV control system.

Automatic containment isolation or main steam line isolation systems may initiate MSIV closure. Usually, the MSIVs cannot be reopened again until plant conditions permit manual reset of the actuation logic which caused MSIV closure. Plant conditions which may initiate MSIV closure may include one or more of the following:

- Containment isolation system actuation
  - safety injection actuation
  - containment high pressure
  - reactor coolant system low pressure

- Main steam line isolation actuation
  - steam generator high pressure
  - steam generator low pressure
  - containment high pressure
  - safety injection actuation

5.5.3 Plant Conditions During Sabotage Scenario

Following loss of offsite power and turbine trip, there would be an immediate reduction of steam flow from the steam generators to the turbine due to closure of the turbine stop valves. The turbine bypass system is not available following loss of offsite power. Under these circumstances, steam generator pressure would normally be limited by the operation of the main steam safety valves and steam generator pressure response would be comparable to that illustrated in Figure 5.5.3 (from Ref. 3). All safety valves (all 16 to 20 valves) are assumed to be sabotaged and therefore no overpressure protection exists for the steam generators and main steam lines.

If maximum steam generator pressure should reach twice the design pressure (e.g., about 2200 psig), stresses at the Level D service limits specified in the ASME Boiler and Pressure Vessel Code (Ref. 1) may be imposed on the steam generator vessel and connected piping and valves. The Level D service limits permit gross general deformations with some consequent loss of dimensional stability and damage requiring repair which may require removal of the component from service. See Section 5.9 for additional information on stress and pressure limits imposed by Section III of the ASME Boiler and Pressure Vessel Code.

Without overpressure protection, it is likely that the steam generators and main steam piping will be physically damaged by the pressure transient resulting from loss of offsite power and turbine trip. From Figure 5.5.3, it can be inferred that very high pressures will be reached in the order of tens of seconds, allowing no time to implement alternate, manually-initiated methods of overpressure protection. If the main steam pressure boundary remains intact, it is likely that extensive inspections and analysis would be required, as a minimum, to determine if other actions are necessary to restore the steam

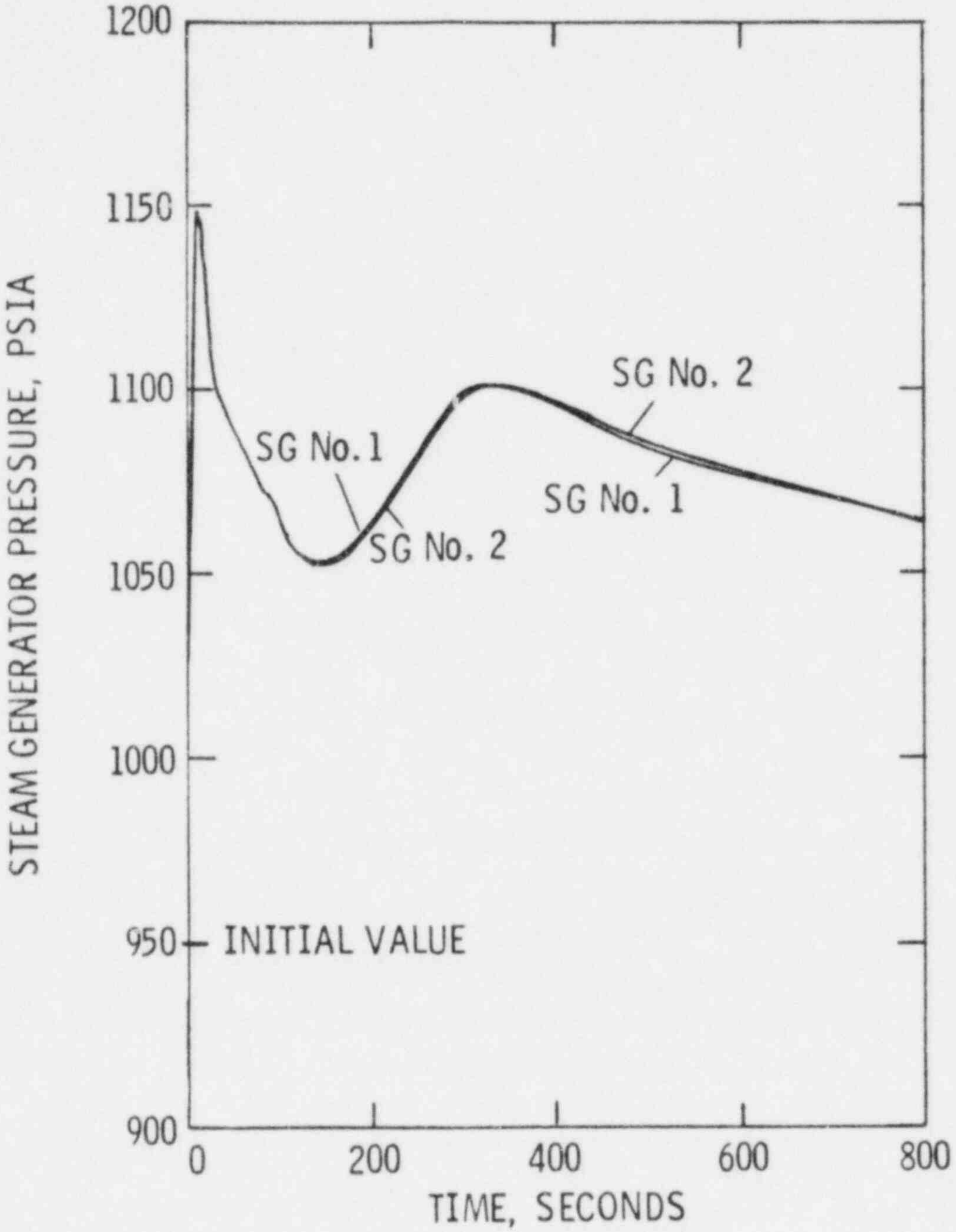


Figure 5.5.3. Typical Steam Generator Pressure Response Following Loss of Offsite Power and Turbine Trip (from Ref. 3).

generators and main steam system to operation. In the worst case, such actions could include steam generator replacement.

5.5.4 System Alignment to Provide an Alternate Path to Vent the Steam Generators to Atmosphere

5.5.4.1 Manually Vent Steam Generators to Atmosphere via the Main Condenser using the Turbine Bypass System

This approach is not technically feasible. See Section 5.5.5.

5.5.4.2 Provide Additional Main Steam Line Safety Valves

An additional set of spring-loaded safety valves, with a capacity comparable to the existing set of code safety valves, could be installed on the main steam lines at a location that is well separated from the code safety valves. The separation is provided to eliminate the possibility that a saboteur could disable the primary and the additional safety valves at a single location. For maximum separation, these additional valves could be connected near the main turbine stop valves. In this location, the redundant steam relief capability is dependent on the MSIVs remaining open (see Figure 5.5.1). If a condition requiring MSIV closure were to occur, the backup overpressure protection capability would be negated.

The redundant steam relief capability must operate automatically to provide rapid response and adequate overpressure protection under the postulated sabotage scenario. The spring-loaded safety valves provide the necessary rapid response. Decay heat removal can be accomplished with the auxiliary feedwater system supplying steam generator makeup and the redundant safety valves cycling as necessary to control steam generator pressure. For better control of decay heat removal, it would be desirable to provide one or more of the safety valves with a power-operated capability to permit the plant operators to modulate steam dumping to atmosphere at pressures below the safety valve mechanical setpoint.

5.5.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #5

There do not appear to be significant technical or regulatory impediments to the addition of a redundant set of safety valves to the main steam lines. The following issues, however, dictate against using the TBS to vent the steam generators to atmosphere via the main condensers following the sabotage of all main steam safety valves:

- Average main turbine bypass capacity is approximately one-third of the total main steam safety valve capacity (see Table 5.5.1). Insufficient TBS capacity exists for adequate overpressure protection of the steam generators.

- Main condenser and low pressure main turbine casing integrity may be jeopardized by continuous TBS steam venting without the main circulating water system in operation. Existing overpressure protection for the main condenser and low pressure main turbine casing may not be adequate for this proposed operating mode of the TBS.

- The TBS would normally be unavailable following loss of offsite power. Substantial control system modifications would be required to make this system available in emergencies. These modifications would include adding the capability to bypass the low condenser vacuum interlock. Impact of the TBS control system modifications on frequency of transients induced by TBS failure (e.g., TBS valves stuck open) should be assessed.

5.5.6 Conclusions and Recommendations Regarding Damage Control Measure #5

Steam generator overpressure protection is a more immediate concern than decay heat removal following loss of offsite power and turbine trip. Use of the TBS to provide overpressure protection following sabotage of all main steam safety valves is not technically feasible. Installation of a redundant set of safety valves could provide a backup overpressure protection capability and would support subsequent decay heat removal for those events which do not require MSIV closure.

5.5.7 Section 5.5 References

1. ASME Boiler and Pressure Vessel Code, Section III, American Society of Mechanical Engineers.

2. Heddleson, F. A., "Summary Report on a Survey of Light Water Reactor Safety Systems," NUREG/CR-2069, Oak Ridge National Laboratory, Nuclear Safety Information Center, October 1981.

3. "San Onofre Nuclear Generating Station Units 2 and 3, FSAR," Docket 50361, Southern California Edison and San Diego Gas and Electric.

5.6 DAMAGE CONTROL MEASURE #6 - BWR

The purpose of damage control measure #6 is to use the high pressure coolant injection (HPCI) system or the high pressure core spray (HPCS) system to supply coolant to the reactor vessel in the event that the reactor core isolation cooling (RCIC) system has been sabotaged.

5.6.1 Sabotage Scenario

Loss of offsite power occurs. The main turbine generator trips on loss of load. The power conversion system (main steam, feedwater and condensate and circulating water system) is unavailable. The emergency diesel generators operate and supply Class 1E power to safety-related systems. The RCIC system has been sabotaged. Other safety-related systems operate properly.

5.6.2 System Description During Normal Operation

The RCIC system (found in BWR/3 to BWR/6 plants) is normally in standby. During power operation, reactor coolant inventory control is maintained by the feedwater system, with some minor additional makeup from normal control rod drive hydraulic system leakage into the reactor coolant system. The RCIC system is actuated automatically on reactor vessel low water level. The single, 100 percent capacity, turbine-driven RCIC pump is intended to provide adequate core cooling when the reactor vessel is isolated from the main condenser (e.g., the main steam isolation valves are closed) and normal feedwater flow is lost. In this condition, the reactor coolant system will be at high pressure, with energy being removed by blowdown through the safety valves to the suppression pool. Continued RCIC system operation in the injection mode will cause a fairly rapid heatup of the suppression pool, necessitating the actuation of suppression pool cooling systems or the changeover to the closed-loop steam-condensing mode of RCIC system operation (found in BWR/5 and BWR/6 plants). In this mode of RCIC operation, energy is removed from the reactor coolant system via the residual heat removal (RHR) heat exchangers operating in the steam-condensing mode. The safety valves will close, and suppression pool heatup rate will be reduced to approximately $3^{0}F/hr$ from RCIC turbine exhaust (Ref. 1). Requirements for suppression pool cooling can thereby be postponed. The RCIC system is not considered as part of the emergency core cooling system (ECCS). A typical RCIC system is illustrated in Figure 5.6.1 (from Ref. 2).

Like the RCIC, the HPCI system (found in BWR/3 and BWR/4 plants) is normally in standby. This system is part of the ECCS, and is automatically actuated on either reactor vessel low water level or high drywell pressure. The single, 100 percent capacity, turbine-driven HPCI pump is intended to provide adequate coolant inventory in the reactor vessel across a spectrum of LOCA conditions that do not result in rapid depressurization of the reactor coolant system. By design, the system also serves as a backup to the injection mode of the RCIC system. HPCI flow rate is approximately five to eight times that of the RCIC system at comparable pump head (e.g., 1120 psid). A typical HPCI system is illustrated in Figure 5.6.2 (from Ref. 2).

The HPCS system (found in BWR/5 and BWR/6 plants) is functionally a motor-driven equivalent of an HPCI system. The HPCS, by design, serves as a backup to the injection mode of the RCIC system. A typical HPCS system is illustrated in Figure 5.6.3 (from Ref. 2). Table 5.6.1 presents a comparison of typical RCIC, HPCI and HPCS systems.

5.6.3 System Conditions During Sabotage Scenario

When normal feedwater is lost, water level in the reactor vessel will fall. RCIC and HPCI (or HPCS) systems are typically actuated when the water level drops to approximately ten feet above the top of the active fuel (e.g., Level 2). If RCIC fails to start, coolant inventory will be adequately maintained by the HPCI (or HPCS) system.

5.6.4 System Alignment Necessary to Substitute the HPCI or HPCS System for the RCIC System

There is no need to provide additional measures to use the HPCI or HPCS system as a substitute for the RCIC system. The HPCI system is normally aligned to inject coolant into the core during a loss of coolant accident or to provide reactor cooling and coolant inventory control functions if the RCIC should fail to operate when required.

Table 5.6.1. Comparison of Typical RCIC, HPCI and HPCS Systems

	RCIC[1]	HPCI[2]	HPCS[3]
Number of Pumps	1	1	1
Type of Pump	Multi-Stage Centrifugal	Multi-Stage Centrifugal	Multi-Stage Centrifugal
Drive	Steam Turbine	Steam Turbine	Electric Motor
Horsepower	460-925	2675-4600	3000-3500
Flowrate (@ Pump Head)	400-800 gpm (@ 1120 psid)	2980-4250 gpm (@ 1120 psid)	1465-1650 gpm (@ 1130 psid)
Water Source	Condensate Storage Tank or Suppression Pool	Same	Same
Actuation Signal	Low Reactor Vessel Water Level	Low Reactor Vessel Water Level or High Drywell Pressure	Low Reactor Vessel Water Level or High Drywell Pressure
Modes of Operation	Injection or Steam Condensing[4]	Injection	Injection

Notes: (1) BWR/3 to BWR/6 plants, except Dresden 2 & 3, and Millstone 1.
(2) BWR/3 and BWR/4 plants, except Millstone 1.
(3) BWR/5 and BWR/6 plants.
(4) Steam condensing only in BWR/5 and BWR/6 plants.

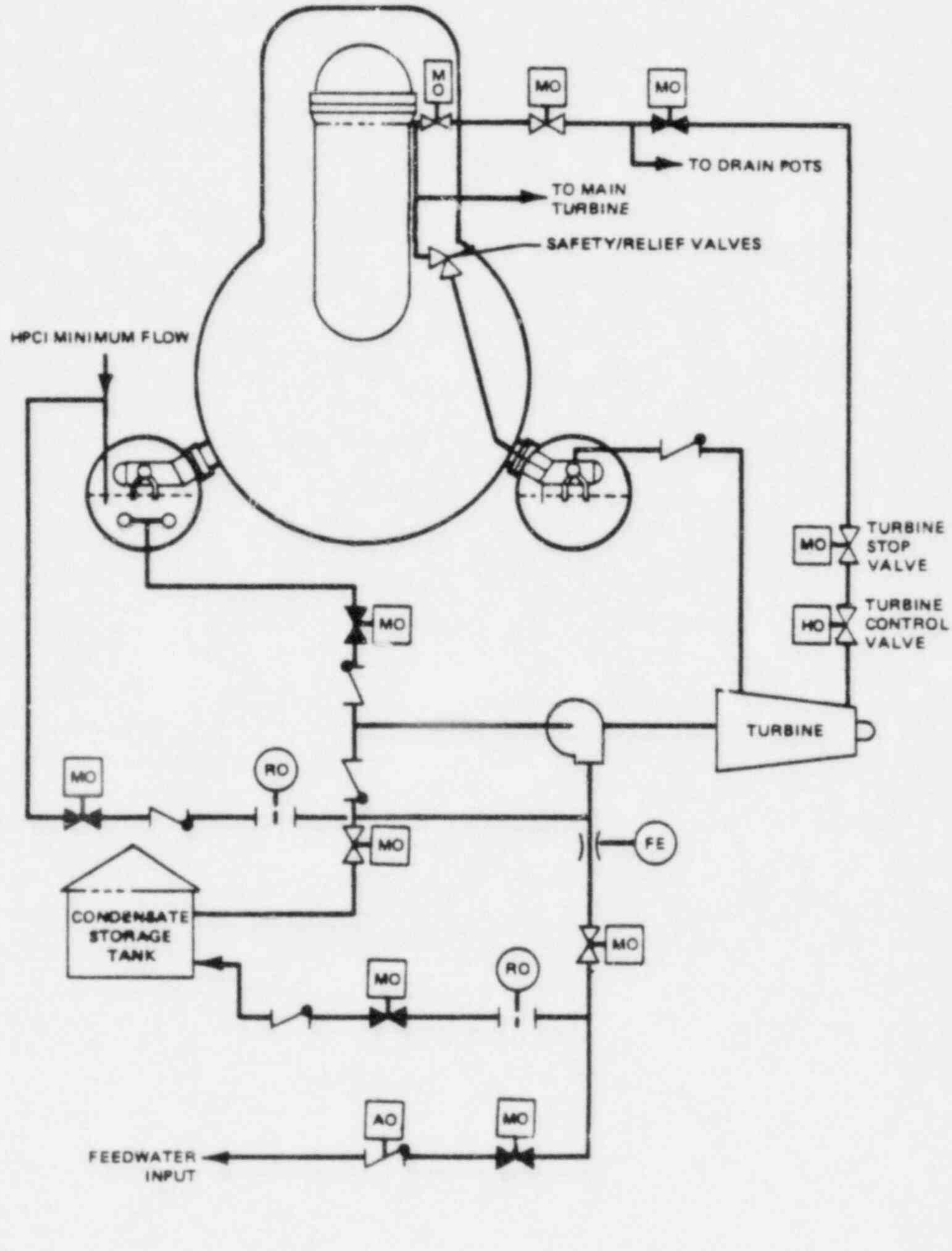


Figure 5.6.1. Reactor Core Isolation Cooling (RCIC) System, Injection Mode Only (From NUREG-0626).

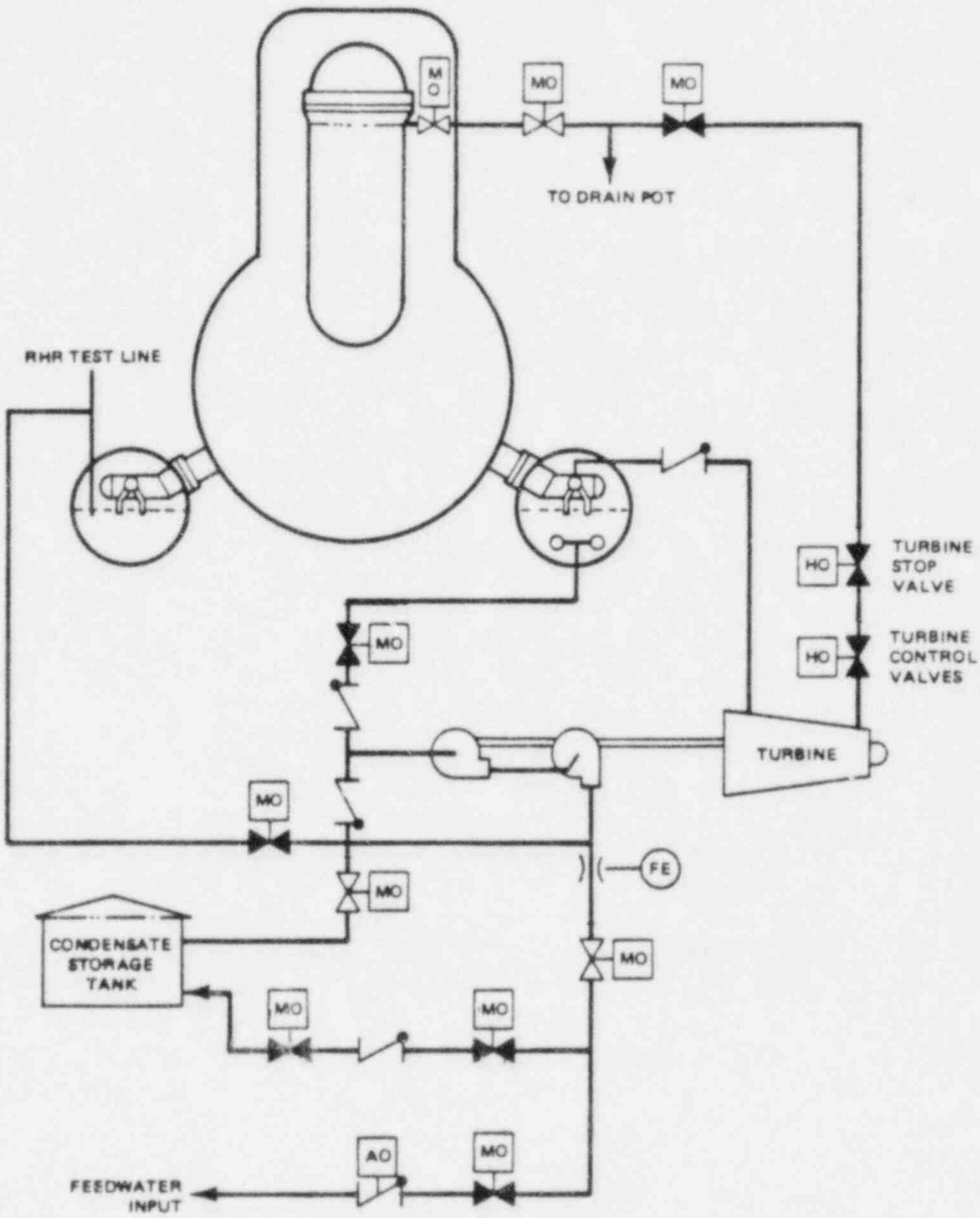


Figure 5.6.2. High Pressure Coolant Injection (HPCI) System (From NUREG-0626).

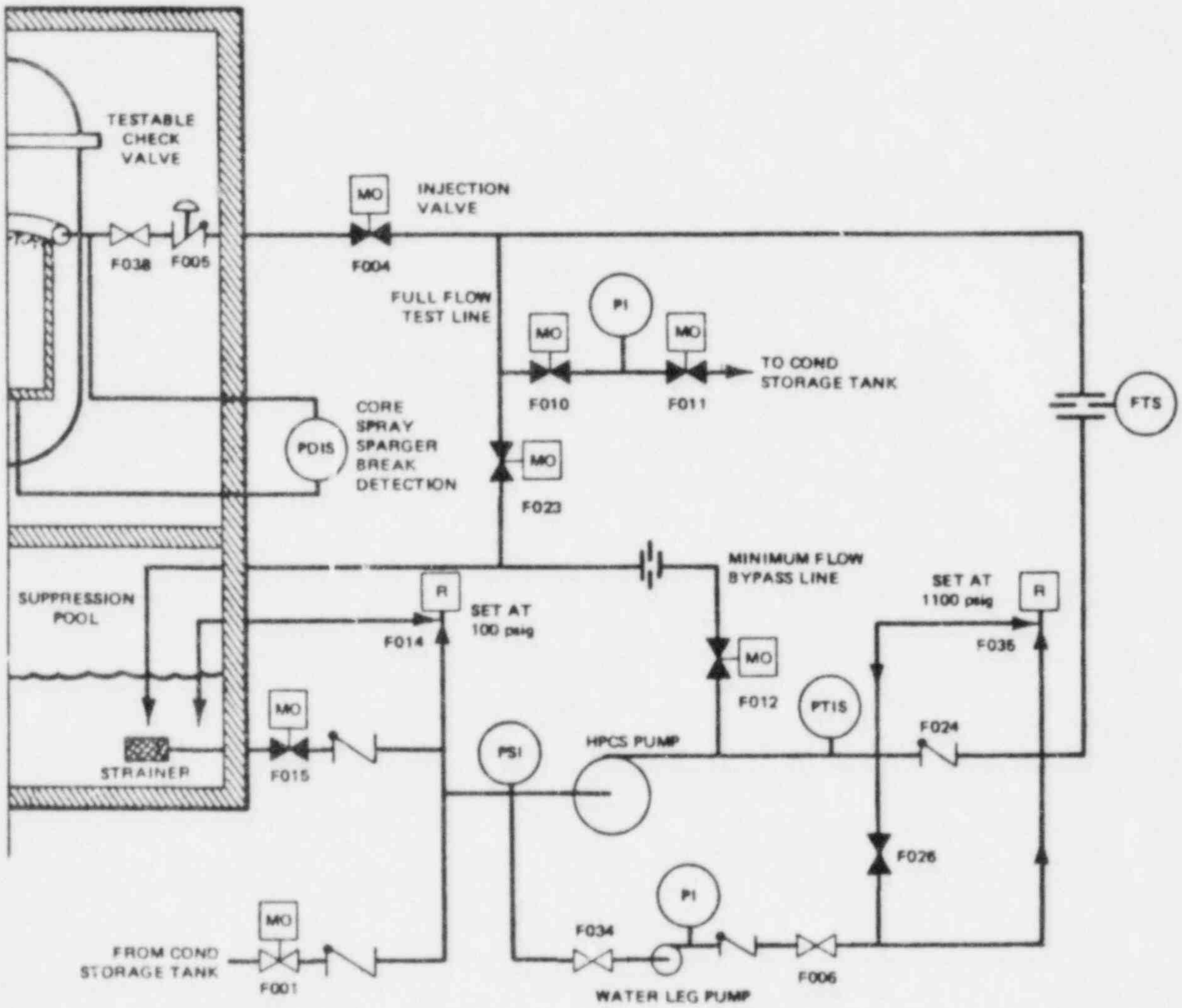


Figure 5.6.3. High Pressure Core Spray (HPCS) System (From NUREG-0626).

5.6.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #6

None

5.6.6 Conclusions and Recommendations Regarding Damage Control Measure #6

This damage control measure is, in actuality, a normal design feature of most BWRs.

5.6.7 Section 5.6 References

1. "238 Nuclear Steam Supply System - GESSAR," Docket STN-50550, General Electric Company.
2. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

5.7 DAMAGE CONTROL MEASURE #7 - BWR

The purpose of damage control measure #7 is to use an alternate service water system to supply cooling water to the secondary side of the residual heat removal (RHR) or suppression pool cooling system exchanger in the event that the essential service water pumps are disabled.

5.7.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of the service water pumps that supply cooling water to the suppression pool cooling heat exchangers (in most BWR plants, these are the residual heat removal system heat exchangers). The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to Class 1E AC buses. The reactor core isolation cooling (RCIC) and the high pressure coolant injection (HPCI) or high pressure core spray (HPCS) systems operate properly to maintain reactor coolant inventory. The suppression pool cooling (or RHR) system is operable, but a complete heat transfer path from the suppression pool to the ultimate heat sink cannot be established.

5.7.2 System Descriptions

5.7.2.1 Suppression Pool Cooling Systems

See Section 5.2.

5.7.2.2 Residual Heat Removal System

See Section 5.11.

5.7.2.3 BWR Service Water Systems

A. Essential Service Water (ESW) System

In many BWR plants, the ESW system is the normal system for completing the heat transfer path between the RHR heat exchangers and the ultimate heat sink. A representative BWR essential service water system is described in Section 5.13. The ESW system is powered from the Class 1E electrical power system and is operable following loss of offsite power.

B. Nonsafety-Related Service Water Systems

Other service water systems provide cooling for a variety of nonsafety related equipment. Specific design details vary greatly among plants. Generally, these systems receive Nonclass 1E power and are not available following loss of offsite power.

5.7.3 Plant Conditions During Sabotage Scenario

Following loss of offsite power and main turbine trip, the primary coolant system safety/relief valves will open, as necessary, to provide overpressure protection for the reactor coolant system (RCS). After the initial blowdown to the suppression pool, core decay heat will be transferred to the suppression pool by intermittent safety/relief valve operation and by operation of the turbine-driven reactor core isolation cooling (RCIC) and/or high pressure coolant injection (HPCI) pumps which exhaust to the suppression pool. It has been estimated that a suppression pool will reach 150^{o}F approximately 3.1 hours following loss of offsite power with no suppression pool cooling (Ref. 1). Suppression pool temperature will continue to rise unless service water can be restored to the RHR heat exchangers or other measures can be taken to stabilize suppression pool temperature (e.g., see damage control measure #2).

5.7.4 System Features Necessary to Align an Alternate Service Water System to the Suppression Pool Cooling (or RHR) Heat Exchangers

The basic interface requirement to be met by an alternate service water system is that adequate cooling water flow be provided to the RHR heat exchangers. Estimated service water flow rate requirements are listed in Table 5.7.1. Any service water system that can provide this flow rate is a potentially viable substitute for the ESW pumps. An approach for connecting an alternate service water system to an RHR heat exchanger is illustrated in Figure 5.7.1. The alternate service water supply is manually aligned when required. The existing ESW outfall (return) line continues to be used. An alternate outfall line could also be added to further improve the flexibility of the system to bypass disabled components. If an alternate outfall line is used, it should be provided with a radioactivity monitoring capability (e.g., gross gamma

Table 5.7.1. Estimated Service Water Flow Rate Required by RHR Heat Exchangers.

TIME AFTER SHUTDOWN	DECAY HEAT POWER RELATIVE TO OPERATING POWER(1)	APPROPRIATE SERVICE WATER FLOW RATE TO RHR HEAT EXCHANGERS(2)	
		2000 MWt BWR	3000 MWt BWR
10^4 sec. (2.8 hrs.)	9.976×10^{-3}	6800 gpm	10000 gpm
10^5 sec. (28 hrs.)	5.26×10^{-3}	3600 gpm	5400 gpm

Notes: (1) From ANSI/ANS 5.1-1979, "Decay Heat Power in Light Water Reactors," Example 3

(2) Assumes 100°F service water inlet temperature, 120°F outlet temperature, and that RHR heat exchangers transfer actual decay heat load to service water system

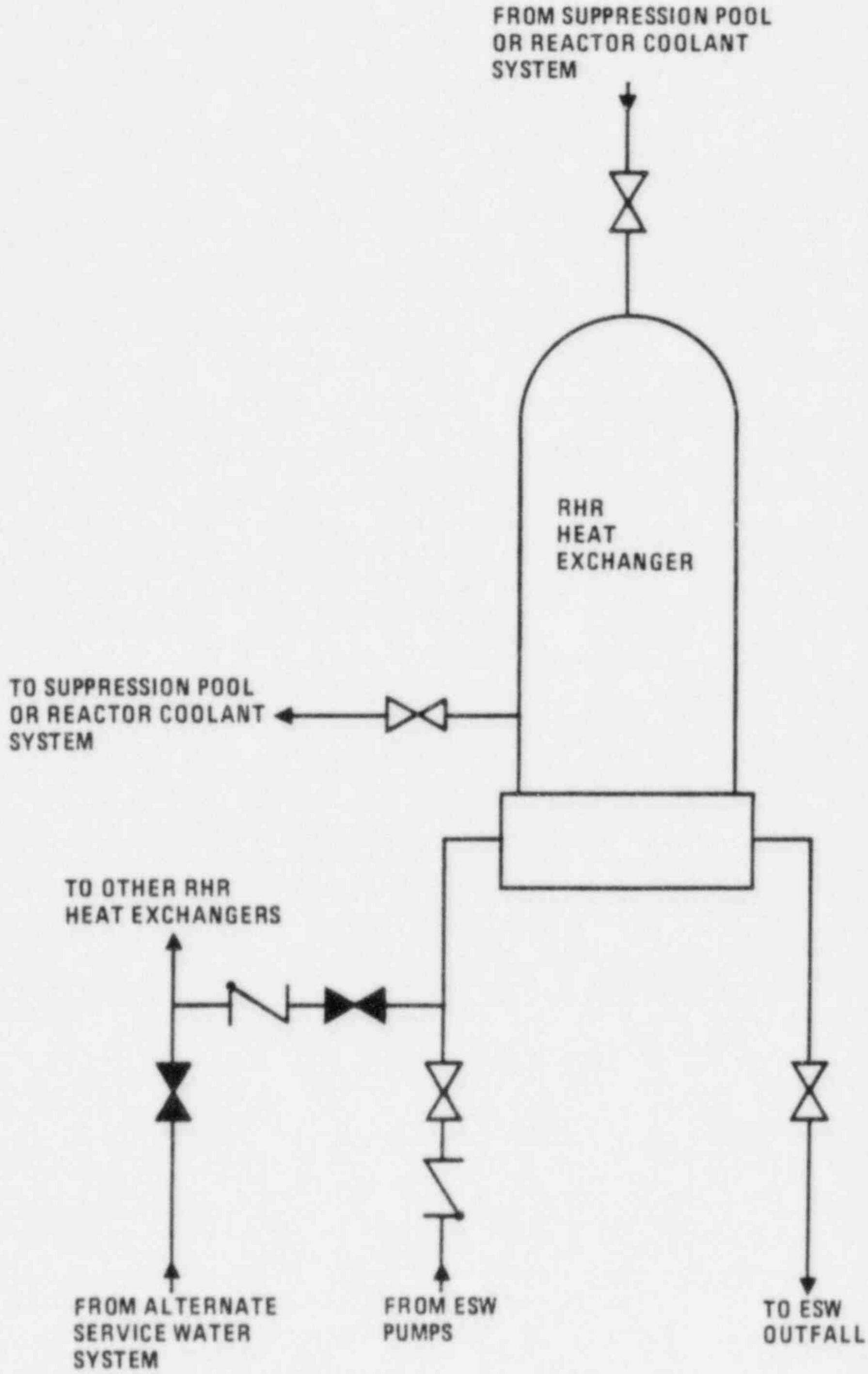


Figure 5.7.1. Connection of Alternate Service Water System to RHR Heat Exchanger.

monitoring) to detect leakage from the RHR heat exchanger into the alternate service water system.

Electric power must be restored to the alternate service water system following loss of offsite power. This can be accomplished by supplying the system from the Class 1E power system (see damage control measure #19) or from an alternate onsite source of Nonclass 1E power (see damage control measure #26).

5.7.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #7

Any electrical interconnections between the Nonclass 1E and the Class 1E AC distribution systems would require particular attention to assure that the Class 1E system is not degraded because of the interconnection. See Section 5.19 for additional information.

5.7.6 Conclusions and Recommendations Regarding Damage Control Measure #7

This damage control measure appears to be technically feasible. Sufficient time is available to permit the manual operations necessary to align an alternate service water system to supply an RHR heat exchanger. This damage control measure would increase the flexibility of BWR decay heat removal systems to bypass disabled components and maintain an effective decay heat removal capability.

5.7.7 Section 5.7 References

1. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

5.8 DAMAGE CONTROL MEASURE #8 - BWR

The purpose of damage control measure #8 is to use the fire water system to supply cooling water to the secondary side of the residual heat removal (RHR) or suppression pool cooling system heat exchangers in the event that the essential service water pumps are disabled.

5.8.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of the service water pumps that supply cooling water to the suppression pool cooling or residual heat removal system heat exchangers (in most BWR plants, these are the same heat exchangers). The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to Class 1E AC buses. The reactor core isolation cooling (RCIC) and the high pressure coolant injection (HPCI) or high pressure core spray (HPCS) systems operate properly to maintain reactor coolant inventory. The suppression pool cooling (or RHR) system is operable, but a complete heat transfer path from the suppression pool to the ultimate heat sink cannot be established.

5.8.2 System Descriptions

5.8.2.1 Suppression Pool Cooling Systems

See Section 5.2.

5.8.2.2 Residual Heat Removal Systems

See Section 5.11.

5.8.2.3 Essential Service Water System

See Section 5.13.

5.8.2.4 Fire Water System

See Section 5.15.

5.8.3 Plant Conditions During Scenario

Following loss of offsite power and main turbine trip, the primary coolant system safety/relief valves will open, as necessary, to provide overpressure protection for the reactor coolant system (RCS). After the initial blowdown to the suppression pool, core decay heat will be transferred to the suppression pool by intermittent safety/relief valve operation and by operation of the turbine-driven reactor core isolation cooling (RCIC) and/or high pressure coolant injection (HPCI) pumps which exhaust to the suppression pool. It has been estimated that a suppression pool will reach 150^{o}F approximately 3.1 hours following loss of offsite power with no suppression pool cooling (Ref. 1). Suppression pool temperature will continue to rise unless service water can be restored to the RHR heat exchangers or other measures can be taken to stabilize suppression pool temperature (e.g., see damage control measure #2).

Nonclass 1E electric motor-driven fire water pumps are unavailable. The diesel engine-driven fire water pump is operable, and if the fire water system has Class 1E motor-driven pumps, these are also operable.

5.8.4 System Features Necessary to Align the Fire Water System to the Suppression Pool Cooling (or RHR) Heat Exchangers

The basic interface requirement to be met by a fire water system is that adequate cooling water flow be provided to the RHR heat exchangers, as described in Section 5.7. If a fire water system can provide the required flow rate to the secondary side of the RHR heat exchangers, it could be considered as a potentially viable backup to the ESW system. A comparison of the basic characteristics of ESW and fire water pumps is presented in Section 5.15. There is a marked disparity between the capacity of these pumps. The capacity of a single ESW pump exceeds the capacity of the entire fire water system. The total flow rate of the fire water system described in Section 5.15 is about 5500 gpm at 280 feet head. This flow rate would only be available if electric power is restored to the motor-driven fire water pumps. This could be accomplished by supplying the pumps from the Class 1E system (see damage control measure #19) or from an alternate onsite source of Nonclass 1E power (see damage control measure #26).

When crossconnected to the RHR heat exchangers, the fire water pumps would likely be operating under runout conditions (e.g., at significantly less than design discharge head) and system flow rate may be on the order of 1.4 to 1.6 times the design flow rate at 280 feet head (e.g., 7700 to 8300 gpm). The system runout flow rate is comparable to the service water requirements of an RHR heat exchanger approximately 2.8 hours after reactor shutdown (see Section 5.7). If the entire fire water system were realigned to provide cooling water to the RHR heat exchangers, it should be possible to stabilize suppression pool temperatures before suppression pool design temperature limits are reached and ultimately to cool the suppression pool when the heat transfer capability of the realigned fire water system exceeds the decay heat generation rate. Use of this fire protection system in this alignment leaves the plant without a water fire fighting capability.

A more balanced system alignment would be to reserve one fire water pump (e.g., the diesel engine-driven pump) for fire protection duties and to align the motor-driven pumps to supply the ESW system. This alignment is described in Section 5.5 and would be capable of supplying 100 percent of required fire water flow but only about 50 percent of the required ESW flow 2.8 hours after shutdown. Without substantial redesign to upgrade its pumping capability, the fire water system cannot provide both fire protection and alternate ESW services. Major fire water system design changes to provide the upgraded pumping capability are described in Section 5.15.

5.8.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #8

See Section 5.15.

5.8.6 Conclusions and Recommendations Regarding Damage Control Measure #8

Adequate RHR cooling may require diversion of the pumping capability of the entire fire water system. Regulatory constraints are likely to prohibit this system alignment. This damage control measure would therefore only be practical if the fire water system is substantially redesigned to upgrade its pumping capability.

5.9 DAMAGE CONTROL MEASURE #9 - PWR

The purpose of damage control measure #9 is to connect safety injection pumps in series to increase the pump discharge pressure and permit coolant to be injected into the reactor vessel at full reactor coolant system pressure.

5.9.1 Sabotage Scenario

Loss of offsite power is assumed to occur coincidentally with sabotage actions that create the need for a core coolant injection capability at design reactor coolant system pressure (e.g., loss of main and auxiliary feedwater). The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.9.2 Safety Injection System Description

The safety injection (SI) system is an element of the emergency core cooling system (ECCS). During normal power operation, the system is in standby. Following a loss of coolant accident (LOCA) the safety injection pumps are automatically started and supply borated water to the reactor coolant system (RCS) from the refueling water storage tank (RWST). When RWST water has been exhausted, the suction of the safety injection pumps can be shifted to the containment sump. Post-LOCA core cooling is continued by recirculating water from the sump back to the reactor vessel. Safety injection system operation may also be required to maintain adequate core coolant inventory following some transients. A summary of PWR high pressure makeup capabilities is presented in Table 5.9.1. A safety injection system for a typical Combustion Engineering PWR is illustrated in Figure 5.9.1 (from Ref. 1).

There are two basic safety injection subsystems providing high pressure safety injection (HPSI) and low pressure safety injection (LPSI) functions. In many plants, the HPSI function is performed by positive displacement or centrifugal charging pumps that are capable of providing makeup to the RCS against full system pressure. Typical capacity of a centrifugal pump that doubles as a HPSI pump is in the 140 to 270 gpm range at 2500 psid (5760 feet).

Three charging pumps are usually provided, and total high pressure injection flow rate at 2500 psid is in the range from 355 to 810 gpm (one of the three charging pumps may be a lower capacity positive displacement pump providing 50 to 100 gpm flow).

Many plants have separate pumps for the HPSI and normal charging functions. In these plants, the HPSI pumps cannot provide makeup against full RCS pressure. These HPSI pumps have a design flow rate of 375 to 425 gpm at a head of 1150 to 1225 psid (2650 to 2822 feet). Two or three HPSI pumps are usually provided, yielding a design HPSI system flow rate of 750 to 1275 gpm. The separate charging pumps are usually positive displacement and are rated at 33 to 98 gpm. Three charging pumps are usually provided, and total charging system flow rate is in the range from 100 to 260 gpm.

Low pressure safety injection pumps have a design flow rate of 2500 to 4200 gpm at a head of 140 to 170 psid (320 to 390 feet). Two or three LPSI pumps are usually provided, yielding a design LPSI system flow rate of 7500 to 12600 gpm. LPSI pumps generally serve a dual role, and are also used in the residual heat removal (RHR) system to provide for normal shutdown cooling of the RCS following cooldown to approximately 350°F and 350 psig by another system (e.g., auxiliary feedwater or main turbine bypass system).

5.9.3 Plant Conditions During Sabotage Scenario

For this discussion, it is assumed that a total loss of feedwater has occurred following loss of the main and auxiliary feedwater systems. The pressurizer safety or power-operated relief valve (PORV) will initially open and then reclose. RCS pressure and temperature will drop immediately following valve closure because, for limited periods of time, there may be more energy removed by the steam generators then is being put into the system by the stored and decay heat of the core. As the steam generators boil off their secondary-side water inventory, this imbalance will shift so that more heat is being added to the RCS than is being removed through the steam generators. RCS temperature and pressure will rise again to the PORV and/or safety valve setpoint (Ref. 2). The steam generators are expected to boil dry in 14 to 43 minutes (Refs. 3 and 4).

Following steam generator dryout, blowdown through the pressurizer safety valves is the only significant heat removal path from the RCS and the primary system will likely remain at high pressure.

Plants without safety injection systems capable of pumping against full RCS pressure probably would not be able to maintain adequate core coolant inventory with the low capacity charging system alone. Under station blackout conditions (e.g., with no makeup to the RCS), it has been estimated that the core will be uncovered to its midplane in approximately two hours (Ref. 5).

5.9.4 System Alignment Necessary to Operate Safety Injection Pumps in Tandem

As noted in Table 5.9.1, the HPSI pumps in many plants cannot provide makeup to the RCS when system pressure is at the pressurizer safety valve setpoint (e.g., approximately 2500 psig), as it might be during some severe post-accident plant conditions. In these plants, tandem operation of safety injection pumps might provide the necessary pumping head to supply coolant to the RCS under these conditions.

General characteristics of HPSI and LPSI pumps are summarized in Table 5.9.2. A HPSI and a LPSI pump operating in tandem could deliver flow at a maximum discharge pressure of about 1400 psig. This combination of pumps cannot pump against design RCS pressure. Two HPSI pumps operating in tandem could deliver near design flow rate with the RCS at approximately 2500 psig (e.g., at the primary system safety valve setpoint).

Because of the wide variety of safety injection system designs, an approach for operating HPSI pumps in tandem will be described only for the system illustrated in Figure 5.9.1. In this Combustion Engineering system, there are two independent, 100 percent capacity HPSI trains. Three HPSI pumps are provided, but only two are aligned for operation. The third pump is essentially a maintenance spare, and it can take the place of either "primary" HPSI pump. The third pump is a third-of-a-kind load, and can be supplied from the electrical division and by the auxiliaries of the HPSI pump it replaces.

Table 5.9.1. PWR High Pressure Coolant Makeup Capabilities

PLANT	CHARGING PUMPS			HIGH PRESSURE SAFETY INJECTION PUMPS		
	NO.	TYPE	CAPACITY (GPM)	NO.	TYPE	GPM @ 2500 psig
Arkansas 1	3	Cent.	270 @ 2500 psig	same as charging pumps		
Arkansas 2	3	P.D.	44	3	Cent.	0
Beaver Valley	3	Cent.	140 @ 2485 psig	same as charging pumps		
Calvert Cliffs 1&2	3	P.D.	44	3	Cent.	0
Cook 1&2	1	P.D.	98 @ 2500 psig	2	Cent.	0
	2	Cent.	150 @ 2500 psig			
Crystal River	3	Cent.	260	same as charging pumps		
Davis Besse	2	Cent.	150 @ 2514 psig	2	Cent.	0
Diablo Canyon	3	P.D.	60	2	Cent.	0
Farley 1&2	3	Cent.	250 @ 2485 psig	same as charging pumps		
Fort Calhoun	3	P.D.	40	3	Cent.	150
Ginna	3	P.D.	60	3	Cent.	0
Indian Point 2&3	3	P.D.	87	3	Cent.	0
Kewaunee	3	P.D.	46	2	Cent.	0
Maine Yankee	3	Cent.	150 @ 2485 psig	same as charging pumps		
McGuire	2	Cent.	150 @ 2514 psig	same as charging pumps		
	1	P.D.	55			
Millstone 2	3	P.D.	44	3	Cent.	0
North Anna	3	Cent.	225 @ 2485 psig	same as charging pumps		
Oconee 1,2&3	3	Cent.	270 @ 2500 psig	same as charging pumps		
Palisades	3	P.D.	40	3	Cent.	0
Point Beach	3	P.D.	60.5	2	Cent.	0
Prairie Island	3	P.D.	60.5	2	Cent.	0
Rancho Seco	3	Cent.	270 @ 2500 psig	same as charging pumps		
Robinson 2	3	P.D.	69	3	Cent.	0
Salem 1&2	2	Cent.	150 @ 2514 psig	same as charging pumps		
	1	P.D.	55			
San Onofre 1	same as S.I. system			2	Cent.	0
San Onofre 2&3	3	P.D.	44	3	Cent.	0

P.D. = Positive Displacement Type Pumps
Cent. = Centrifugal Type Pumps

Table 5.9.1. PWR High Pressure Coolant Makeup Capabilities (continued)

PLANT	CHARGING PUMPS			HIGH PRESSURE SAFETY INJECTION PUMPS		
	NO.	TYPE	CAPACITY (GPM)	NO.	TYPE	GPM @ 2500 psig
Sequoyah 1&2	2	Cent.	150 @ 2514 psig	same as charging pumps		
	1	P.D.	55			
St. Lucie 1&2	3	P.D.	44	3	Cent.	0
Summer 1	3	Cent.	150	same as charging pumps		
Surry 1&2	3	Cent.	150 @ 2485 psig	same as charging pumps		
Three Mile Island 1&2	3	Cent.	270	same as charging pumps		
Trojan	2	Cent.	150 @ 2500 psig	2	Cent.	0
	1	P.D.	98 @ 2500 psig			
Turkey Point	3	P.D.	69	4	Cent.	0
Watts Bar	2	Cent.	150 @ 2514 psig	same as charging pumps		
	1	P.D.	55			
Yankee Rowe	3	P.D.	33	3	Cent.	0
Zion 1&2	2	Cent.	150 @ 2514 psig	same as charging pumps		
	1	P.D.	98			
B-SAR-205 Standard Plant	3	Cent.	306 @ 2815 psig	same as charging pumps		
RESAR-3S Standard Plant	2	Cent.	150 @ 2448 psig	2	Cent.	0

P.D. = Positive Displacement Type Pumps
Cent. = Centrifugal Type Pumps

Table 5.9.2. Comparison of Typical HPSI and LPSI Design Characteristics.

	HPSI Pump	LPSI Pump
Type	Multi-stage Centrifugal	Single-stage Centrifugal
Design Head	1150 to 1225 psid (2650' to 2822')	145 to 165 psid (340' to 370')
Design Flowrate	375 to 425 gpm	2500 to 4200 gpm
Shutoff Head	1495 to 1535 psid (3450' to 3550')	140 to 170 psid (320' to 390')
Design Pressure	1750 to 1950 psig	550 to 650 psig
Max. Suction Pressure	400 to 430 psig	400 to 430 psig
Design Code	ASME III, Class 2	ASME III, Class 2

NOTE: System is shown in lineup for ECCS injection. During normal power operation, this system is in standby.

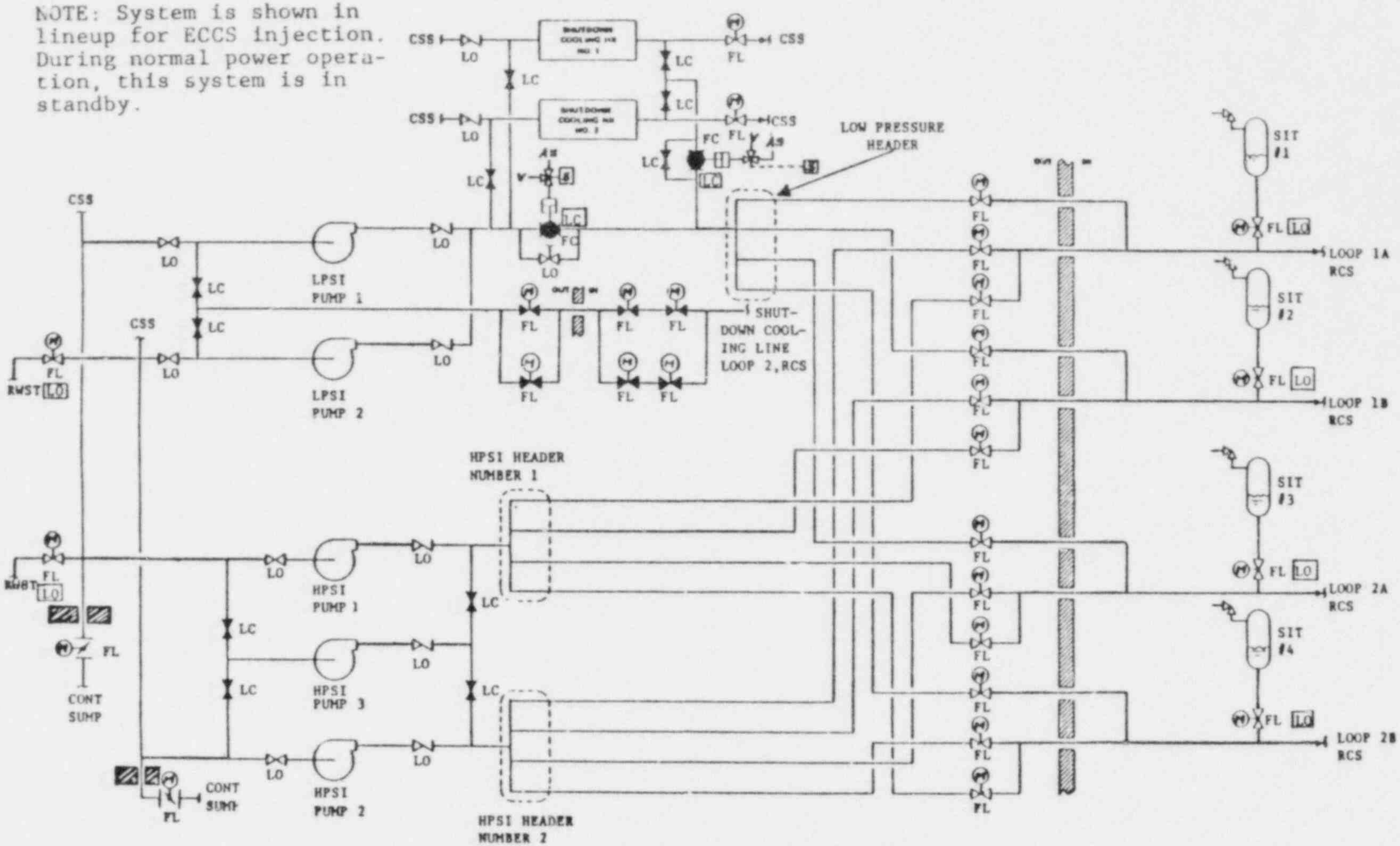


Figure 5.9.1. Typical Combustion Engineering Emergency Core Cooling System (from SAI01379-626LJ)

Adequate makeup can be provided by a single HPSI train. Tandem operation would involve either HPSI pump 1 or 2 being aligned to discharge to the suction side of the third-of-a-kind HPSI pump (pump 3), and that pump being aligned to supply the RCS. The system modifications to permit tandem HPSI pump operation are illustrated in Figure 5.9.2. This arrangement does not require any cross connections that would violate the independence of the two HPSI trains.

As a minimum, the third-of-a-kind pump and its suction-side piping will require replacement. In addition a large number of valves and a great deal of system piping would likely require replacement to accommodate the new system operating pressure capabilities. Design pressure would be the same as the reactor coolant system (approximately 2500 psig).

This damage control measure does not apply to PWR plants which use charging pumps for the high pressure safety injection function (see Table 5.9.1). These plants can provide considerable makeup with RCS pressure at the pressurizer safety valve setpoint.

5.9.5 Technical and Regulatory Impediments to Damage Control Measure #9

Without replacing a significant portion of the HPSI system with components designed to accommodate the higher operating pressure, there are significant technical and regulatory impediments to implementing this damage control measure. These deal primarily with the stress and pressure conditions that would likely exist in a large portion of the safety injection system when HPSI pumps are run in tandem, and with the operability of active components under these conditions.

Section III of the ASME Boiler and Pressure Vessel Code (Ref. 6) establishes rules intended to ensure the integrity of the pressure retaining boundary of safety class components. The ASME Code defines stress and pressure limits for four service limits of components design (e.g., Levels A, B, C, and D). Table 5.9.3 summarizes the effect on a component of stress at each of the four service limits.

Table 5.9.3. Definition of Service Limits Specified in The ASME Boiler and Pressure Vessel Code.

Service Limits	Description
Level A	These are limits which must be satisfied for all loadings identified in the design specifications to which the component or support may be subjected in the performance of its service function.
Level B	These are limits which must be satisfied for all loadings identified in the design specifications for which these service limits are designated. The component or support must withstand these loadings without damage requiring repair.
Level C	These sets of limits permit large deformations in areas of structural discontinuity. The occurrence of stress to Level C limits may necessitate the removal of the component from service for inspection or repair of damage to the component or support.
Level D	These sets of limits permit gross general deformations with some consequent loss of dimensional stability and damage requiring repair, which may require removal of the component from service.

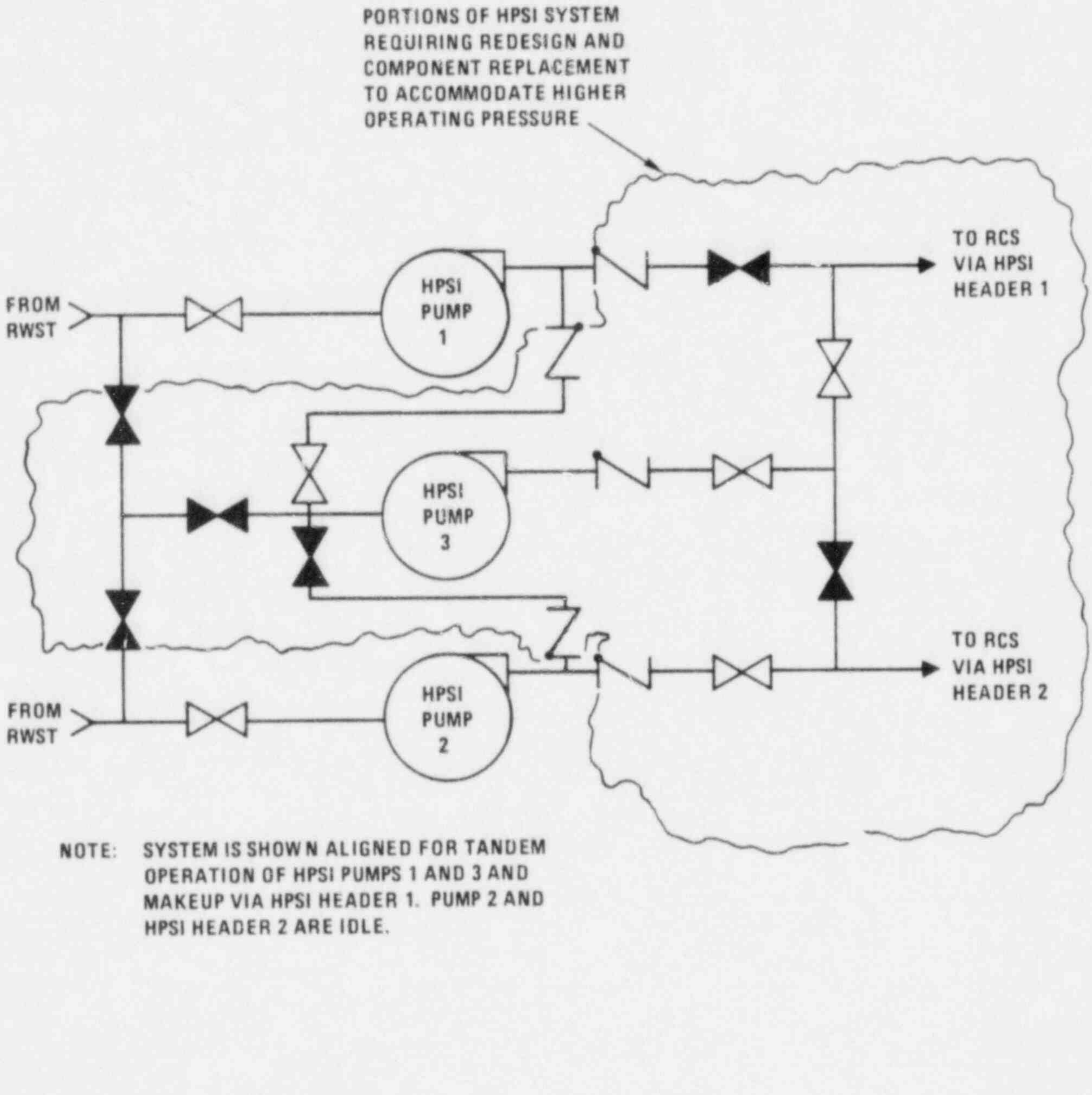


Figure 5.9.2. Modifications to Operate HPSI Pumps in Tandem.

The majority of the components in the safety injection system are designed as ASME Code Class 2 components, and are subject to subsection NC of the ASME Code. Applicable stress and pressure limits are summarized in Table 5.9.4. These limits do not assure the operability of components in which mechanical motion is required.

The safety injection pumps and the valves that must move during the course of accomplishing the system safety function are considered as active pumps and valves. The NRC specifies the following design limits for active ASME Code Class 2 pumps in Regulatory Guide 1.48 (Ref. 7).

> "The primary membrane stress should not exceed the allowable stress value S, and the sum of the primary membrane and the primary bending stresses should not be exceeded by more than 50 percent of S when the component is subjected to either: (1) concurrent loadings associated with either the normal plant condition or the upset plant condition and the vibratory motion of 50 percent of the SSE, or (2) loadings associated with the emergency plant condition, or (3) concurrent loadings associated with the normal plant conditions, the vibratory motion of the SSE, and the dynamic system loadings associated with the faulted plant condition."

These limits correspond to Level A Service Limits in Table 5.9.4. This is the most restrictive service level from a design standpoint, and its application is a measure of the level of conservatism required by the NRC in the design of the safety injection system.

Realigning the safety injection pumps as illustrated in Figure 5.9.2 would expose a significant portion of the safety injection system to pressures up to approximately 2500 psig. This exceeds the HPSI pump design pressure listed in Table 5.9.2 by a factor of 1.28 to 1.43. From Table 5.9.4 it can be seen that this maximum pressure (P_{max}) falls between Level C and D Service Limits. The effect of stress at these levels is briefly outlined in Table 5.9.3. Although stress increases for the modified safety injection system have not been determined, it is likely that the stress would also be well beyond Level A Service Limits.

Table 5.9.4. ASME Stress and Pressure Limits for Design and Service Loadings(1).

Service Limit	Valves and Centrifugal Pumps		Piping	
	Stress Limit(2)	P_{max} (3)	Stress Limit(2)	P_{max} (3)
Level A	$\sigma_m \leq S$ $(\sigma_m \text{ or } \sigma_L) + \sigma_b \leq 1.5S$	1.0	1.0 Sh	1.0
Level B	$\sigma_m \leq 1.1S$ $(\sigma_m \text{ or } \sigma_L) + \sigma_b \leq 1.65S$	1.1	1.2 Sh	1.1
Level C	$\sigma_m \leq 1.5S$ $(\sigma_m \text{ or } \sigma_L) + \sigma_b \leq 1.8S$	1.2	1.8 Sh	1.5
Level D	$\sigma_m \leq 2.0S$ $(\sigma_m \text{ or } \sigma_L) + \sigma_b \leq 2.4S$	1.5	2.4 Sh	2.0

Notes: (1) From ASME B & PV Code, Section III, Division 1, Subsection NC, Paragraphs NC-3416 (pumps), NC-3521 (valves) and NC 3611.2 (piping),

(2) S = allowable stress

σ_m = general or primary membrane stress

σ_L = local membrane stress

σ_b = bending stress

Sh = basic material allowable stress at maximum temperature

(3) The maximum pressure shall not exceed the tabulated factors listed under P_{max} times the design pressure. The design pressure of a component is the maximum difference in pressure between the inside and outside of an item, or between any two chambers of a combination unit, which exists under the most severe loadings for which the Level A Service Limits are applicable.

With the possible exception of suction side piping and valves, and the HPSI pump suction casing, the pressure boundary of the safety injection system may remain intact at the elevated pressures created by the modified system alignment. Operability of active components under these conditions would remain to be demonstrated. The NRC requires that assurance of operability under all design loading combinations be provided in any of the following measures (Ref. 7):

- In situ testing (e.g., preoperational testing after the component is installed in the plant).
- Full-scale prototype testing.
- Detailed stress and deformation analyses (includes experimental stress and deformation analyses).

In the performance of tests or analyses to demonstrate operability, the structural interaction of the entire assembly (e.g., valve-operator and pump-motor assembly) should be considered.

5.9.6 Conclusions and Recommendaions Regarding Damage Control Measure #9

This damage control measure cannot be implemented without wholesale redesign and requalification of the HPSI system to accommodate higher operating pressures and to retain the current level of conservatism in HPSI system design. If this damage control measure were implemented in selected PWRs, it might reduce the dependence on the auxiliary feedwater system for RCS pressure reduction following feedwater transients and small-break LOCAs. Alternatives to this damage control measure include the following:

- Installing higher capacity HPSI pumps capable of providing adequate makeup at design RCS pressure.
- Installing a power-operated relief valve (PORV) capability adequate for reliably depressurizing the RCS to the point where an existing HPSI system can provide adequate core coolant inventory control. This system would be analogous to the automatic depressurization system in a BWR. A pressure suppression volume within the containment would also be required to collect the blowdown from the PORVs.

5.9.7 Section 5.9 References

1. Lobner, P., et al., "The Pressurized Water Reactor - A Review of a Typical Combustion Engineering PWR Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

2. NUREG-0560, "Staff Report on Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock and Wilcox Company," U. S. Nuclear Regulatory Commission, May 1979.

3. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Westinghouse - Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

4. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

6. ASME Boiler and Pressure Vessel Code, Section III, Subsection NC, "Class 2 Components," American Society of Mechanical Engineers.

7. USNRC Regulatory Guide 1.48, "Design Limits and Loading Combinations for Seismic Category 1 Fluid System Components."

5.10 DAMAGE CONTROL MEASURE #10 - BWR

The purpose of damage control measure #10 is to provide post-accident reactor coolant makeup using the Control Rod Drive Hydraulic System (CRDHS) in the event other high pressure injection systems are inoperable because of sabotage actions.

5.10.1 Sabotage Scenario

Loss of offsite power is assumed to occur coincidentally with successful sabotage of the BWR high pressure injection systems which may include the Reactor Core Isolation Cooling (RCIC) System, High Pressure Core Spray (HPCS) System, High Pressure Coolant Injection (HPCI) System, or the Feedwater Coolant Injection (FWCI) System. Availability of any one of these systems would negate the need for considering this damage control measure. The main turbine generator trips on loss of load. A reactor scram occurs and the control rods are inserted by the control rod drive hydraulic system. The emergency diesel generators operate to supply AC power to the Class 1E buses.

5.10.2 System Descriptions

5.10.2.1 Control Rod Drive Hydraulic System

The control rod drive hydraulic system (CRDHS) supplies pressurized water to operate and cool the control rod drive mechanisms. The water used for these functions is ultimately discharged into the reactor vessel and provides a backup source of water in an emergency. A typical CRDHS is illustrated in Figure 5.10.1 (from Ref. 1).

The CRDHS has two pumps, each rated at 100 percent capacity. Maximum flow rate for each pump at operating reactor pressure (e.g., 1000 psig) is about 104 gpm (Ref. 2). Shutoff head for the CRDHS pumps is approximately 1750 psig. These pumps are usually considered as nonsafety loads, but may be powered from the Class 1E electrical system. Water for the CRDHS is supplied from the condensate storage tank.

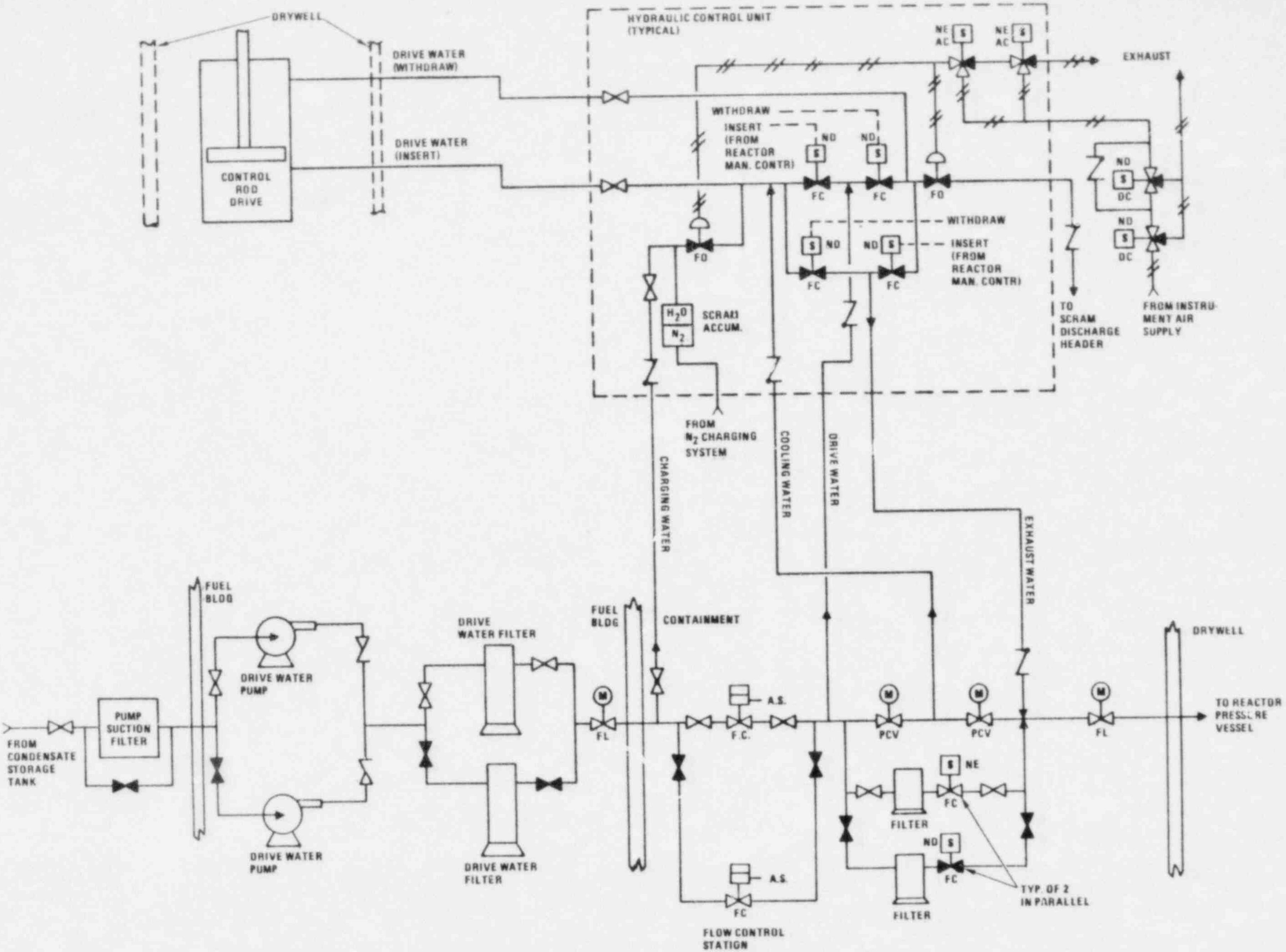


Figure 5.10.1. Typical Control Rod Drive Hydraulic System (from SAI01379-627LJ).

Control valves distribute the high pressure water from the CRDHS pumps as follows (refer to Figure 5.10.1):

- Drive Water: A flow rate of approximately 4 gpm is required to insert a control rod, and 2 gpm is required to withdraw a control rod. An individual control rod or gang of control rods (e.g., 3 to 4 rods) may be operated at one time. Maximum drive water flow rate would be 12 to 16 gpm. A pressure control valve downstream of the drive water supply line to the control rod hydraulic control units maintains drive water pressure about 260 psi above reactor pressure.

- Cooling Water: A flow rate of 0.22 to 0.35 gpm per drive mechanism is required for seal cooling. For a typical BWR/6 with 117 control rods, a cooling water flow rate of 26 to 41 gpm would be required. Cooling water can be interrupted for short periods without damaging the drive, however, extended loss of cooling water flow will shorten seal life. A pressure control valve downstream of the cooling water supply line to the control rod hydraulic control units maintains cooling water pressure about 20 psi above reactor pressure. This low pressure difference (with respect to reactor pressure), allows cooling water flow to be supplied via the drive water "insert" lines without unlatching the drive mechanisms. Water not required for drive cooling passes through the pressure control valve to the reactor vessel via the control rod hydraulic return line.

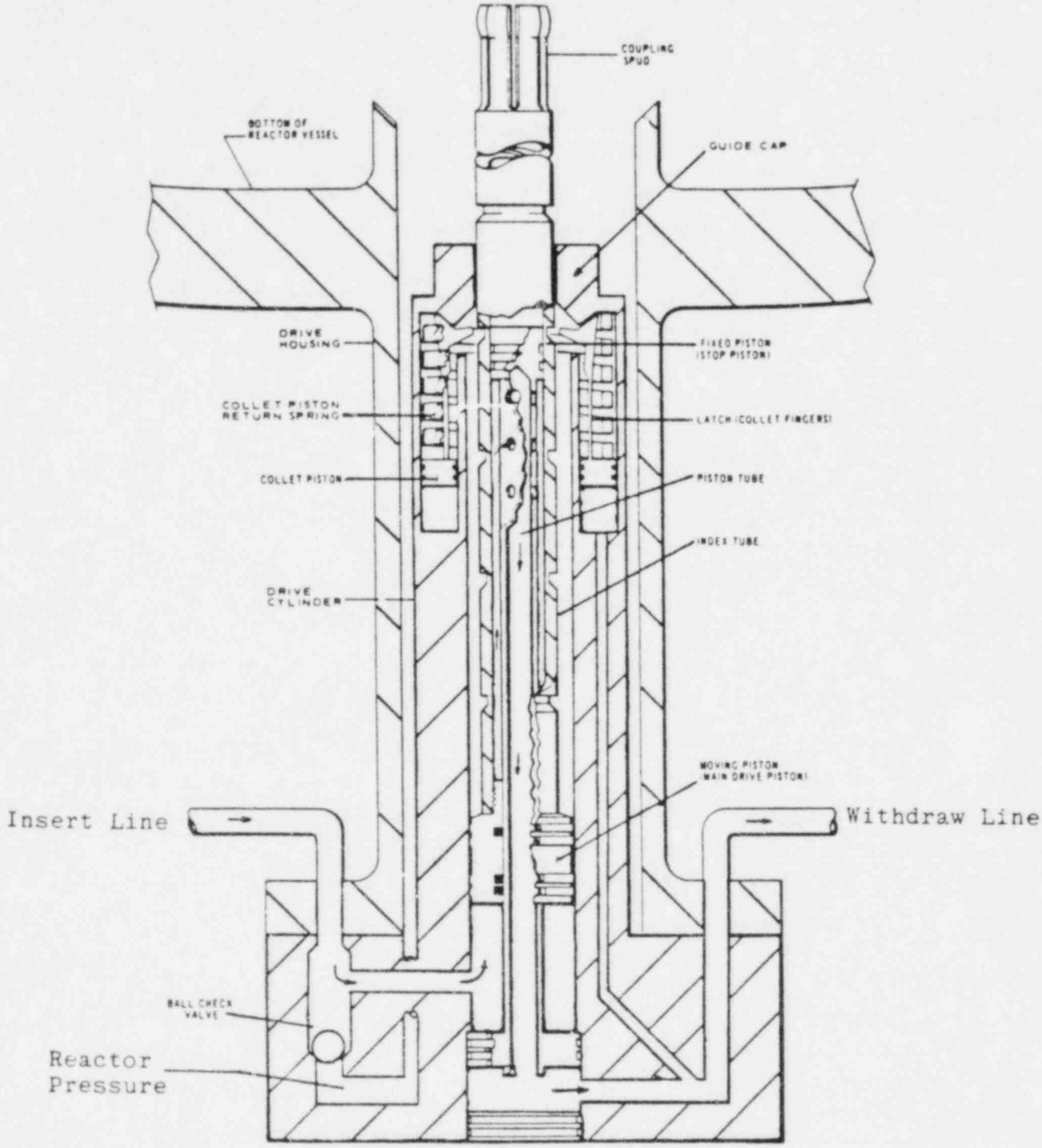
- Charging Water: Scram accumulator pressure is established by the discharge pressure of the CRDHS pumps. During normal operation, there is no flow in the charging water line. During a scram, the "withdraw" side of each drive mechanism is vented to the scram discharge volume (or scram dump tank in early BWRs) which is at atmospheric pressure. The scram accumulators discharge to the drive water "insert" lines and cause rapid rod insertion. The resulting pressure decrease in the charging water header allows the CRDHS pump to achieve a maximum (runout) flow rate of approximately 200 gpm into the charging header, and to the control rod drive mechanisms. The flow sensing system upstream of the accumulator charging header detects high flow and closes the flow control valve downstream of the charging header. This action maintains increased flow in the charging header. After the scram is complete, the control rod drive seal leakage (from "insert" side to the "withdraw" side of the drive mechanism piston) continues to flow to the scram discharge volume until discharge volume pressure equals the reactor pressure. Charging water flow also recharges the scram accumulators. With the accumulators recharged and the scram discharge volume at reactor pressure, control rod drive seal leakage is then directed to the reactor vessel and serves as an additional source of coolant makeup.

- Exhaust Water: Water vented from the drive mechanisms during control rod operation is directed to the reactor vessel via the control rod hydraulic return line.

Because of control rod drive hydraulic return line nozzle cracking problems, General Electric has recommended the removal of the CRD return line piping and capping of the return nozzle (Ref. 3). Testing performed on an operating reactor revealed that, with the return line blocked, rod drive water is returned to the reactor vessel through a reverse flow path involving the insert exhaust directional control valves of nonactuated CRD hydraulic control units. Analysis has predicted that the CRD pumps can deliver close to their rated flow through the charging water and cooling water headers when the drives are scrammed (Ref. 3). The NRC has approved this approach, subject to the demonstration of an adequate high pressure coolant makeup capability for the CRDHS (Ref. 4). The recommended coolant makeup capability is that which matches the coolant boiloff rate approximately 40 minutes after shutdown (based on the actual CRDHS makeup capability observed following the Browns Ferry fire). Some plants have been able to demonstrate greater than 180 gpm makeup flow rate with both CRDHS pumps running.

Once a control rod has been moved to a desired position in the core by the CRDHS, a collet assembly latches with the drive mechanism index tube (connected to the control rod) to prevent the control rod from accidentally moving downward (see Figure 5.10.2, from Ref. 2). In the latched position, fingers on a collet piston engage a locking groove on the index tube. A pressure of about 180 psi above reactor pressure must be applied to the collet piston to spread the latch fingers out so they do not engage a locking groove. This is accomplished when drive water (e.g., 260 psi above reactor pressure) is supplied to the drive mechanism. Cooling water (e.g., 20 psi above reactor pressure) cannot unlatch a drive mechanism. Downward force on the index tube holds the latch fingers in place. Once inserted following a scram, the latches can hold the control rods in place without requiring continued hydraulic pressure from the CRDHS or scram accumulators.

There are variations to the CRDHS system illustrated in Figure 5.10.1. Some early BWRs such as Dresden 2 can direct CRDHS pump flow to a reactor vessel head spray that is used to maintain acceptable reactor vessel head temperatures during a plant cooldown (Ref. 5). Some other plants such as Monticello have a CRDHS pump test bypass line capable of aligning the pump discharge directly to the reactor vessel via the normal control rod drive hydraulic return line



Note: Arrows show water flow during scram

Figure 5.10.2. BWR Control Rod Drive Unit.

(Ref. 6). A CRDHS with both of these capabilities is illustrated in Figure 5.10.3 (from Ref. 7). Other aspects of the operation of these CRDHS designs are similar to the previously described system.

5.10.2.2 Reactor Core Isolation Cooling System

The RCIC system is intended to provide adequate core cooling when the reactor vessel is isolated from the main condenser (e.g., the main steam isolation valves are closed) and normal feedwater is lost. In this condition, the reactor coolant system will be at high pressure with energy being removed through the safety valves to the suppression pool. A description of the RCIC system is provided in Sections 5.6 and 5.25.

5.10.3 Plant Conditions During Sabotage Scenario

The reactor would have scrammed for any of the following reasons following loss of offsite power: turbine stop valve closure, turbine control valve fast closure, high reactor pressure or low reactor water level. A low reactor water level scram typically occurs at "Level 3" which is approximately 14 feet above the top of the core. If the CRDHS pumps are nonsafety loads supplied from the the Class 1E system, they would not automatically be reenergized when the diesel generators come on line. The control room operator could restart the CRDHS pumps manually. If the CRDHS pumps are supplied only from the Nonclass 1E AC system, electric power would not be available to restart the pumps.

High pressure injection systems are normally actuated when reactor water level drops to "Level 2," which is approximately 10 feet above the top of the core. With high pressure injection systems unavailable, reactor water level will continue to drop. When "Level 1" (about 1.5 feet about the top of the core) is reached, the Automatic Depressurization System (ADS) should be actuated and the low pressure injection systems placed in operation. For non-LOCA conditions, such as this postulated sabotage scenario, manual actuation of the ADS would be required because the coincidence logic of the ADS (e.g., low reactor water level and high drywell pressure) would not be satisfied.

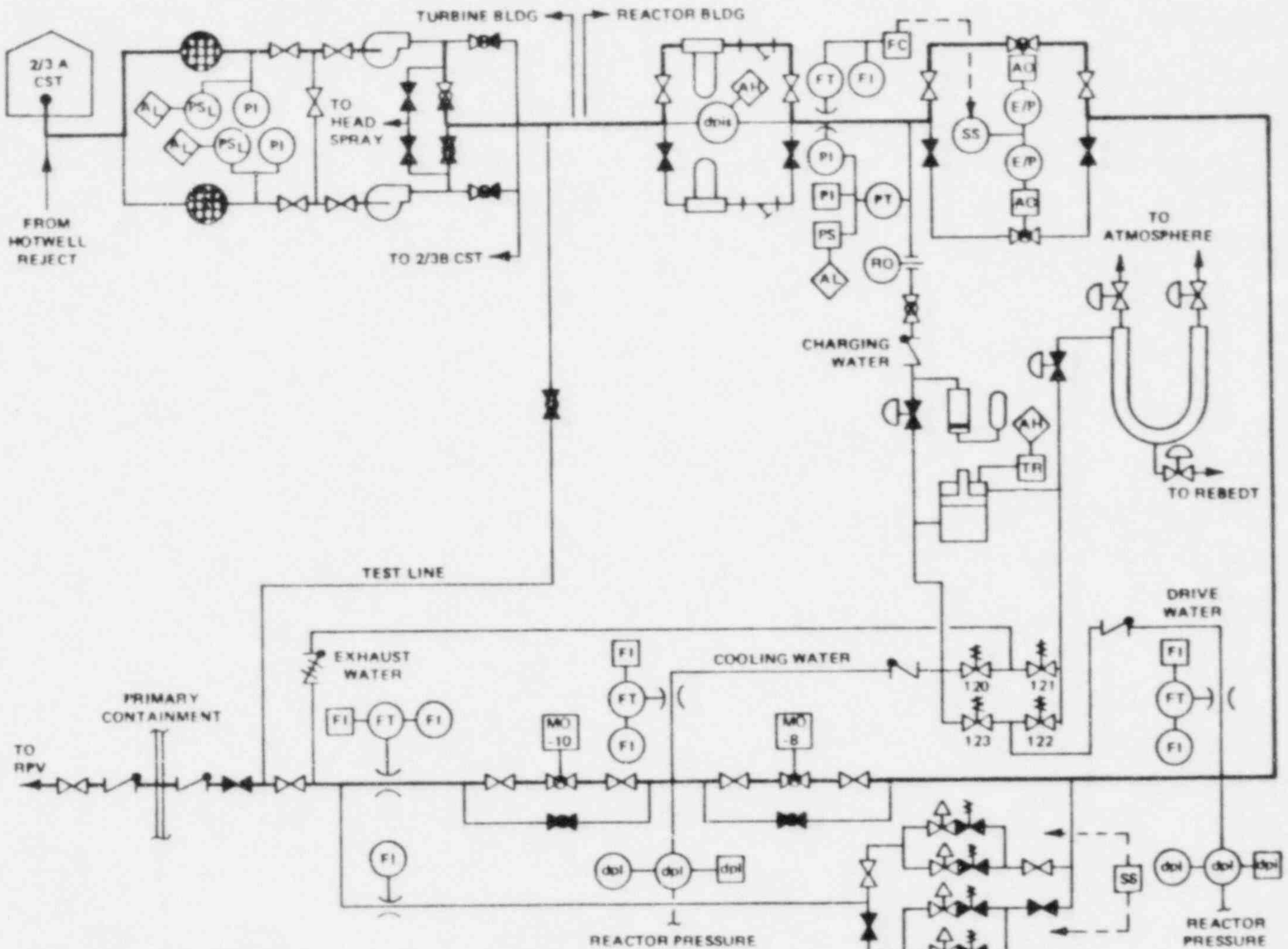


Figure 5.10.3. Control Rod Drive Hydraulic System with Valving for Reactor Vessel Head Spray and Pump Test (from NUREG-0626).

5.10.4 System Alignment Necessary To Use The CRDHS as a Substitute for the RCIC System

A comparison of RCIC and CRDHS pumps is presented in Table 5.10.1. The combined capacity of the two CRDHS pumps provide only about 30 percent of the flow rate of an RCIC pump at normal reactor pressure. The CRDHS would not likely be able to provide adequate coolant makeup for the full spectrum of events which the RCIC system is designed to mitigate. The value of the CRDHS as a high pressure reactor coolant makeup system in past events at Browns Ferry and Oyster Creek has been noted (Refs. 7 and 8). Coolant makeup contributions from the CRDHS have been considered in recent BWR feedwater transient and small-break LOCA analysis (Ref. 7), although makeup rate was assumed to be only 7.5 pounds/sec (about 60 gpm). Traditionally, no credit has been taken for the coolant makeup capability of the CRDHS in accident analysis in support of plant licensing. Generic emergency procedures prepared by the BWR Owner's Group (Ref. 9) do, however, include the CRDHS as a potential system for high pressure coolant injection.

In actual practice, the existing CRDHS system design appears to provide a makeup capability following reactor scram at or near the rated capacity of the CRDHS pumps. Further upgrading would be necessary for this system to fully replace the injection capability of the RCIC system. Some enhancement of injection capability may be realized by providing a head spray capability similar to the system illustrated in Figure 5.10.2. There would be reduced head losses using this injection path, and injection flow rate may increase to approximately 200 gpm at normal reactor pressure, with both pumps running. This small increase would be at the expense of drive mechanism cooling.

Further improvement of the CRDHS coolant makeup capability would require the installation of higher capacity pumps and a wide variety of other system design changes. Potentially affected areas include system line sizes, control rod drive seal design, CRD flow control subsystem operation, CRD filter design and pump cooling requirements. In short, a wholesale redesign of the CRDHS might be required. Impact of these changes on normal CRDHS operation would have to be evaluated in detail.

Table 5.10.1. Comparison of RCIC and Control Rod Drive Pump Characteristics

	RCIC Pump	Control Rod Drive Pump
Type	Multi-Stage Centrifugal	Multi-Stage Centrifugal
Drive	Steam Turbine	Electric Motor
Flowrate (@ Pump Head)	700 gpm (@ 1120 psid)	104 gpm (@ 1000 psid)
Water Source	Condensate Storage Tank or Suppression Pool	Condensate Storage Tank

5.10.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #10

There are no technical impediments to the use of the CRDHS for reactor coolant makeup in its present form. Major system redesign would likely be be required to provide a makeup capability comparable to the RCIC system. Such redesign may introduce a number of technical concerns associated with normal CRDHS operation.

No significant regulatory concerns have been identified other than the control rod drive hydraulic return line nozzle cracking generic problem discussed previously. It is likely, however, that a significant redesign of the CRDHS would open a renewed licensing review of this system.

5.10.6 Conclusions and Recommendations Regarding Damage Control Measure #10

The CRDHS has been recognized and utilized as a high pressure reactor coolant makeup system in its present configuration. This high pressure coolant makeup capability is a normal design feature of the CRDHS. This coolant makeup capability does not match the capability of the RCIC system. Therefore, the CRDHS would not be expected to provide adequate coolant inventory control for as broad a spectrum of accidents as the RCIC. Significantly upgrading the makeup capability of the CRDHS could impact normal reactivity control operations of the system, and would require further investigation to determine technical feasibility.

5.10.7 Section 5.10 References

1. Lobner, P., et al., "The Boiling Water Reactor - A Review of a Typical General Electric BWR/6 Plant," SAI01379-627LJ, Science Applications, Inc., March 23, 1979.

2. "238 Nuclear Steam Supply System - GESSAR," Section 4.2.3.2.2.3, Docket STN-50550, General Electric Company.

3. "Control Rod Drive Hydraulic Return Line Modification," BWR Services Information Letter SIL No. 200, Supplement 2, General Electric Company, November 18, 1977.

4. NUREG-0619, Rev. 1, "BWR Feedwater Nozzle and Control Rod Drive Return Line Cracking, Resolution of Generic Technical Activity A-10," U. S. Nuclear Regulatory Commission, November 1980.

5. NEDO-10128, "BWR Training Center - General Description of the Dresden II Boiling Water Reactor," General Electric Company, April 1973.

6. "Monticello Nuclear Generating Plant, Unit 1, Final Safety Analysis Report," Section 5.3.2, Docket 50263.

7. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

8. Scott, R. L., "Browns Ferry Nuclear Power Plant Fire on Mar. 22, 1975," Nuclear Safety, Vol. 17, No. 5, September-October 1976.

9. "Emergency Procedure Guidelines - BWR 1 Through 6," Revision 1, BWR Owner's Group, January 30, 1981.

5.11 DAMAGE CONTROL MEASURE #11 - BWR

The purpose of damage control measure #11 is to provide reactor coolant makeup using low pressure injection systems in the event that high pressure injection systems have been disabled by sabotage action.

5.11.1 Sabotage Scenario

Loss of offsite power is assumed to occur coincidentally with the successful sabotage of the reactor coolant high pressure injection systems which will include one or more of the following: reactor core isolation cooling (RCIC) system, high pressure core spray (HPCS) system, high pressure coolant injection (HPCI) system, the feedwater coolant injection (FWCI) system and the control rod drive hydraulic system (CRDHS). The main turbine generator trips on loss of load. The emergency diesel generators operate and supply power to the Class 1E buses. Systems for depressurizing the reactor coolant system and for coolant injection of low pressure are operable.

5.11.2 BWR Low Pressure Core Cooling Systems

Table 5.11.1 summarizes the BWR systems provided for a variety of functions, including core coolant injection at low pressure and shutdown core cooling. The low pressure core spray (LPCS) system, residual heat removal (RHR) system and the low pressure coolant injection (LPCI) system are discussed in more detail in this section.

5.11.2.1 Low Pressure Core Spray (LPCS) System

All BWRs have an LPCS system. This system provides for core coolant inventory control when the plant is at low pressure following: (1) a large LOCA, (2) plant cooldown by another system, or (3) rapid plant depressurization with the automatic depressurization system (ADS).

Table 5.11.1. Summary of BWR High and Low Pressure Coolant Injection, Shutdown Cooling and Containment Cooling Capabilities

	BWR Type	Systems for Core Coolant Injection at High Pressure(1)					Systems for Core Coolant Injection at Low Pressure and Other Functions(1)				Systems Performing Only a Shutdown Cooling Function(1)		Systems for Containment Spray and Suppression Pool Cooling(1)	
		RCIC	HPCI	HPCS	FWCI(2)	CRDHS(2)	LPCS	LPCI	RHR-M1	RHR-M2	RHR-S	Isolation Condenser	CS-S	CS-M
Dresden 1	1	-	(4)	-	-	X	X	-	-	-	X	X	X	-
Humboldt Bay	1	-	-	-	X	X	X	X	-	-	X	X	X	-
Big Rock Point	1	-	-	-	-	X	(5)	-	-	-	X	X	-	(7)
Oyster Creek	2	-	-	-	-	X	X	-	-	-	X	X	X	-
Nine Mile Point	2	-	-	-	X	X	X	-	-	-	X	X	X	-
Millstone 1	3	-	-	-	X	X	X	X	-	-	X	X	-	(8)
Dresden 2 & 3	3	-	X	-	-	X	X	X	-	-	X	X	-	(8)
Pilgrim	3	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Monticello	3	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Quad Cities 1 & 2	3	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Hatch 1 & 2	4	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Browns Ferry 1, 2 & 3	4	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Vermont Yankee	4	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Peach Bottom 2 & 3	4	X	X	-	-	X	X	-	X	-	-	-	-	(9)
Cooper	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Duane Arnold	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Fitzpatrick	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Brunswick 1 & 2	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Shoreham	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Fermi 2	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
Susquehanna 1 & 2	4	(3)	X	-	-	X	X	-	-	X	-	-	-	(9)
LaSalle 1 & 2	5	(3)	-	X	-	X	(6)	-	-	X	-	-	-	(9)
Zimmer	5	(3)	-	X	-	X	(6)	-	-	X	-	-	-	(9)
Hanford 2	5	(3)	-	X	-	X	(6)	-	-	X	-	-	-	(9)
Grand Gulf 1 & 2	6	(3)	-	X	-	X	(6)	-	--	X	-	-	-	(9)
Other BWR/5 & /6		(3)	-	X	-	X	(6)	-	-	X	-	-	-	(9)

Table 5.11.1. Summary of BWR High and Low Pressure Coolant Injection, Shutdown Cooling and Containment Cooling Capabilities (continued)

Notes:

(1) RCIC = reactor core isolation cooling system
HPCI = high pressure coolant injection system
HPCS = high pressure core spray system
FWCI = feedwater coolant injection system
CRDHS = control rod drive hydraulic system
LPCS = low pressure core spray system
LPCI = low pressure coolant injection system (single mode system)
RHR-M1 = multi-mode RHR system performing LPCI, shutdown cooling, suppression pool cooling and containment spray functions
RHR-M2 = same as RHR-M1 plus steam condensing operation with RCIC
RHR-S = single-mode residual heat removal system
CS-M = containment spray, which is an operating mode of some other multi-mode system
CS-S = single-mode containment spray system

(2) Non-engineered safety feature system except Millstone 1 FWCI

(3) Injection plus steam-condensing modes of operation

(4) Being installed

(5) Also performs suppression pool cooling function

(6) Only a single 100% capacity LPCS pump. Other plants typically have two 100% capacity LPCS trains

(7) Containment/suppression pool cooling is an operating mode of LPCS system

(8) Containment/suppression pool cooling is an operating mode of the LPCI system

(9) Containment/suppression pool cooling is an operating mode of the multi-mode RHR system (RHR-M1 or RHR-M2)

There are two basic LPCS system configuations. BWR/2 through BWR/4 plants typically have two 100 percent capacity LPCS loops. Each loop has either one 100 percent pump or two 50 percent pumps, and can supply water to the reactor vessel from the suppression pool or the condensate storage tanks. A system of this type is illustrated in Figure 5.11.1 (from Ref. 1). BWR/5 and BWR/6 plants have a single LPCS loop, with a single 100 percent capacity pump. This system supplies water to the reactor vessel from the suppression pool, as illustrated in Figure 5.11.2.

BWR/1 plants have a variety of other LPCS system configurations. Dresden 1 uses three LPCS pumps to supply water directly to each fuel bundle. Big Rock Point uses two core spray pumps and two fire water pumps to feed a ring sparger and a top head nozzle. Humboldt Bay has two core spray pumps delivering water through a single spray ring.

During normal power operation, the LPCS is in standby and the discharge valves are closed. The LPCS system is automatically actuated by low reactor vessel water level (e.g., Level 1, or about 1.5 feet above the top of the core), or high drywell pressure. The discharge valves automatically open when reactor coolant system (RCS) pressure drops below an interlock setpoint.

5.11.2.2 Residual Heat Removal (RHR) System

The basic RHR system function is to provide for removal of core decay heat after reactor shutdown and cooldown to 280^{o}-350^{o}F by another heat removal system (e.g., turbine bypass system, isolation condenser system or RCIC system). All BWRs have an RHR system, however, the design details and functional capabilities vary significantly among plants.

There are three basic RHR system configurations. Earlier-vintage BWRs, including BWR/1, BWR/2 and some BWR/3 plants, typically have a single-mode RHR system. Its only function is core shutdown heat removal. When the entire system is in operation, it is rated at 100 percent of the required cooling capability. RHR system operation is manually-initiated when RCS temperature and pressure limits have been satisfied. Single-mode RHR systems are illustrated in Figure 5.11.3 for a BWR/ plant and in Figure 5.11.4 for a BWR/2 or BWR/3 plant. In

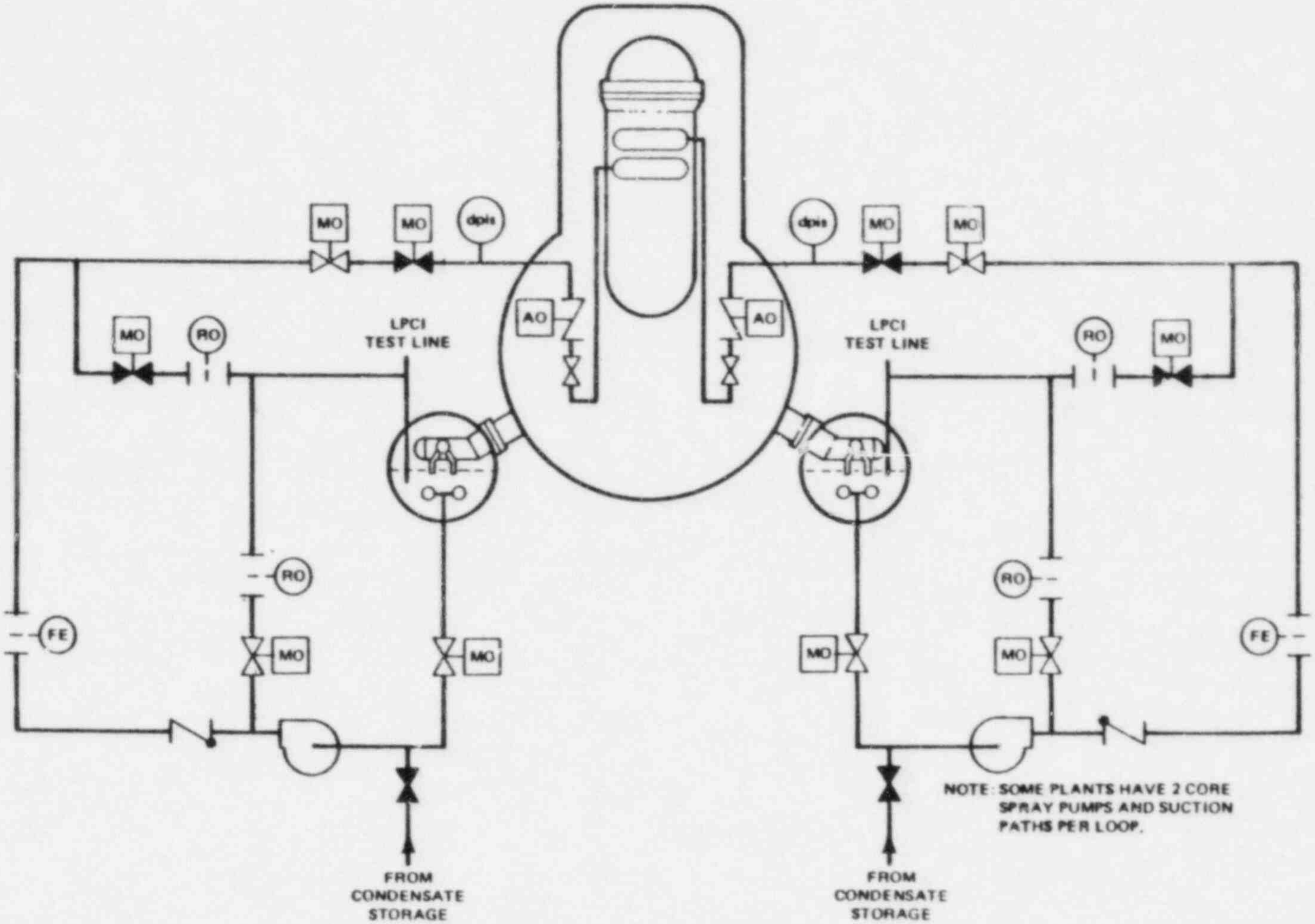


Figure 5.11.1. BWR/2 to BWR/4 Low Pressure Core Spray System (from NUREG-0626)

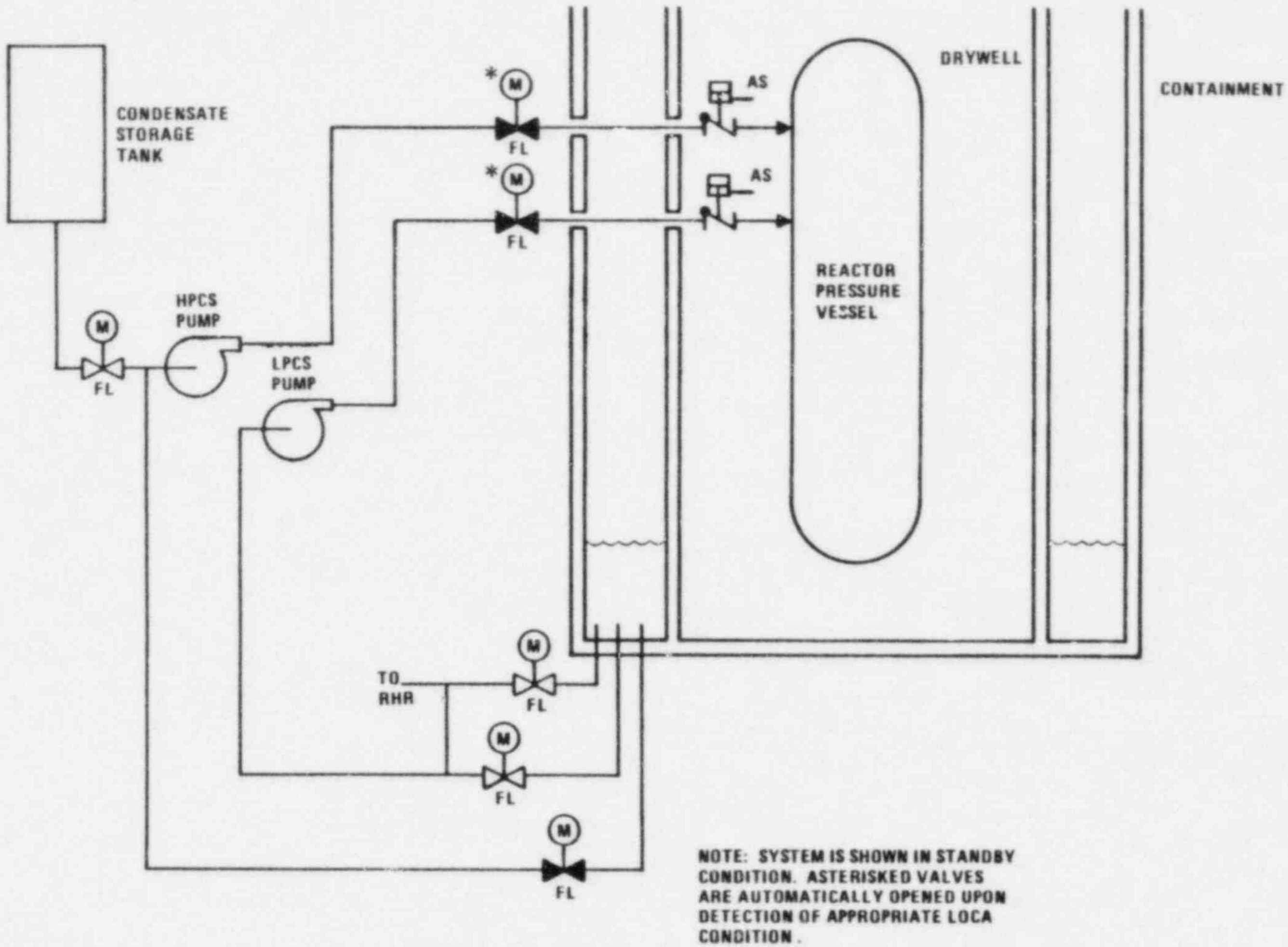


Figure 5.11.2. BWR/5 or BWR/6 Core Spray System

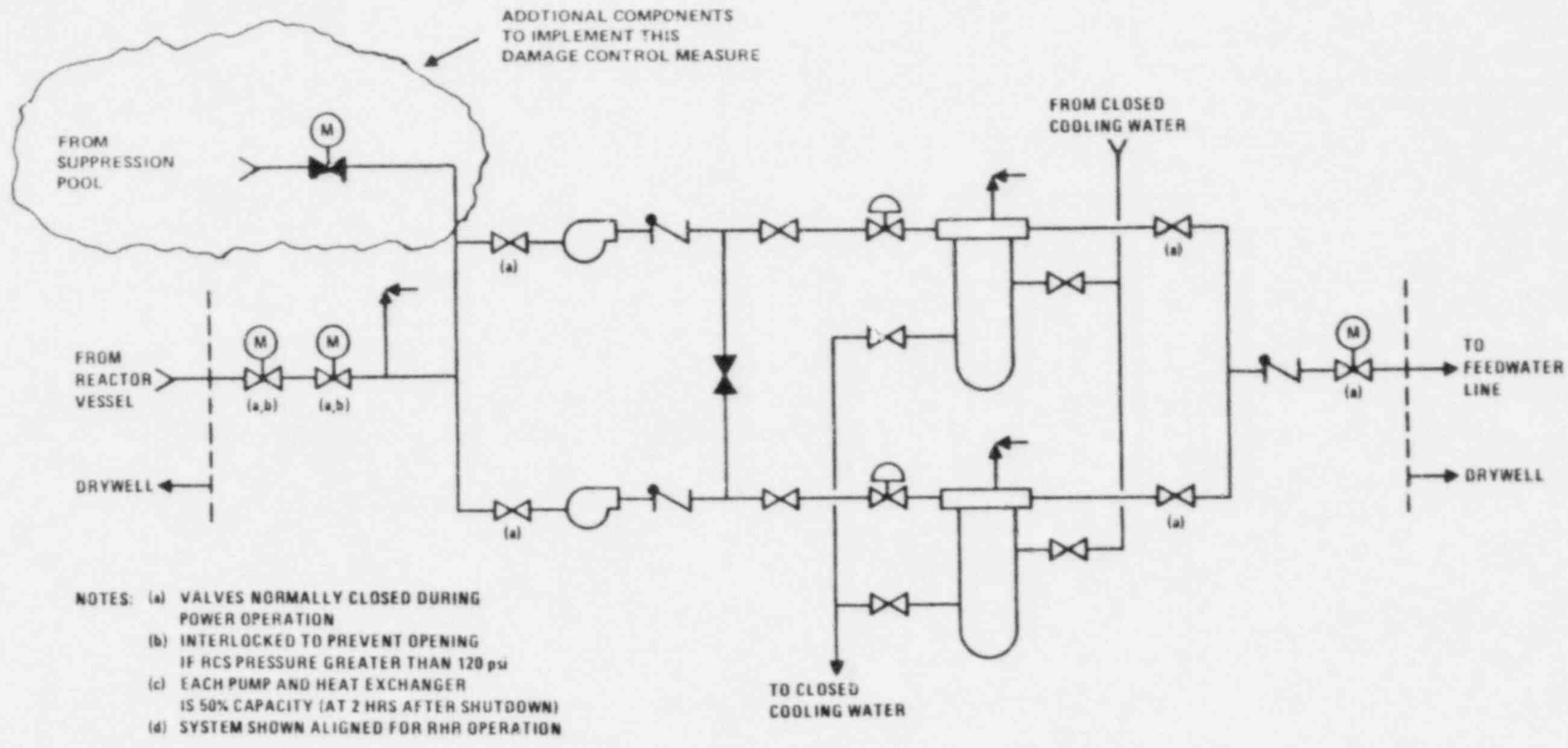


Figure 5.11.3. Typical BWR/1 (Humboldt Bay) Residual Heat Removal System

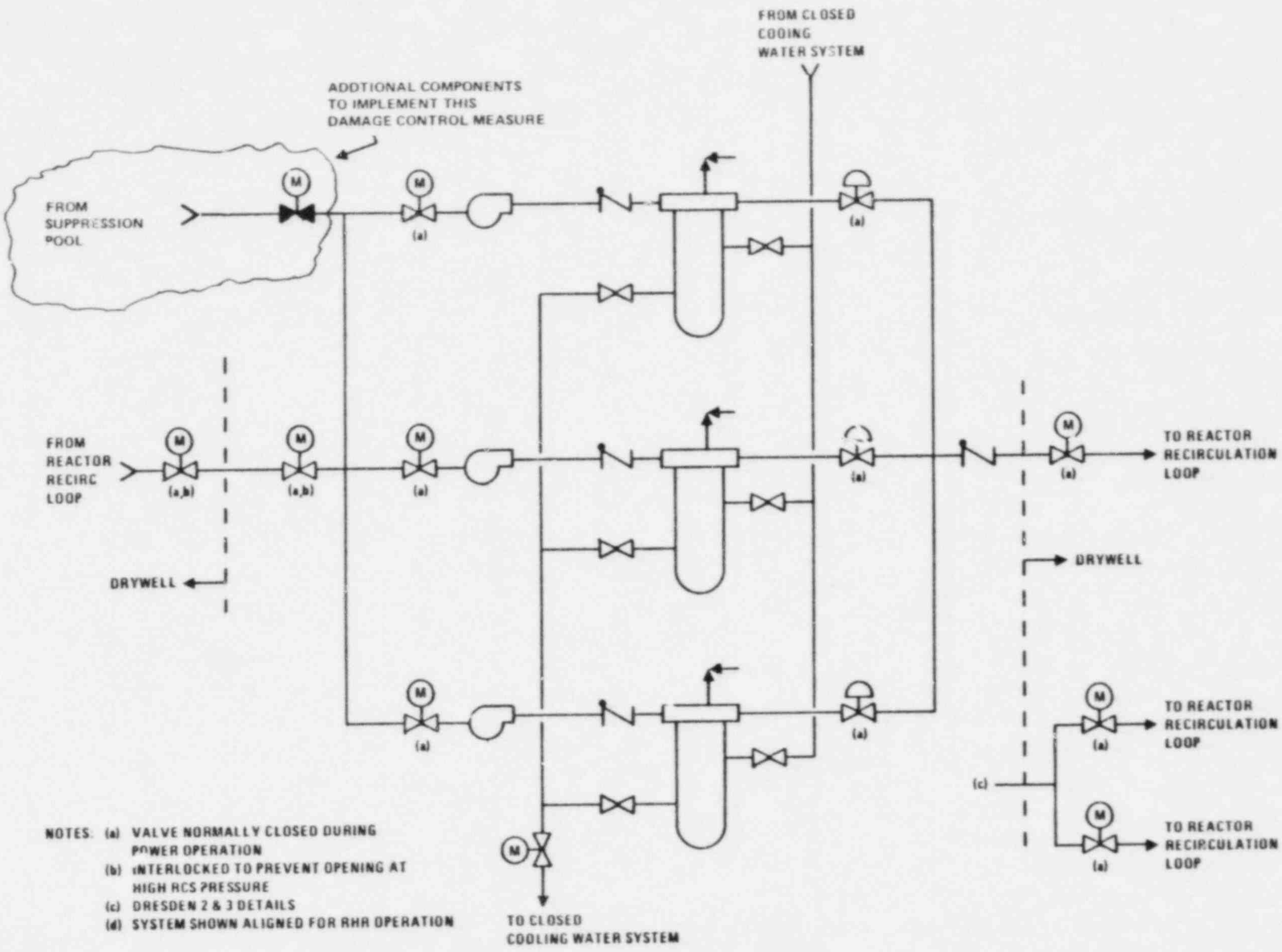


Figure 5.11.4. Typical BWR/2 or 3 (Nine Mile Point, Dresden 2 & 3) Residual Heat Removal System

plants having a single-mode RHR system, low pressure core coolant makeup is provided by the LPCS system and, in a few plants, by a dedicated low pressure coolant injection (LPCI) system.

Middle-vintage BWRs, including some BWR/3 and BWR/4 plants, introduced a multi-mode RHR system. This system performs the following three functions:

- Core shutdown heat removal
- Low pressure coolant injection (as part of the emergency core cooling system)
- Containment cooling (spray or suppression pool recirculation)

A system of this type is illustrated in Figure 5.11.5. It typically consists of two loops, each rated at 100 percent of the required cooling or flow capabilty. For shutdown cooling operation, the RHR pump suction and discharge are aligned to the RCS. Low pressure coolant injection is accomplished by shifting the pump suction to the suppression pool. The LPCI mode of operation is automatically initiated by low reactor vessel water level (e.g., Level 1) or high drywell presure. Other modes of operation are manually initiated.

Later-vintage BWRs, including some BWR/4 and all BWR/5 and BWR/6 plants, continued the evolution of the multi-mode RHR system with the introduction of a system capable of being aligned to perform any of the three functions listed above plus steam-condensing in conjunction with the RCIC system. In this latter mode of operation, one or both RHR heat exchangers are used to condense steam from the reactor vessel. The condensate is returned to the reactor vessel by the RCIC pump. The RHR pumps are not used in this mode of operation. A typical BWR/6 system of this type is illustrated in Figure 5.11.6.

All RHR systems have suction and discharge lines connected to the RCS. During normal power operation, redundant containment isolation values in the suction line, and one or more power-operated containment isolation valves in the return line are closed. In the return line, there is also a check valve. The outer containment isolation valves form the boundary of the high-pressure portion of the RHR system. The remainder of the RHR system is a low pressure system that is not designed for operation at full RCS pressure. During plant operation when

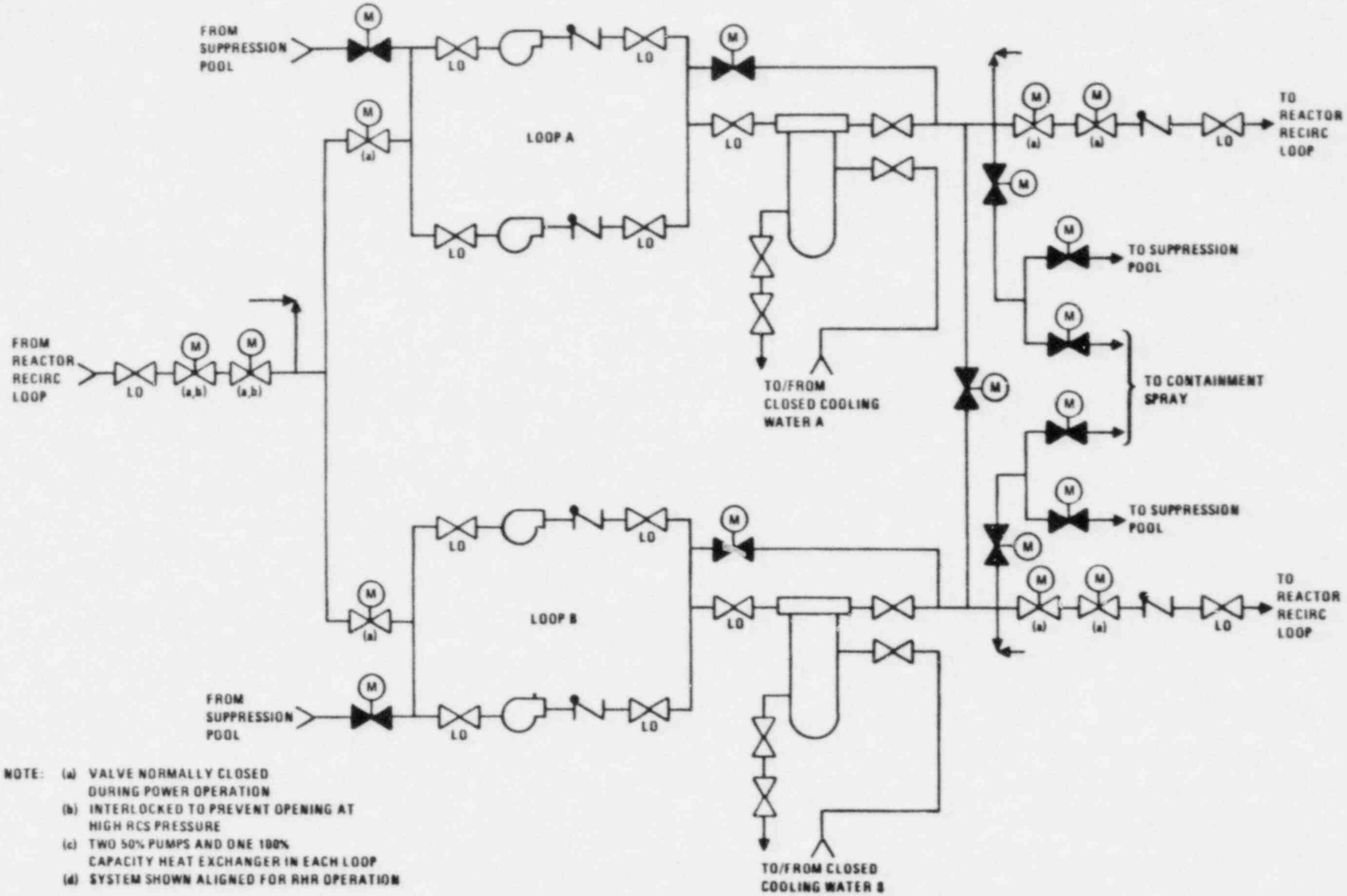


Figure 5.11.5. Typical BWR/3 or BWR/4 (Monticello) Multi-Mode Residual Heat Removal System

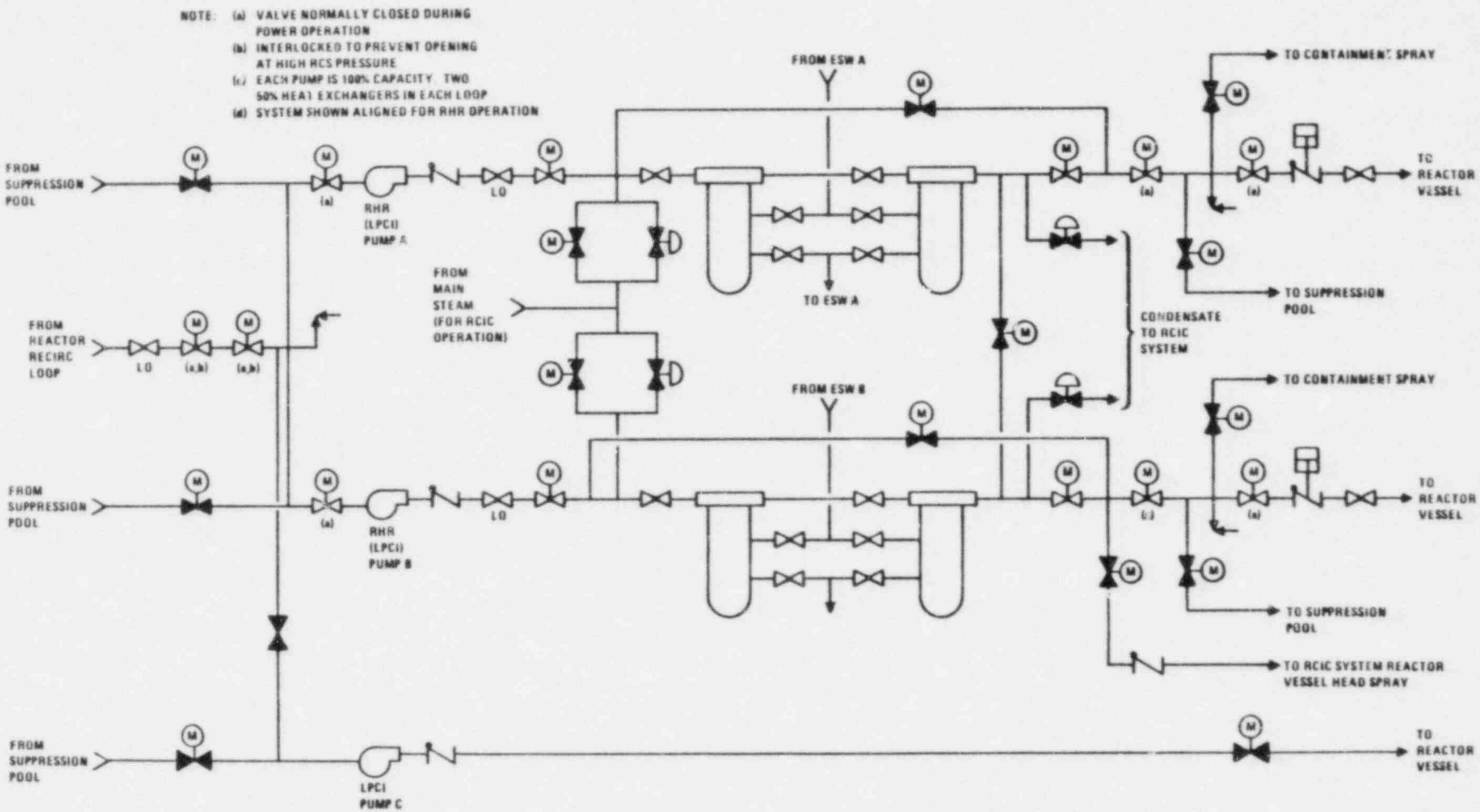


Figure 5.11.6. Typical BWR/5 or BWR/6 (Grand Gulf) Residual Heat Removal System

RCS pressure exceeds the RHR system design pressure, the RHR system is protected against overpressure by the following design features:

- Redundant, normally closed containment isolation valves in the shutdown cooling suction line are interlocked to prevent their opening when RCS pressure exceeds the design pressure for the RHR system.

- Safety valves located at the heat exchangers and, in some plants, in the return line to the RCS protect RHR system components against overpressure due to leakage from the RCS.

5.11.2.3 Low Pressure Coolant Injection (LPCI) System

As described previously, low pressure coolant injection in most BWR plants is performed by an operating mode of the RHR system. Notable exceptions listed in Table 5.11.1 include Humboldt Bay, Millstone 1, and Dresden 2 and 3.

At the Humboldt Bay plant, low pressure coolant injection is accomplished with a crossconnection to the fire water system. Three fire water pumps serve as LPCI pumps.

Millstone 1 has two independent LPCI loops, each with two 33 percent capacity pumps to supply water from the suppression pool. A similar system is provided at Dresden 2 and 3.

5.11.3 <u>BWR Containment Cooling Systems</u>

As summarized in Table 5.11.1, containment cooling (spray and/or suppression pool recirculation) is usually performed by an operating mode of the RHR system. A few BWR/1 and BWR/2 plants, however, have a dedicatd containment spray system. This system at Oyster Creek consists of two independent 100 percent capacity loops. Each loop has two 50 percent capacity pumps and heat exchangers. Pump suction can only be aligned to the suppression pool, with discharge to several spray headers (see Figure 5.11.7). This system is similar to a multi-mode RHR system that is aligned for containment spray.

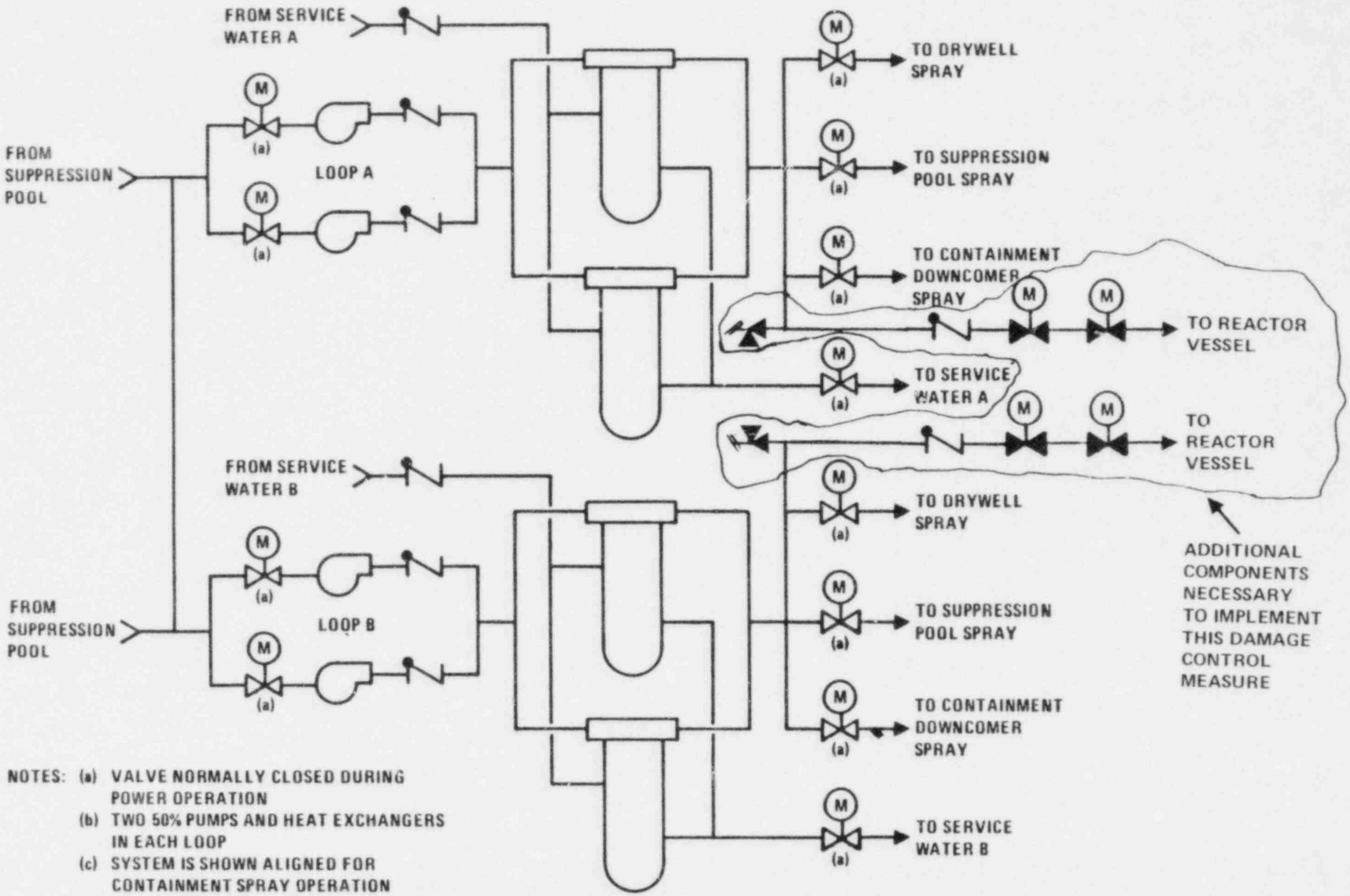


Figure 5.11.7. Typical BWR/2 (Oyster Creek) Containment Spray System

5.11.4 Plant Conditions During Sabotage Scenario

When normal feedwater level is lost, water level in the reactor vessel will decrease. The high pressure coolant injection systems (e.g., RCIC, HPCS, HPCI, FWCI) normally would be started when reactor vessel water level dropped to Level 2 (about ten feet above the core). These systems are assumed to be sabotaged. The CRDHS does not have the makeup capacity to match coolant boiloff until approximately 40 minutes after reactor shutdown (Ref. 2). When reactor vessel water level drops to Level 1 (about 1.5 feet above the top of the core), the low pressure coolant injection systems (LPCS, LPCI and LPCI mode of the RHR system) will be automatically actuated. The ADS system will be automatically actuated for LOCAs, but must be actuated manually to depressurize the plant following transients. ADS actuation logic is the coincidence of Level 1 reactor vessel water level and high drywell pressure. In addition, a permissive interlock in the ADS logic requires that an LPCS or LPCI pump be in operation before the ADS is actuated. With the RCS depressurized, adequate core cooling is provided by the low pressure systems.

5.11.5 System Alignment Necessary to Provide Adequate Core Cooling With the Low Pressure Core Cooling Systems

There is no need to provide additional measures to use the LPCS, LPCI or a multi-mode RHR system for core cooling during accident conditions. This is a normal capability of these systems. Design changes could, however, be made to single-mode RHR and containment spray systems to provide an additional low pressure coolant injection capability for BWR/1, BWR/2 and some BWR/3 plants.

To modify a single-mode RHR system to perform the LPCI function, piping and valves must be added to allow the RHR pumps to take a suction on the suppression pool. Figures 5.11.3 and 5.11.4 include the additional components that would be required. When operating in a LPCI mode, the redundant suction valves in the line from the RCS would be closed and the suppression pool suction line valve would be open. Having made these changes, it would be desirable to provide for automatic system actuation in the LPCI mode. The same actuation logic already available for the LPCS system could provide this capability.

A single-mode containment spray system could also be modified to perform an LPCI function. In this system, the changes would be on the discharge side of the pumps, as illustrated in Figure 5.11.7. During standby operation, the normal containment spray suction and discharge valves are closed creating a closed system. A relief valve is included in the new reactor coolant injection path to provide overpressure protection against leakage from the RCS when the system is in standby, and from transient pressure conditions that may occur during LPCI operation. When operating in the LPCI mode, the containment spray discharge valves would be closed and the isolation valves in the line to the reactor vessel would be open. Automatic actuation could also be provided for this modified system using the available LPCS actuation logic.

5.11.6 Technical and Regulatory Impediments to Implementing Damage Control Measure #11

None

5.11.7 Conclusions and Recommendations Regarding Damage Control Measure #11

This damage control measure is, in actuality, a normal design feature of all BWRs. The identified design changes to single-mode RHR and containment spray systems would provide an added low pressure coolant injection capability for BWR/1, BWR/2 and some BWR/3 plants.

5.11.8 Section 5.11 References

1. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

2. NUREG-0619, Rev. 1, "BWR Feedwater Nozzle and Control Rod Drive Return Line Nozzle Cracking -- Resolution of Generic Technical Activity A-10," U. S. Nuclear Regulatory Commission, November 1980.

5.12 DAMAGE CONTROL MEASURE #12 - BWR

The purpose of damage control measure #12 is to provide reactor coolant using the main condensate pumps to supply water in the event that the normal reactor coolant makeup systems have been disabled by sabotage.

5.12.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of all normal coolant makeup systems. Table 5.12.1 summarizes the high and low pressure coolant makeup capabilities of BWR plants. The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.12.2 System Descriptions

5.12.2.1 Main Feedwater (MFW) System

The main feedwater system is used to supply feedwater to the reactor vessel during normal operations. BWR feedwater and condensate system configurations are summarized in Table 5.12.2. A representative BWR condensate and feedwater system is illustrated in Figure 5.12.1 (from Ref. 1).

The condensate pumps draw a suction on the main condenser hotwell. Usually when two or three condensate pumps are provided, each is rated at 50 percent capacity. The flow from the condensate pumps is directed through several auxiliary condensers, a full flow condensate cleanup system (demineralizer), feedwater heaters, and then to the suction of the booster pumps. Usually when two or three booster pumps are provided, each is rated at two 50 percent capacity. From the booster pumps, flow may be directed through additional feedwater heaters, and then to the main feedwater pump suctions. From the main feedwater pumps, coolant is returned to the reactor vessel. Regulating valves modulate feedwater flow as necessary to maintain normal reactor vessel water level. Feedwater systems usually include 50 percent capacity or three 33 1/3 percent capacity main feedwater pumps. Bypass lines are commonly provided around

Table 5.12.1. Summary of BWR High and Low Pressure Coolant Injection Capabilities

	BWR Type	Systems for Core Coolant Injection at High Pressure(1)					Systems for Core Coolant Injection at Low Pressure and Other Functions(1)			
		RCIC	HPCI	HPCS	FWCI(2)	CRDHS(2)	LPCS	LPCI	RHR-M1	RHR-M2
Dresden 1	1	-	(4)	-	-	X	X	-	-	-
Humboldt Bay	1	-	-	-	X	X	X	X	-	-
Big Rock Point	1	-	-	-	-	X	(5)	-	-	-
Oyster Creek	2	-	-	-	-	X	X	-	-	-
Nine Mile Point	2	-	-	-	X	X	X	-	-	-
Millstone 1	3	-	-	-	X	X	X	X	-	-
Dresden 2 & 3	3	-	X	-	-	X	X	X	-	-
Pilgrim	3	X	X	-	-	X	X	-	X	-
Monticello	3	X	X	-	-	X	X	-	X	-
Quad Cities 1 & 2	3	X	X	-	-	X	X	-	X	-
Hatch 1 & 2	4	X	X	-	-	X	X	-	X	-
Browns Ferry 1, 2 & 3	4	X	X	-	-	X	X	-	X	-
Vermont Yankee	4	X	X	-	-	X	X	-	X	-
Peach Bottom 2 & 3	4	X	X	-	-	X	X	-	X	-
Cooper	4	(3)	X	-	-	X	X	-	-	X
Duane Arnold	4	(3)	X	-	-	X	X	-	-	X
Fitzpatrick	4	(3)	X	-	-	X	X	-	-	X
Brunswick 1 & 2	4	(3)	X	-	-	X	X	-	-	X
Shoreham	4	(3)	X	-	-	X	X	-	-	X
Fermi 2	4	(3)	X	-	-	X	X	-	-	X
Susquehanna 1 & 2	4	(3)	X	-	-	X	X	-	-	X
LaSalle 1 & 2	5	(3)	-	X	-	X	(6)	-	-	X
Zimmer	5	(3)	-	X	-	X	(6)	-	-	X
Hanford 2	5	(3)	-	X	-	X	(6)	-	-	X
Grand Gulf 1 & 2	6	(3)	-	X	-	X	(6)	-	-	X
Other BWR/5 & /6		(3)	-	X	-	X	(6)	-	-	X

Notes:

(1) RCIC = reactor core isolation cooling system
HPCI = high pressure coolant injection system
HPCS = high pressure core spray system
FWCI = feedwater coolant injection system
CRDHS = control rod drive hydraulic system
LPCS = low pressure core spray system
LPCI = low pressure coolant injection system (single mode system)
RHR-M1 = multi-mode RHR system performing LPCI, shutdown cooling, suppression pool cooling and containment spray functions
RHR-M2 = same as RHR-M1 plus steam condensing operation with RCIC

(2) Non-engineered safety feature system except Millstone 1 FWCI

(3) Injection plus steam-condensing modes of operation

(4) Being installed

(5) Also performs suppression pool cooling function

(6) Only a single 100% capacity LPCS pump. Other plants typically have two 100% capacity LPCS trains

Table 5.12.2. Summary of BWR Feedwater and Condensate System Configurations

Plant	BWR Type	Feedwater Pumps Number	Feedwater Pumps Drive(1)	Booster Pumps(2)	Condensate Pumps(2)
Dresden 1	1	2	E	-	(?)
Humboldt Bay	1	2	E	-	2
Big Rock Point	1	2	E	(?)	(?)
Oyster Creek	2	3	E		
Nine Mile Point	2	2,1	E,S	3	3
Millstone 1	3	3	E	3	3
Dresden 2&3	3	3	E	4	4
Pilgrim	3	3	E	-	3
Monticello	3	2	E	-	2
Quad Cities 1&2	3	3	E		
Hatch 1&2	4	2	S	3	3
Browns Ferry 1,2&3	4	3	S	3	3
Vermont Yankee	4	3	E		2
Peach Bottom 2&3	4	3	S	-	3
Cooper	4	2	S	3	3
Limerick	4	3	S	-	3
Duane Arnold	4	2	E		2
Fermi 2	4	2	S	3	3
Fitzpatrick	4	2	S	3	3
Shoreham	4	2	S	2	2
Brunswick 1&2	4	2	S	3	3
Zimmer	5	2	S	3	3
La Salle 1&2	5	2	S	3	3
Grand Gulf 1&2	6	2	S	3	3

Notes:

(1) E = electric motor-driven, S = steam turbine-driven
(2) All electric motor-driven

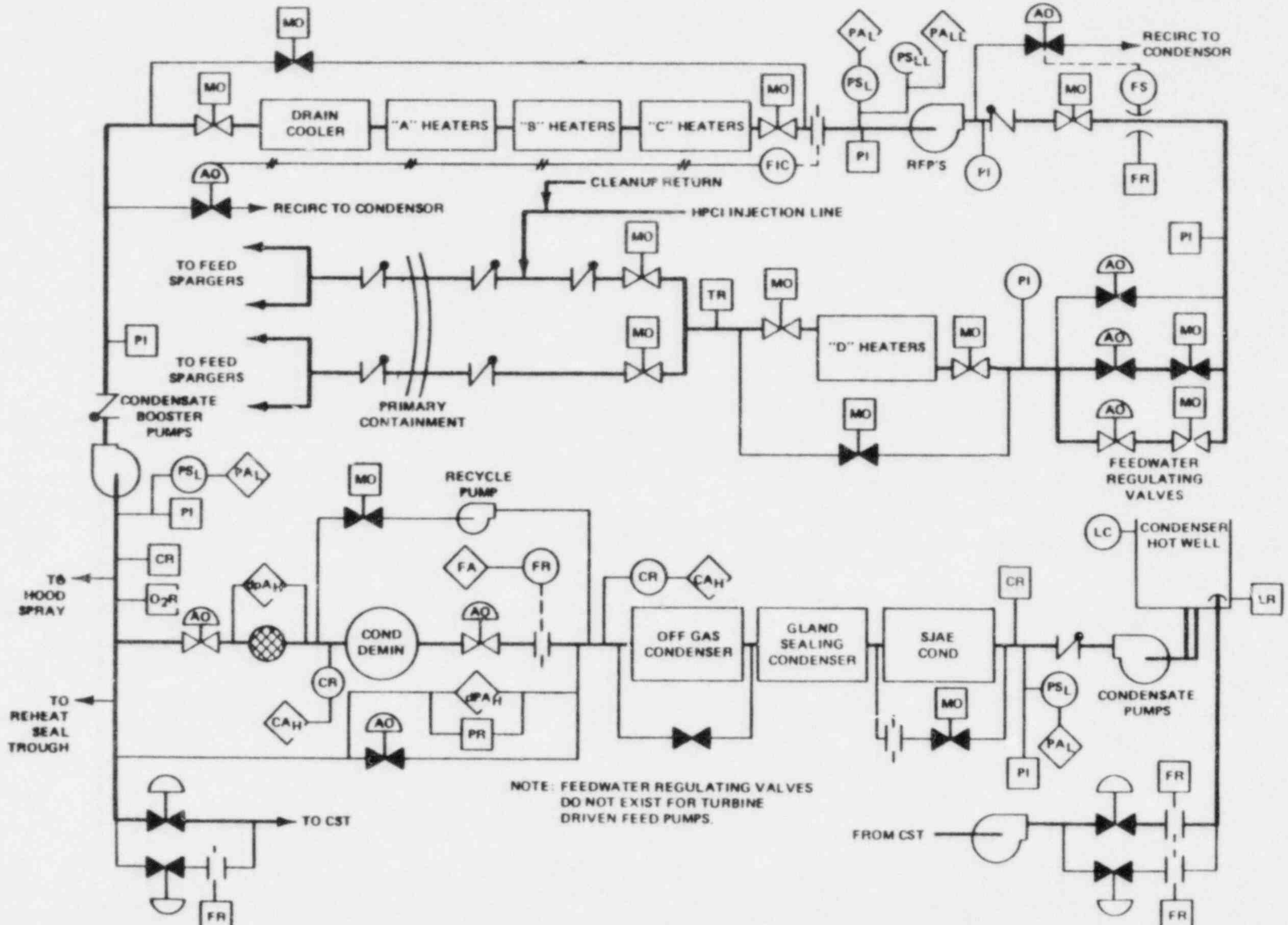


Figure 5.12.1. Condensate and Feedwater System (from NUREG-0626).

the condensate cleanup system, feedwater heaters, auxiliary condensers, and feedwater regulating valves.

The main feedwater and condensate systems are supplied by Nonclass 1E power (except for Millstone 1) and are not available following loss of offsite power.

A few BWR plants use the main feedwater and condensate systems in a high pressure coolant injection mode following events that result in low reactor vessel level. In this mode of operation, the system is referred to as the feedwater coolant injection (FWCI) system. This system takes the place of the high pressure coolant injection (HPCI) or high pressure core spray (HPCS) system found in most other BWRs. At the Humboldt Bay and Nine Mile Point plants, the FWCI system is a nonsafety system. At Millstone 1, however, Class 1E power is provided to operate this system following loss of offsite power.

The FWCI system continues to use the normal feedwater and condensate flow paths to the reactor vessel. If a reactor vessel low level condition exists, the FWCI system isolates all flow paths that could divert feedwater away from the reactor vessel (e.g., steam jet air ejector condenser and gland seal condenser cooling water), thereby maximizing makeup flow to the vessel.

5.12.2.2 Systems for Coolant Makeup at High Pressure

At most BWR plants, high pressure coolant makeup following loss of normal feedwater is provided by the reactor core isolation cooling (RCIC) system and by either a high pressure coolant injection (HPCI) or high pressure core spray (HPCS) system. The RCIC and HPCI (or RCIC and HPCS) systems together provide a redundant high pressure coolant makeup capability. These systems are described in Section 5.5. The control rod drive hydraulic system (CRDHS) is not usually considered as a high pressure coolant makeup system. This system has, however, demonstrated the capability to provide makeup at a rate equal to the coolant boiloff rate approximately 40 minutes after reactor shutdown (Ref. 2). The CRDHS is described in Section 5.10.

5.12.2.3 Systems for Coolant Makeup at Low Pressure

Low pressure coolant makeup following loss of normal feedwater is provided by a low pressure core spray (LPCS) system and by either a separate low pressure coolant injection (LPCI) system or by a residual heat removal (RHR) system operating in the LPCI mode. The LPCS system in BWR/1 through BWR/4 plants typically includes two 100 percent capacity independent loops, each with one pump. A few plants such as Browns Ferry and Peach Bottom, have two LPCS loops, each with two 50 percent capacity pumps. In BWR/5 and BWR/6 plants the LPCS system only has a single 100 percent capacity loop. In all BWR plants, a redundant low pressure coolant makeup capability is provided by the separate LPCI system or by the RHR system operating in the LPCI mode.

For events other than large loss of coolant accidents (LOCAs), the Automatic Depressurization System (ADS) must operate to depressurize the reactor vessel to the point where effective coolant makeup can be provided by the low pressure pumps. Following transients, the ADS must be actuated manually from the control room. The coincidence logic for automatic actuation is only satisfied during LOCA conditions (e.g., reactor vessel low water level <u>and</u> high drywell pressure). In addition, a permissive interlock in the ADS logic requires that an LPCS or LPCI pump be operating before the ADS is actuated. The LPCS, LPCI and RHR systems are described in Section 5.11 and the ADS is described in Section 5.1.

5.12.3 Plant Conditions During Sabotage Scenario

The electrically-powered condensate, booster and main feedwater pumps are inoperable (except at Millstone 1) because of loss of Nonclass 1E AC power. When normal feedwater is lost, water level in the reactor vessel will decrease. The high pressure coolant injection systems (e.g., RCIC, HPCS, HPCI, FWCI) normally would be started when reactor vessel water level drops to Level 2 (about ten feet above the core). These systems are assumed to be sabotaged. The CRDHS does not have the makeup capacity to match coolant boiloff until approximately 40 minutes after reactor shutdown (Ref. 2). This system is assumed to be sabotaged. When reactor vessel water level drops to Level 1 (about 1.5 feet above the top of the core), the low pressure coolant injection systems (LPCS, LPCI and LPCI of the

RHR system) normally would be automatically actuated. These systems are also assumed to be sabotaged. The ADS system will be actuated automatically for LOCAs, but must be actuated manually to depressurize the plant following transients. The pump permissive interlocks in the ADS actuation logic cannot be satisfied following sabotage of the low pressure coolant makeup systems. The control room operator, therefore, cannot initiate reactor coolant system (RCS) depressurization using the ADS actuation logic. The operator can, however, open the safety/relief valves using their individual valve control circuits which are not part of the ADS actuation logic. Therefore, the RCS can be depressurized. With the RCS depressurized, it may be possible to provide adequate core cooling by restoring the condensate pumps to operation.

If a coolant makeup capability cannot be restored, it has been estimated that reactor vessel water level will fall to the core midplane approximately 1.4 hours after the loss of offsite power (Ref. 3).

If reactor vessel level can be restored, the next major problem to be faced is suppression pool cooling. In most BWR plants, suppression pool cooling is provided by an operating mode of the RHR system which also performs the low pressure coolant makeup function. This system is assumed to be sabotaged. Alternate methods of providing suppression pool cooling are described in damage control measure #2.

5.12.4 System Alignment Necessary to Provide a Low Pressure Coolant Injection Capability Using the Condensate Pumps

A comparison of the general characteristics of condensate, LPCS and LPCI pumps is provided in Table 5.12.3. A condensate pump could provide greater coolant makeup flow than either an LPCS or LPCI (RHR) pump at comparable discharge pressure. A summary of LPCS and LPCI system characteristics is provided in Table 5.12.4.

To provide adequate core cooling at low pressure, a single 100 percent capacity LPCS pump (or two 50 perecent capacity pumps in some plants) is required. Comprable flow could be provided by a single condensate pumps. Most BWR/3 and BWR/4 plants have four RHR pumps capable of performing the LPCI function. Adequate core cooling usually requires the operation of 2-of-4 or

Table 5.12.3. Comparison of Condensate, Low Pressure Core Spray and Low Pressure Coolant Injection Pump Characteristics.

	Condensate Pump	LPCS Pump	LPCI Pump
Type	Multi-Stage Centrifugal	Single-Stage Centrifugal	Single-Stage Centrifugal
Flowrate	7000 to 12,000 gpm	3000 to 6110 gpm	4000 to 10,000 gpm
Design Head	Several hundred feet	90 to 145 psid (207 to 334 feet)	20 to 125 psid (46 to 287 feet)
Horespower	Several hundred horsepower	500 to 1750	300 to 900

Table 5.12.4. Summary of BWR Low Pressure Core Spray (LPCS) and Low Pressure Coolant Injection (LPCI) System Characteristics.[1]

BWR Plant	BWR Type	LPCS[2]	LPCI[2]
Oyster Creek	2	(8x) 3400 @ 110 (4/8)	-
Nine Mile Point	2	(8x) 1700 @ 113 (2/8)	-
Millstone 1	3	(2x) 3600 @ 90 (1/2)	(4x) 2500 @ 165 (2/4)
Dresden 2 & 3	3	(2x) 4500 @ 90 (1/2)	(4x) 2675 @ 200 (2/4)
Pilgrim	3	(2x) 3600 @ 120 (1/2)	(4x) 4800 @ 20 (3/4)
Monticello	3	(2x) 4500 @ 145 (1/2)	(4x) 4000 @ 20 (2/4)
Quad Cities 1 & 2	3	(2x) 4500 @ 90 (1/2)	(4x) 4830 @ 20 (2/4)
Hatch 1 & 2	4	(2x) 4625 @ 132 (1/2)	(4x) 7700 @ 20 (2/4)
Browns Ferry 1, 2 & 3	4	(4x) 3125 @ 122 (2/4)	(4x) 9999 @ 20 (2/4)
Vermont Yankee	4	(2x) 3000 @ 120 (1/2)	(4x) 7200 @ 20 (2/4)
Peach Bottom 2 & 3	4	(4x) 3125 @ 122 (2/4)	(4x) 10000 @ 20 (2/4)
Cooper	4	(2x) 4500 @ 115 (1/2)	(4x) 7700 @ 20 (1/4)
Duane Arnold	4	(2x) 3020 @ 113 (1/2)	(4x) 4800 @ 20 (3/4)
Fitzpatrick	4	(2x) 4625 @ 120 (1/2)	(4x) 7710 @ 290 (3/4)
Brunswick 1 & 2	4	(2x) 4725 @ 100 (1/2)	(4x) 4100 @ 246 (1/2)
Shoreham	4	(2x) 4725 @ 121 (1/2)	(4x) 7700 @ 20 (2/4)
LaSalle 1 & 2	5	(1x) 6350 @ 122 (1/1)	(3x) 7450 @ 20 (2/3)
Zimmer	5	(1x) 4625 @ 119 (1/1)	(3x) 5050 @ 20 (2/3)
Grand Gulf 1 & 2	6	(1x) 7000 @ 122 (1/1)	(3x) 7450 @ 20 (2/3)
Perry 1 & 2	6	(1x) 6000 @ 122 (1/1)	(3x) 7100 @ 20 (2/3)

Notes:

(1) Abstracted from NUREG/CR-2069, "Summary Report on A Survey of Light Water Reactor Safety Systems," with modifications and additions from other safety analysis reports.

(2) System characteristics are listed as follows: the number in the first set of parentheses indicates the number of pumps (e.g., "4x" means four pumps), the fraction in the second set of parentheses is the system success criteria (e.g., "2/4" means that two of four pumps are required for the system safety function to be successful). The data between the two sets of parentheses includes the capacity of each pump (in gallons per minute) at a specified discharge head (in psid). The code "(4x) 7700 @ 20 (2/4)" is therefore read as follows: four pumps rated at 7700 gpm at 20 psid, two-of-four pumps are required.

3-of-4 pumps (Ref. 4). Required LPCI system flow ranges from 8000 to 20,000 gpm at 20 psid. Two condensate pumps may be required to provide this flow rate. BWR/5 and BWR/6 plants have three RHR pumps capable of performing the LPCI function. For events other than a design basis LOCA, 2-of-3 pumps can provide adequate core cooling (Ref. 5). Total LPCI system flow likely would be in the 10,000 to 15,000 gpm range at 120 psid. Two condensate pumps also may be required to provide this flow rate.

The system interconnections necessary to use the condensate pumps for low pressure coolant makeup are illustrated in Figure 5.12.2, and are discussed below.

- Piping interconnections and appropriate valving are added to align the condensate pump suctions to the condensate storage tank or to the suppression pool. These interconnections are required so that the condensate pumps have access to long term water sources for core cooling. All valves in these interconnections are normally closed. At least two valves must be opened to align the condensate pump suction to either of these two new sources of water.

- A valve is added to isolate the suction-side of the condensate pumps from the main condenser hotwell when water is being supplied from the condensate storage tank or the suppression pool. This is required to prevent air-binding the pumps when the hotwell is emptied.

- Piping interconnections and appropriate valving are added to align the condensate pump discharge to the LPCS spray header. This interconnection allows the condensate pumps to perform the function of the LPCS system. The normal injection path via the main feedwater system is functionally comparable to the LPCI injection path.

- Electric power must be restored to the following condensate and feedwater system components:

  - One or two condensate pumps.

  - One or two booster pumps (if provided, and if necessary to provide a higher injection head).

  - Any auxiliary systems required by the condensate or booster pumps (e.g., lube oil, cooling water, etc.).

  This can be accomplished by supplying these components with Class 1E power (see damage control measure #19) or with an alternate onsite source of Nonclass 1E power (see damage control measure #26).

In addition to these design changes, plant operators would likely use existing

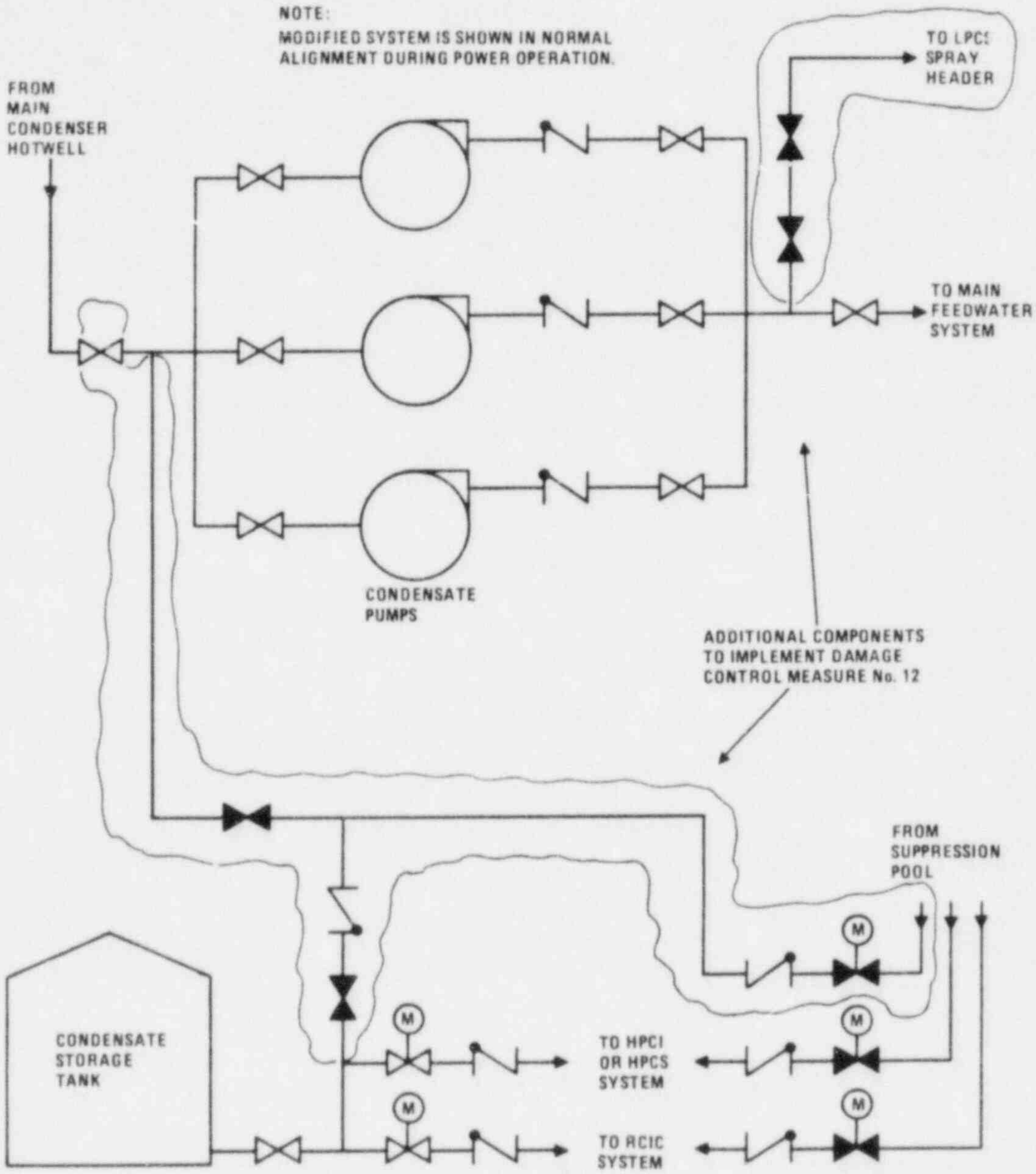


Figure 5.12.2. Modifications Necessary to Implement Damage Control Measure #12.

equipment to realign the feedwater and condensate system and establish bypass flow paths around the following components:

- The auxiliary condensers (e.g., steam jet air ejector, off-gas, and gland sealing condensers)
- Full flow condensate cleanup demineralizers
- Feedwater heaters
- Steam drain coolers
- Feedwater regulating valves.

With this modified system in operation during accident conditions, reactor vessel water level can be maintained by manually throttling valves at the feedwater regulating valve station, or by manually cycling the condensate pumps "ON" and "OFF". With suitable operating procedures and operator training, it should be possible to realign the condensate system and restore a low pressure core coolant inventory control capability.

5.12.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #12

It is technically feasible to install properly sized piping interconnections between the condensate pump suctions and alternate water sources. With this piping and associated valving in place, and with the ability to restore power to the condensate pumps, damage control measure #12 could provide a backup low pressure coolant makeup capability.

The potential regulatory impediments to implementing this damage control measure include the following:

- The condensate storage tank is the normal water source for the HPCS (or HPCI) system and the RCIC system. Aligning the modified main feedwater system to this tank during an emergency should be acceptable, when other systems have failed to provide adequate coolant inventory control. If, however, the main feedwater system were inadvertently connected to the condensate storage tank during normal power operations, the availability of this emergency source of coolant could be paced in jeopardy. Normally closed and locked series valves with suitable physical protection may provide adequate assurances against inadvertent alignment of the condensate pump suction to the condensate storage tank.

- Any electrical interconnections between the Nonclass 1E and the Class 1E AC distribution systems would require particular attention to assure that the Class 1E system is not degraded because of the interconnection. See damage control measure #19 for additional information.

5.12.6 Conclusions and Recommendations Regarding Damage Control Measure #12

This damage control measure appears to be technically feasible. Sufficient time is avaiable to permit the manual operations necessary to realign the condensate and feedwater systems, and to restore power to the required equipment. This damage control measure would provide another means to restore the low pressure coolant inventory control function.

5.12.7 Section 5.12 References

1. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

2. NUREG-0619, Rev. 1, "BWR Feedwater Nozzle and Control Rod Return Line Cracking, Resolution of Generic Technical Activity A-10," U. S. Nuclear Regulatory Commission, November 1980.

3. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

4. Heddleson, F. A., "Summary Report on a Survey of Light Water Reactor Safety Systems," NUREG/CR-2069, Oak Ridge National Laboratory, October 1981.

5. "238 Nuclear Steam Supply System-GESSAR," Docket STN-50550, General Electric Company.

5.13 DAMAGE CONTROL MEASURE #13 - PWR AND BWR

The purpose of damage control measure #13 is to crossconnect the plant service water system to the essential service water (ESW) system to restore cooling water flow to components and systems in the event that the ESW pumps are disabled through sabotage actions.

5.13.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the sabotage of all ESW pumps. The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to the Class 1E electrical system.

5.13.2 System Descriptions

5.13.2.1 PWR Essential Service Water and Component Cooling Water Systems

A. Essential Service Water System

The ESW system is used to transfer heat from a component cooling water (CCW) system to the ultimate heat sink during normal operations and emergencies. The system typically consists of two independent trains. A simplified schematic of a representative ESW system is shown in Figure 5.13.1.

The ESW system uses water from the ultimate heat sink which may be a pond, river, lake, ocean or a cooling tower. The water is usually treated using simple filtration and chlorination at the pump intake structure, and generally no attempt is made to further treat the water. Consequently, service water may contain relatively large quantities of particulates and chemical contaminants and water is used to cool the secondary side of the CCW heat exchangers rather than for direct cooling of the operating components. Table 5.13.1 summarizes the PWR systems and components that may be served by a CCW system, and hence would be dependent on ESW system operation. Each safety-related system in this table is typically arranged with two redundant, independent subsystems (or loops). The separation criteria adopted for nuclear power plant design results in these subsystems being divided into two or more redundant, independent groups, each of which is served by a redundant, independent loop of CCW, electric power and any other required services. During a design basis accident, a CCW loop is capable of providing the full cooling capacity required by the subsystems it serves. Typically, the CCW loops do not operate crossconnected. Loss of a single CCW loop (e.g., due to partial

Table 5.13.1 Typical PWR Systems and Components Requiring Component Cooling Water.

Safety-related systems and components	Diesel generators (diesel cooling system heat exchangers)(2) High pressure safety injection system (pumps) Low pressure safety injection system (pumps) Containment spray system (pumps) Containment cooling system (emergency fan coolers) Fuel handling building cleanup system (post-accident cleanup unit coolers) Control room and auxiliary building emergency HVAC system (emergency chillers) Shutdown cooling system (RHR heat exchangers)(3) Chemical and volume control system (letdown heat exchangers and charging pumps)
Nonsafety-related systems and components(1)	Reactor coolant pumps (pump and motor coolers, pump seals) Control rod drive mechanism cooling units Spent fuel pool cooling system (pool cooling heat exchangers) Radwaste system (boric acid concentrator, waste evaporator, waste gas compressors, gas strippers) Reactor coolant sampling system (sample cooler)

Note: (1)Cooling for these components may be terminated automatically during an accident, and restarted manually, as necessary.

(2)Diesels may be cooled directly by an essential service water system, or by a separate water-to-air (e.g., radiator) cooling system rather than by the CCW system.

(3)RHR heat exchangers may also be used in the containment spray system.

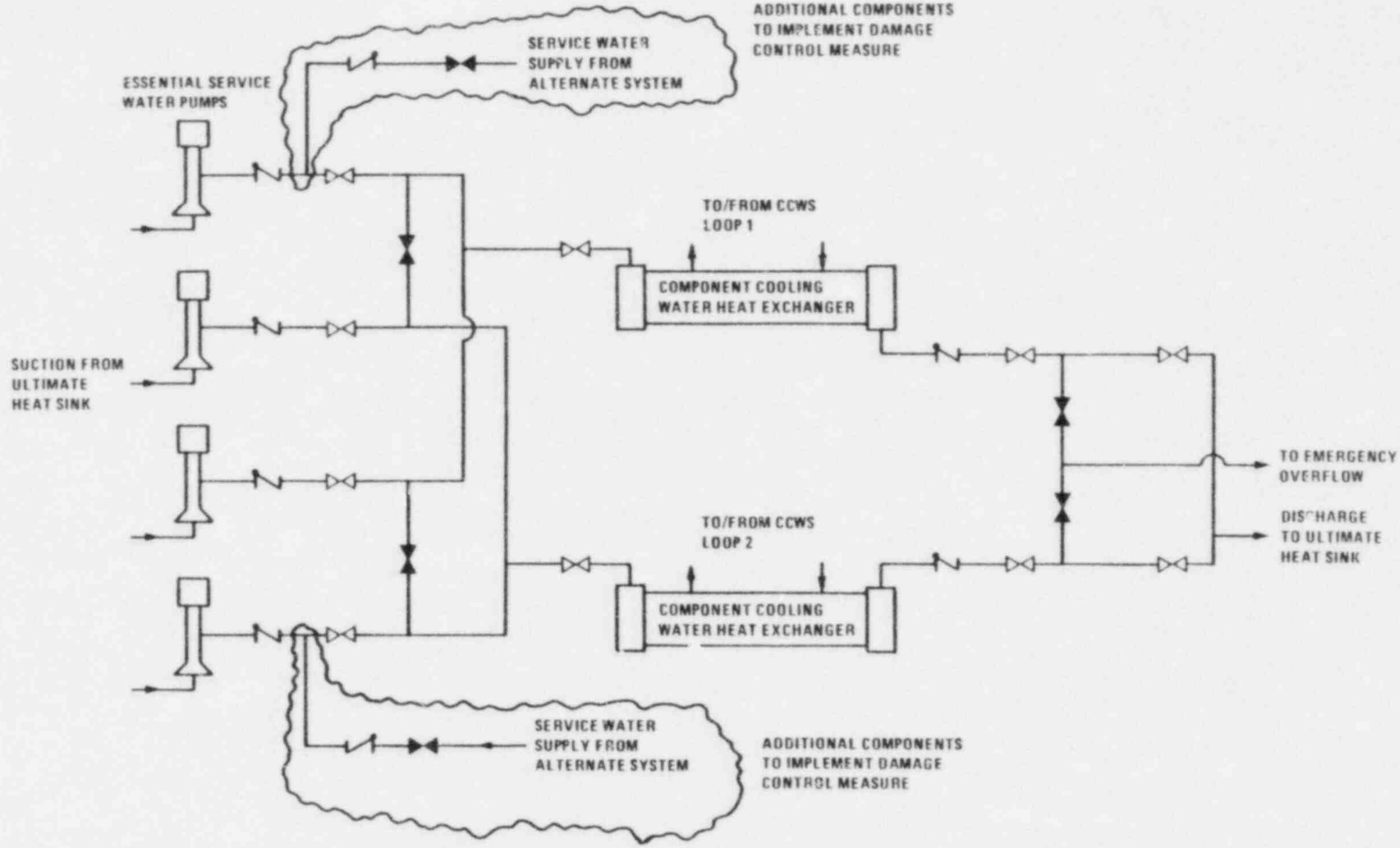


Figure 5.13.1. Representative Essential Service Water System.

failure or loss of one train of ESW) does not affect the ability to maintain the plant in a safe condition.

During normal plant conditions, only one loop of the ESW system in Figure 5.13.1 is in operation, providing secondary-side cooling for one train of the CCW system. Only one ESW pump per loop is required. The second pump in each loop is a backup. After flowing through the CCW heat exchangers, service water is returned to the ultimate heat sink.

ESW pumps are typically vertical turbine wet-pit pumps with single-stage or multi-stage impellers. These pumps are electrically powered from the Class 1E system. ESW system water flow rates are plant specific and are dependent on the mode of cooling (e.g., air-cooled or water-cooled) selected for the components essential for safe plant shutdown. A representative ESW system may require flow rates on the order of 12,000 to 20,000 gpm per loop at heads of 60 to 100 feet. The ESW system is typically open loop with once-through cooling, except when the ultimate heat sink is a cooling tower. ESW system design normally provides a temperature differential of about 20°F between inlet and outlet under full load. The CCW system flow rates to individual components are summarized in Table 5.13.2 (a rough measure of the heat input to the CCW system by the individual components).

B. Component Cooling Water System

See Section 5.16.

5.13.2.2 BWR Essential Service Water System

A BWR ESW system is used to transfer heat directly from the components listed in Table 5.13.3 to the ultimate heat sink during normal operations and emergencies. The system typically consists of three independent trains or divisions. Divisions 1 and 2 serve all components except those associated with the high pressure coolant injection (HPCI) and high pressure core spray (HPCS) systems which are served by Division 3. The HPCI components requiring ESW cooling include the pumps, room coolers and the dedicated HPCS diesel generator.

A representative Division 1 or 2 ESW loop is illustrated in Figure 5.13.2 and a Division 3 ESW loop is shown in Figure 5.13.3. Divisions 1 and 2 of the ESW system both supply safety-related and nonsafety-related equipment, and will be in operation during normal plant conditions. The Division 3 ESW loop will only be in operation when the HPCI or HPCS system is operating.

Table 5.13.2. PWR and BWR Components Typically Cooled by an Essential Service Water (ESW) or Component Cooling Water (CCW) System.

Components Supported by an Individual Cooling Water Loop(1)	Typical Cooling Water Flow To Component (gpm)(2)	Plan Conditions Requiring Cooling of Component(3)		
		Power Operations	Post-Transient (Hot Shutdown)	Post-LOCA
Shutdown Cooling (RHR) Heat Exchanger	5000-8000		(5)	✓
Diesel Generator	2000-3000(3)		✓	✓
Boric Acid Concentrator & Gas Stripper (PWR only)	2000-3000	✓		
Containment Emergency Fan Coolers(2 coolers PWR only)	1500-2000 (total)			✓
Reactor Coolant Pumps (4 pumps, PWR only)	1200-2000 (total)	✓		
Spent Fuel Pool Cooling Heat Exchanger	1000-1600	✓	(6)	(6)
Drywell Chiller (BWR only)	600-800	✓	(6)	(6)
Emergency HVAC Chiller	500-1300		✓	✓
Normal HVAC Chiller	500-1300	✓	(6)	(6)
Waste Evaporator	150-1300	✓		
Reactor Recirculation Pumps (2 pumps, BWR only)	800-1200 (total)	✓		
Letdown Heat Exchanger (PWR only)	300-1000	✓		
Control Rod Drive Mechanism Coolers (PWR only)	300-400 (total)	✓		
Fuel Handling Building Cleanup System	100-200		(7)	(7)
Hydrogen Recombiner	50-150			✓
Individual Pump Room Cooler	30-90	✓	✓	✓
Sample Cooler	30-40	✓		
Steam Tunnel Cooler (BWR only)	10-50	✓	(6)	(6)
Individual Large Safety-Related Pump	10-40	✓	✓	✓
Waste Gas Compressor	5-25	✓		

Notes:
(1) This is a composite list including PWR and BWR components
(2) Cooling flow per unit, unless otherwise noted
(3) Assumes loss of off-site power in post-transient and post-LOCA conditions
(4) Estimated cooling requirements are approximately 1000 gpm per 2850 kw diesel generator output capacity at 100°F CCW supply temperature (Ref. 3).
(5) PWRs do not require the RHR heat exchanger in a hot shutdown conditon. BWRs may require the RHR heat exchangers for suppression pool cooling or for operating the Reactor Core Isolation Cooling (RCIC) system in the steam-condensing mode.
(6) Cooling may be automatically secured following accidents. Cooling can be manually restared if required.
(7) Required for fuel handling accidents only.

Table 5.13.3. Typical BWR Systems and Components Requiring Essential Service Water.

Safety-related systems and components	Diesel generators (diesel cooling system heat exchangers) High pressure coolant injection or core spray system (HPCI or HPCS pumps and room coolers) Low pressure core spray system (LPCS pumps and room coolers) Low pressure coolant injection or residual heat removal system (LPCI or RHR pumps, heat exchangers and room coolers[2]) Reactor core isolation cooling system (RCIC room cooler) Containment spray/suppression pool cooling system (pumps, heat exchangers and room coolers)[3] Safety-related HVAC system (control building chiller) Hydrogen recombiner system (precooler)[4] Standby gas treatment system (room cooler)
Nonsafety-related systems and components[1]	Drywell chiller Steam tunnel cooler Reactor building chiller Spent fuel pool cooling system (pool cooling heat exchangers) Radwaste system (waste concentrator) Closed cooling water system (heat exchanger)

Note: (1) Cooling for these components may be terminated automatically

(2) In most BWR plants, the LPCI function is performed by an operating mode of the RHR system

(3) In most BWR plants, containment cooling is performed by an operating mode of the RHR system. BWR/1 and BWR/2 plants have a separate system with separate heat exchangers for containment cooling

(4) BWR plants with noninerted containments only

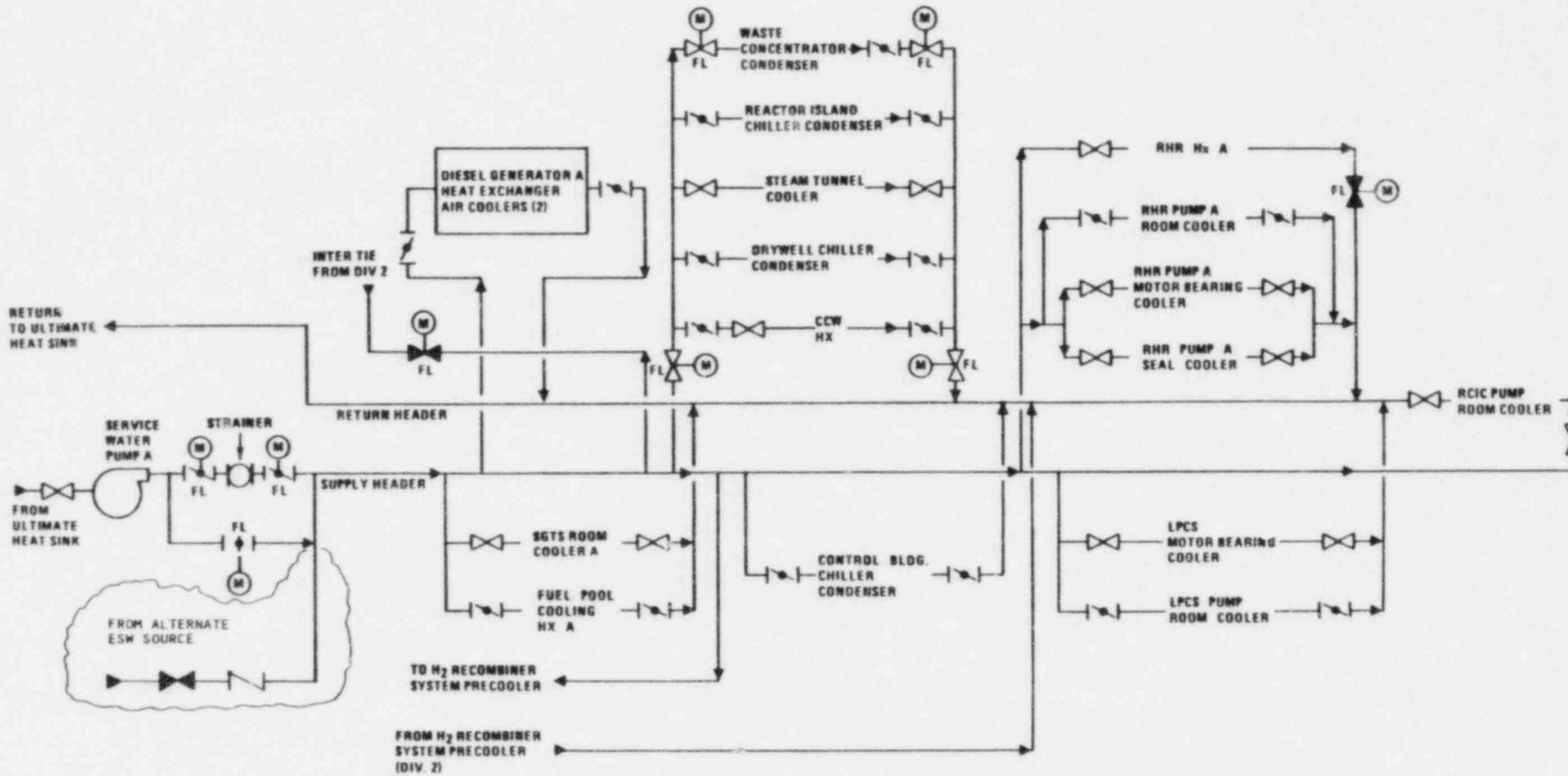


Figure 5.13.2. Representative Division 1 or 2 BWR ESW Loop (from SAI01379-627LJ).

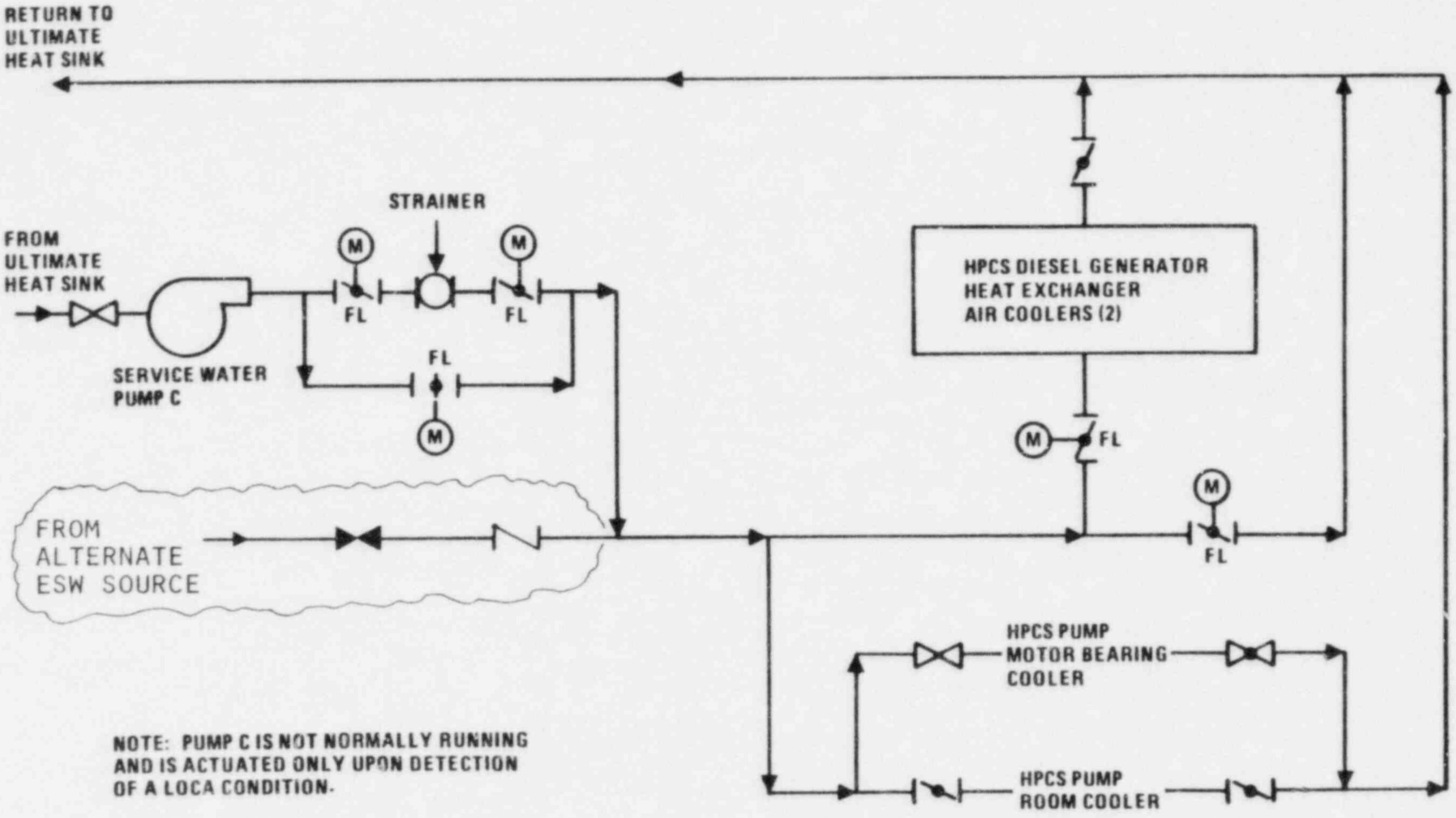


Figure 5.13.3. Representative Division 3 BWR ESW Loop (from SAI01379-627LJ).

ESW pumps are typically vertical turbine wet pit pumps comparable to those described previously. Division 1 and 2 pumps are rated at about 5000 to 9000 gpm and the Division 3 pump is rated at 1000 to 1500 gpm. The ESW system flow rates to individual components are summarized in Table 5.13.2 (a rough measure of the heat input to the ESW system by the individual components).

5.13.2.3 Nonsafety-Related Service Water Systems

Other service water systems provide cooling for a variety of nonsafety equipment. Specific design details vary greatly among plants. Generally, these systems receive Nonclass 1E power and are not available following loss of offsite power.

5.13.3 System Conditions During Sabotage Scenario

The ESW system is inoperable because of sabotage actions. Systems and components cooled directly or indirectly (e.g., via a CCW system) by the ESW system will be operating without a heat sink, and will be heating up. Component failure will occur if flow in the ESW system is not restored. The most critical components may be the diesel generators which are likely to require restoration of adequate cooling water flow within about five minutes after startup (see Section 5.27).

5.13.4 System Alignment Necessary to Crossconnect a Nonsafety-Related Service Water System to an ESW System

The basic interface requirement to be met by an alternate service water system is to provide adequate cooling water flow in the ESW system. The maximum required flow rate would be comparable to the existing ESW flow rate. Lesser flow rates may provide adequate cooling if the heat input to the ESW system can be reduced. Cooling to all nonsafety-related components and systems listed in Tables 5.13.1 and 5.13.3 can be secured. These components and systems are not likely to be operating following loss of offsite power. Components requiring cooling during the postulated sabotage scenario are indicated in the column labeled "Post-Transient (Hot Shutdown)" in Table 5.13.2. For this plant condition, and with all nonessential components isolated, heat input to the ESW system may be 30 to 40 percent less than during normal operations for PWRs. It may however, be significantly greater than during normal operations for BWRs which would require the RHR heat exchangers for suppression pool cooling or for operation of the reactor core isolation cooling (RCIC) system in the steam-condensing mode (BWR/5 and BWR/6 plants only). Any service water system that can provide the required flow rate is a potentially viable substitute for the ESW pumps.

Approaches for connecting an alternate service water system to existing ESW systems are illustrated in Figures 5.13.1, 5.13.2, and 5.13.3. The existing ESW outfall (return) lines continue to be used in all cases. An alternate outfall line could be added to further improve the flexibility of the system to bypass disabled components. If an alternate outfall line is used, it will be necessary to provide it with a radioactivity monitoring capability (e.g., gross gamma monitoring) comparable to the existing ESW outfall line.

As discussed previously, it may be necessary to rapidly restore ESW system flow to support operation of the diesel generators. Power-operated isolation valves in the ESW/alternate service water system crossconnect line would be required to permit rapid, remote realignment of the systems. To extend the time available for operator actions, the diesel generator cooling water system could be redesigned to remove its dependence on external cooling water systems such as an ESW or CCW system (see damage control measure #27).

Electric power must be restored to the alternate service water system following loss of offsite power. This can be accomplished by supplying the system from the Class 1E power system (see damage control measure #19) or from an alternate source of Nonclass 1E power (see damage control measure #26).

5.13.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #13

Any electrical interconnections between the Nonclass 1E and the Class 1E AC distribution systems would require particular attention to assure that the Class 1E system is not degraded because of the interconnections. See Section 5.19 for additional information.

5.13.6 Conclusions and Recommendations Regarding Damage Control Measure #13

This damage control measure appears to be technically feasible, however, only limited time is available to align an alternate service water system if the ESW system directly supplies the diesel generators. Additional time for operator response is available if the diesels are served by a CCW system or by some independent cooling system.

5.14 DAMAGE CONTROL MEASURE #14 - PWR

The purpose of damage control measure #14 is to crossconnect the feedwater system (e.g., from the auxiliary feedwater pump or condensate pump discharges) to the essential service water (ESW) system to provide for heat removal from the component cooling water (CCW) system in the event that the ESW pumps are disabled through sabotage actions.

5.14.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the sabotage of all ESW pumps. The main turbine generator trips on loss of load. The emergency diesel generators operate to supply AC power to the Class 1E electrical system. The other components of the ESW system remain operable.

5.14.2 System Descriptions

5.14.2.1 Essential Service Water System

See Section 5.13.

5.14.2.2 Component Cooling Water System

See Section 5.16.

5.14.2.3 Main Feedwater (MFW) System

The MFW system of the plant is used to supply feedwater to the steam generators. Typical system designs include two 50 percent to 70 percent capacity or three 50 percent capacity MFW pumps. Two to four condensate pumps are provided. Some plants also require booster pumps between the condensate and MFW pumps. A summary of MFW system configurations is included in Section 5.3. A representative MFW system is illustrated in Figure 5.14.1.

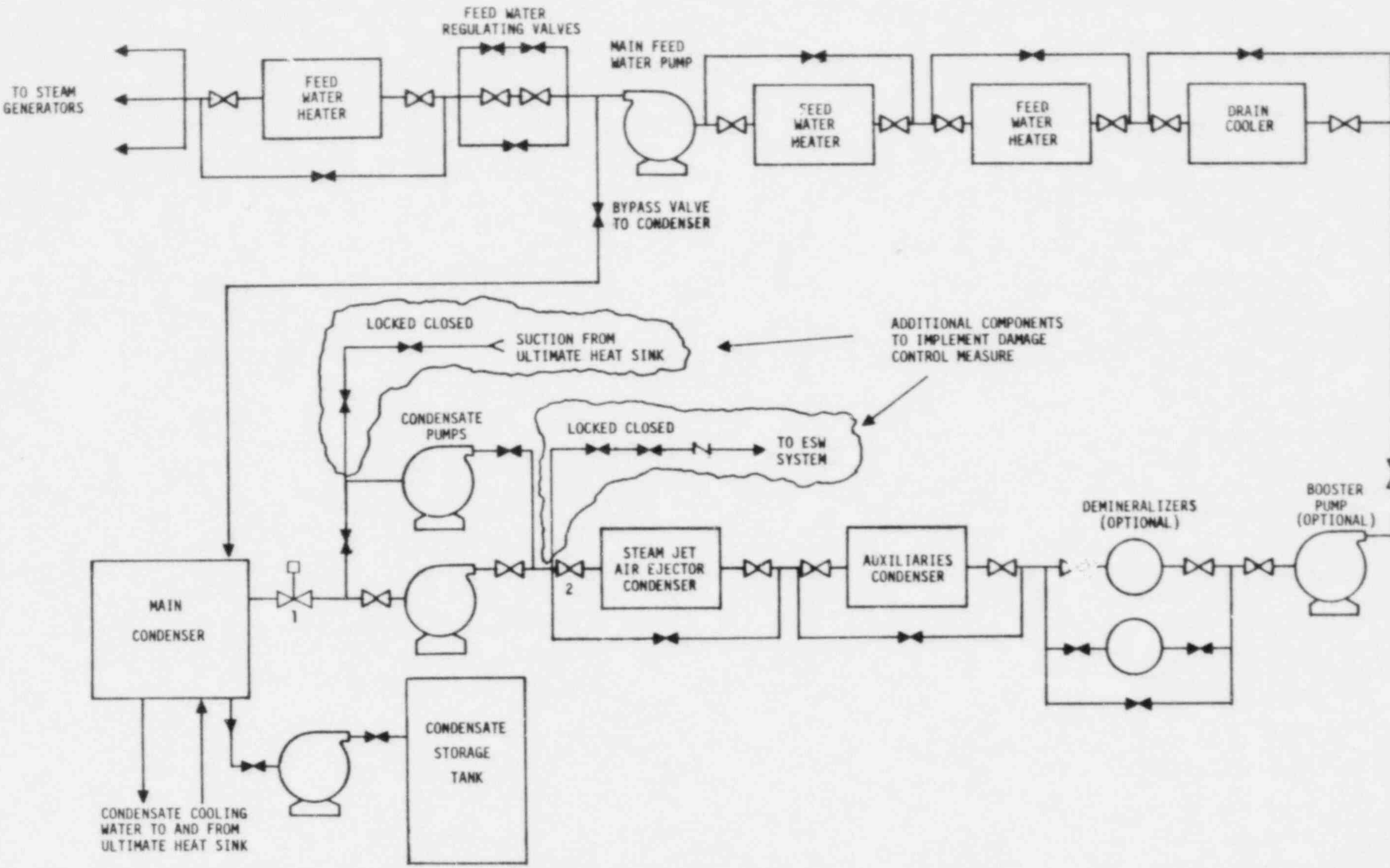


Figure 5.14.1. Representative Main Feedwater System - One of Two Trains.

A common condensate system arrangement has three 50 percent capacity condensate pumps, with a single condensate pump normally aligned in a single feedwater train. The third condensate pump is used essentially as a spare interconnected between the two MFW trains. This arrangement provides flexibility for operating the plant and increases the overall reliability of the MFW system. Condensate pumps in all cases are electrically powered from the normal AC bus system.

Condensate pumps are typically vertical or horizontal multi-stage centrifugal pumps. Representative flow rates are in the range from 6000 to 16000 gpm at several hundred foot discharge head. The condensate pumps take suction from the main condenser hot well with suction pressures on the order of 2 to 10 inches Hg absolute. The condenser vacuum is maintained by steam jet air ejectors. Because the main condenser is cooled by water from the ultimate heat sink, the condensate temperature is normally 10 to 20^{o}F above ambient temperature of the heat sink.

5.14.3 Plant Conditions During Sabotage Scenario

The ESW system is inoperable because of sabotage actions. The CCW system is operating without a heat sink, and therefore is gradually heating up. Being a closed system, the CCW system would pressurize to its relief valve setpoint (e.g., 150 psig). The system can operate in this mode until it heats up to the point where it no longer provided effective component cooling. The power conversion system (main steam, feedwater and condensate and circulating water system) is unavailable due to loss of Nonclass 1E AC power.

5.14.4 System Alignment Necesssary to Restore ESW Flow With A Crossconnected Auxiliary Feedwater Pump

Table 5.14.1 presents a comparison of typical ESW, condensate and AFW pump characteristics. An AFW pump design performance curve is illustrated in Figure 5.14.2. For this pump, maximum (runout) flow is about 1400 gpm. The high head and relatively low flow characteristics of an AFW pump make it an unlikely candidate as a substitute for a low head, high volumetric flow ESW pump. No further consideration will be given to this approach.

Table 5.14.1 Comparison of Typical ESW, Condensate and AFW Pump Characteristics

	ESW Pump	Condensate Pump	AFW Pump
Type	Vertical Turbine	Vertical or Horizontal Multi-Stage Centrifugal	Horizontal Multi-Stage Centrifugal
Flowrate	17,000 gpm	7750 gpm	860 gpm
Design Head	80'	Several hundred feet	2700'
Horsepower	400	Several hundred horsepower	800

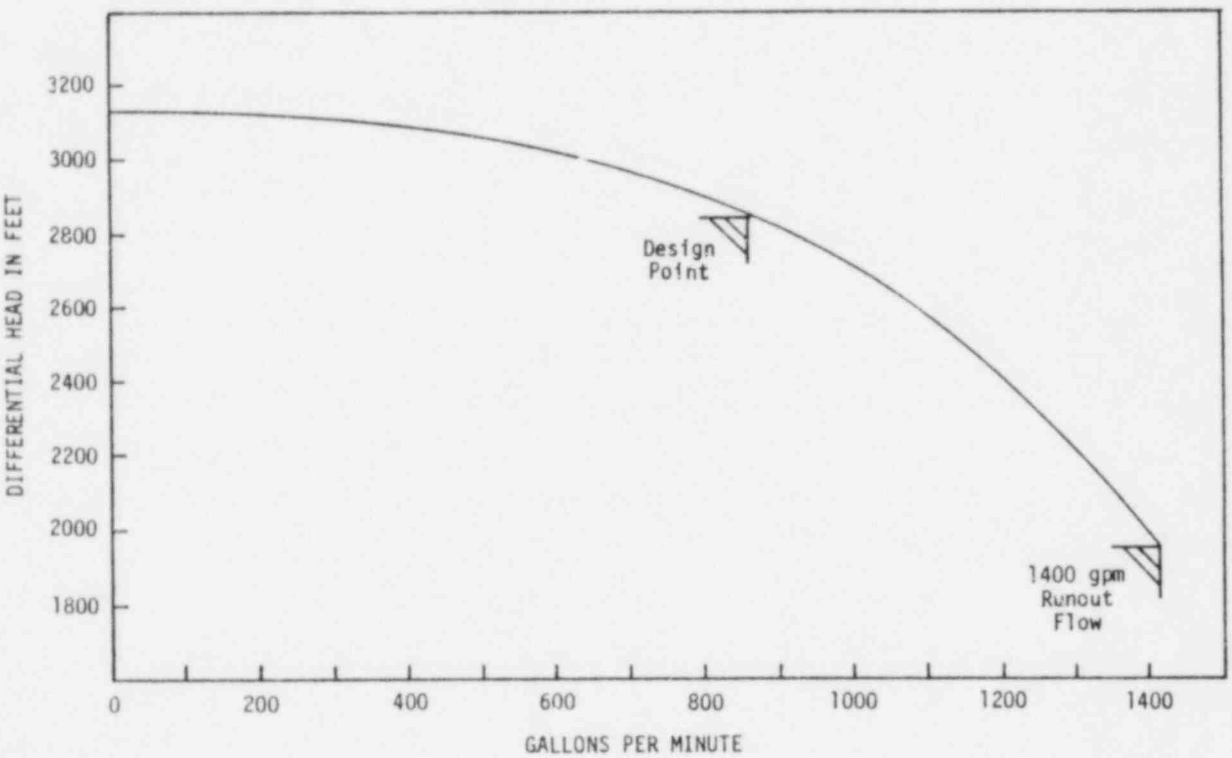


Figure 5.14.2. Typical AFW Pump Design Performance Curve.

5.14.5 System Alignment Necessary To Restore ESW Flow With Crossconnected Condensate Pumps

With the power conversion system unavailable, the condensate pumps are not performing any required functions, unless they are being used to support other damage control measures (e.g., damage control measure #3).

Maximum (runout) flow rate for the condensate pump listed in Table 5.14.1 would likely be 1.4 to 1.6 times its design flow rate (e.g., 10,850 to 12,400 gpm). This is comparable to the ESW flow rate that could be expected when one condensate pump is aligned to supply a single ESW loop. Two condensate pumps could be operated in parallel to meet or exceed the design ESW system flow rate in a single loop. Adequate cooling could thereby be provided to a single CCW heat exchanger. From a safety standpoint, it would be preferable to provide adequate cooling for a single CCW heat exchanger rather than to provide marginal cooling to both.

Piping and valves can be installed to connect the condensate pump suctions to the ultimate heat sink, and the condensate pump discharges to the ESW system as illustrated in Figures 5.1.4.1. The connection with the ESW system would be the same as described in Section 5.13. The crossconnect valves should be normally locked closed to prevent inadvertent contamination of the feedwater and condensate system by poor quality water from the ultimate heat sink. When aligned to provide ESW flow, the condensate pumps would be isolated from the remainder of the feedwater and condensate system by closing the valves in Figure 5.14.1 labeled "1" and "2". Existing piping connections would likely be useable to flush and drain these pumps and piping before restoring normal condensate system lineup.

Electrical power must be restored to the condensate pumps. This can be accomplished by supplying these components with Class 1E power (see damage control measure #19) or with an alternate onsite source of Nonclass 1E power (see damage control measure #25).

Until flow in the ESW system is restored, the CCW system is operating as a passive heat sink and water will be lost from the system once it pressurizes to its relief valve setpoint. When ESW flow is restored, the CCW system will cool and depressurize. Depending on the amount of water lost from relief valve blowdown and on the system surge tank characteristics, the CCW system may depressurize to the point of causing pump cavitation and significant loss of flow in the CCW system. To restore CCW system operation, plant operators could utilize existing system design features to: (1) restore the system surge tanks to their normal water level, (2) repressurize the tanks from their pressure source (e.g., nitrogen system), if necessary, and (3) vent the CCW pumps. This could be a time consuming effort, and would likely require the availability of systems that are not supplied with Class 1E power (e.g., CCW makeup and plant nitrogen systems). Required operator actions can be simplified by making a rapid transition to the use of the condensate pump to reestablish ESW system flow (e.g., before significant CCW system heatup and blowdown).

Design heat transfer capability of a CCW cooling loop is typically in the range from 50 to 130 x 10^6 BTU/hr. For the postulated sabotage scenario, the required heat transfer capability would be much less. None of the LOCA mitigating systems cooled by the CCW system would be operating (e.g., low pressure safety injection pumps, containment spray and cooling system and the RHR heat exchangers). In addition, the control room operator could secure CCW flow to the CVCS letdown heat exchangers and the nonsafety-related components and systems. The major heat load therefore will be the diesel generators, the control room and auxiliary building HVAC system, and, perhaps, a charging pump or high pressure safety injection pump and pump room cooler. These systems and components represent only about 20 to 25 percent of the design heat load on the CCW system. For the purpose of estimating potential CCW system neatup rate without ESW, the following is assumed for each CCW loop: (1) initial heat load of 25 x 10^6 BTU/hr, and (2) initial water volume at 10^5 gallons at an average of 85^{o}F. Under these conditions, initial CCW heatup rate would be approximately 36^{o}F/hr (or 0.6^{o}F/min). Time available to restore ESW flow has not been accurately quantified, but is estimated to be in the range from 30 to 60 minutes.

In some plants, the diesel generator is not served by the CCW system, but instead has its own small-volume closed cooling water system that is cooled by the ESW system (e.g., comparable to the BWR ESW system described in Section 5.13). It has been estimated that this small diesel cooling water system would heat up rapidly after loss of ESW and be at its safety valve setpoint after only five minutes of diesel operation (see Section 5.27). For this type of diesel cooling system, time available to restore ESW flow is very limited.

5.14.6 Technical and Regulatory Impediments to Implementing Damage Control Measure #14

It is technically feasible to install properly sized piping interconnections between the condensate pumps and the ESW system. Depending on the plant layout, this could be a significant pipe run, extending from the turbine building to the ESW pump house, which in some plants is at the site boundary (e.g., adjacent to the ultimate heat sink). The technical impediments to this damage control measure include the following:

- The condensate pumps may not have the required NPSH characteristics to draw water from the plant intake structure. This will likely be a plant-specific consideration that will depend, in part, on the ultimate heat sink characteristics. If required, booster pumps could be added in the new condensate pump suction lines from the ESW intake structure. These pumps could be sized to meet the condensate pump NPSH and flow requirements.

- Periodic testing of this capability may be undesirable because of the contamination of a portion of the condensate system with poor quality water each time the condensate and ESW systems are crossconnected.

The potential regulatory impediments to implementing this damage control measure include the following:

- Any electrical interconnections between the normal AC and the Class 1E distribution systems to support condensate pump operation would require particular attention to assure that the Class 1E system was not degraded because of the interconnection. See damage control measure #19 for additional information.

- The ability to connect the condensate system directly to the ultimate heat sink may introduce significant concerns over secondary system water quality and corrosion effects in the secondary system.

5.14.7 Conclusions and Recommendations Regarding Damage Control Measure #14

This damage control measure appears to be technically feasible, however, only limited time is available to realign the condensate pumps if the ESW system directly supplies the diesel generators. Additional time for operator response is available if the diesel are served by a CCW system or by some indepenent cooling system.

5.15 DAMAGE CONTROL MEASURE #15 - BWR AND PWR

The purpose of damage control measure #15 is to provide cross connections between the fire water system and the essential service water (ESW) system in BWR and PWR plants to provide for heat removal from the safety-related components and systems in the event that the ESW pumps are disabled through sabotage action.

5.15.1 Sabotage Scenario

It is assumed that offsite power is lost coincidentally with successful sabotage of all ESW pumps. Normal AC power is consequently lost and cannot be restored. The emergency diesel generators operate to supply AC power to the Class 1E electrical system.

5.15.2 System Description During Normal Operation

5.15.2.1 Essential Service Water System

See Section 5.13.

5.15.2.2 Fire Water System

A typical fire water system is illustrated in Figure 5.15.1 (from Ref. 1). The system includes one 100 percent capacity diesel engine-driven and two 50 percent capacity electric motor-driven centrifugal fire water pumps. Two small capacity (e.g., 60 gpm) centrifugal jockey pumps maintain the fire mains pressurized at about 125 psig. Fire water pumps typically require a minimum net positive suction head of 9 feet to 12 feet. For an open-loop system such as the fire water system, this NPSH is provided by an elevated water source (e.g., storage tanks or reservoir). Redundant fire water sources are provided, with a minimum capacity of 300,000 gallons each (Ref. 2).

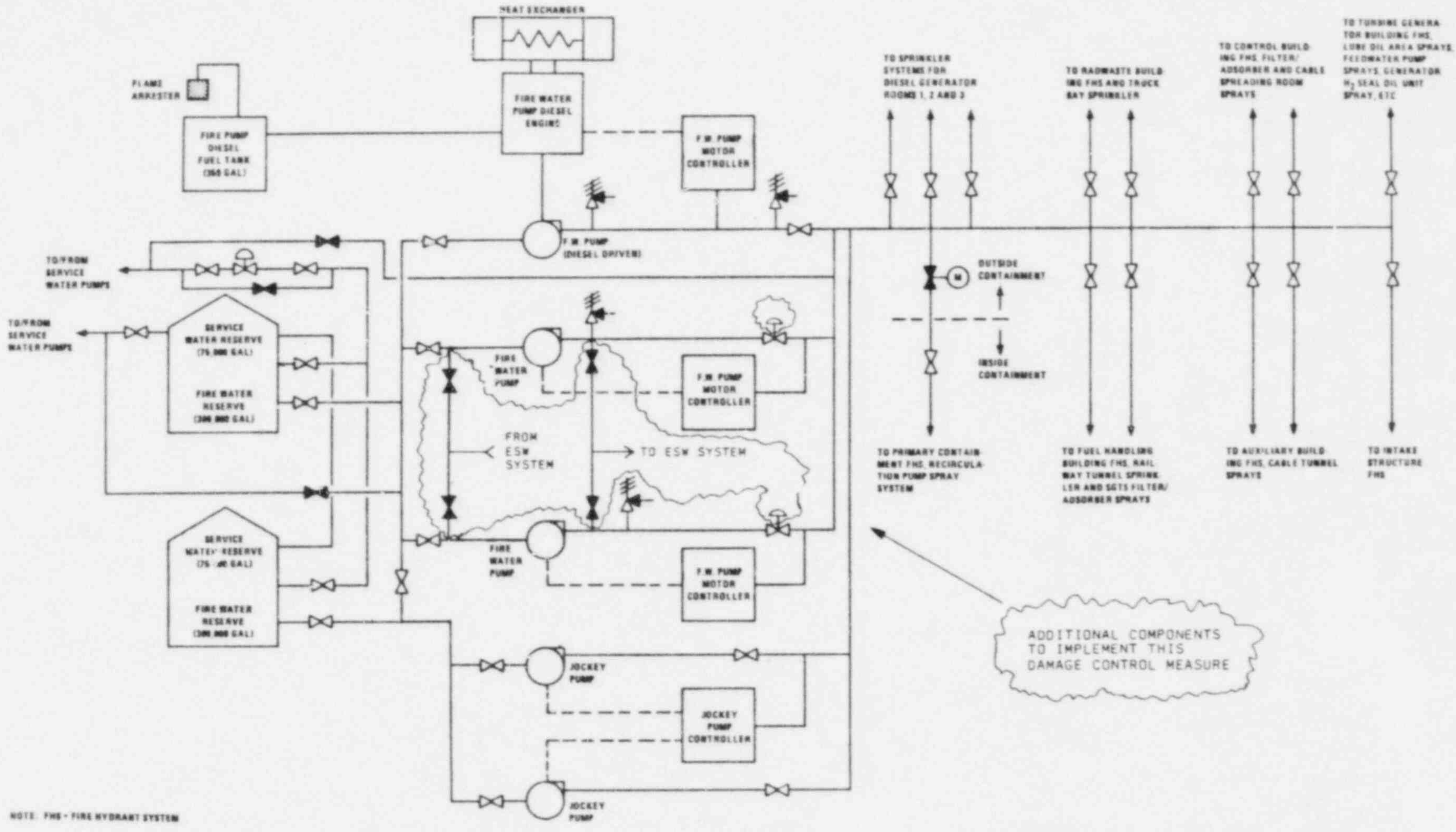


Figure 5.15.1. Typical Fire Water System
(from SAI01379-627LJ)

The fire water system is designed to deliver rated flow following: (1) loss of the largest (e.g., diesel engine-driven) pump, or (2) loss of offsite power. In most nuclear plants, the electric motor-driven pumps are powered from the normal AC system and would not be available following a loss of offsite power. At these plants, the diesel engine-driven pump is designed to be operable following loss of normal AC power. Other fire water system configurations may include two or more Seismic Category I, Class 1E motor-driven pumps powered from redundant Class 1E buses. Loss of offsite power would not affect a system with this configuration.

The fire water system is kept continuously full and pressurized. For the system in Figure 5.15.1, this is accomplished by either one of two jockey pumps which runs continuously. If system pressure drops below a certain level (e.g., about 120 psig), the second jockey pump starts automatically. A continued pressure decrease to about 100 to 105 psig, which may be indicative of a sprinkler system actuation, will automatically start the electric motor-driven pumps. The diesel engine-driven pump will start when system pressure drops further to about 95 psig. Total system flow rate at this time would be about 5620 gpm. At this flow rate, the minimum fire water reserve (e.g., 600,000 gallon) would be exhausted in 1.8 hours. Makeup to the storage tanks in Figure 5.15.1 is provided from a plant service or domestic water system. Typical makeup rates (500 to 1000 gpm) are less than the maximum fire water system pumping capacity.

5.15.3 System Conditions During Sabotage Scenario

The ESW system is inoperable because of sabotage actions. Safety-related components and systems cooled by the ESW system are operating without a heat sink, and therefore are heating up. A closed-loop component cooling water (CCW) system served by the ESW system would pressurize to its relief valve setpoint (e.g., 150 psig). The closed cooling system could operate in this mode until it heated up to the point where it no longer provided effective component cooling.

Nonclass 1E electric motor-driven fire water pumps are unavailable. The diesel engine-driven fire water pump is operable and if the fire water system has Class 1E motor-driven pumps, these are also operable.

5.15.4 System Alignment Necesssary To Restore ESW Flow With Crossconnected Fire Water Pumps

Table 5.15.1 presents a comparison of typical ESW and fire water pump characteristics. The marked disparity of ESW and fire water pump flow rates is readily evident in this table. The maximum flow rate of the fire water system is about 5500 gpm at 280 feet head. When crossconnected to the ESW system, the fire water pumps would likely be operating under runout conditions (e.g., at substanially less than design discharge head), and system flow rate may be on the order of 1.4 to 1.6 times the design flow rate at 280 feet head (e.g., 7200 to 8800 gpm). The system runout flow rate is approximately 50 percent of the flow rate of a single ESW pump. If the motor-driven fire water pumps are supplied from the Nonclass 1E electric system, only the diesel engine-driven fire water pump will be available following loss of offsite power. The diesel engine-driven pump can provide approximately 15 to 25 percent of the flow rate of a single ESW pump. This low flow rate in the ESW system would not be adequate to support the operation of a single ESW loop. Realignment of the diesel fire water pump would also leave the plant without a water fire suppression system.

Electric power could be restored to Nonclass 1E motor-driven fire water pumps. This can be accomplished by supplying these components from the Class 1E power system (see damage control measure #19) or from an alternate onsite source of Nonclass 1E power (see damage control measure #26).

With all fire water pumps in available, a choice must be made regarding the use of these pumps. If one of the fire water pumps were reserved for possible fire protection duties, the remaining two fire water pumps could provide less than 25 percent of the flow rate of a single ESW pump. To transfer the same amount of heat to the ultimate heat sink with this reduced ESW flow rate a proportionate increase in the temperature difference across the components and system heat exchangers cooled by the ESW system is required. Normal temperature rise is 10 to 20^{o}F. At the elevated temperatures resulting from reduced ESW flow, it is doubtful that key components (e.g., diesel generators, large pumps

Table 5.15.1. Comparison of Typical ESW and Fire Water Pump Characteristics

	ESW Pump	Fire Water Pumps Motor-Driven	Diesel Engine-Driven
Type	Vertical Turbine	Horizontal Single-Stage Centrifugal	Horizontal Single-Stage Centrifugal
Flowrate	17,000 gpm	1500 gpm	2500 gpm
Design Head	80'	280 - 290'	280 - 290'
Horsepower	400	<100	<100

and the control room emergency HVAC system) would be capable of continued operation.

Methods for reducing the heat input into the ESW system are discussed in Section 5.13. Using these measures, heat input to a PWR ESW system may be 30 to 40 percent less than during normal power operation. For BWRs, heat input may be greater than during normal power operations because of the need to operate the residual heat removal system for suppression pool cooling or for operation of the reactor core isolation cooling (RCIC) system in the steam condensing mode. It therefore does not appear that effective measures can be taken to reduce the heat input to the ESW system to a point that would permit the fire water pumps to serve as effective replacements for the ESW pumps.

A substantial redesign of the fire water system would be required for it to be useable as a backup for the ESW system. The major changes would entail: (1) increasing selected fire water pump capacity (e.g., a 5 to 10-fold increase of motor-driven pumps), (2) redesigning pumps as necessary to operate with NPSH available from the ultimate heat sink, (3) providing the motor-driven pumps with Class 1E power, (4) increasing system piping sizes to handle the increased flow rate, and (5) providing flow control valves between the motor-driven pumps and the fire water main to modulate flow when these pumps serve in a fire protection role. An alternative to (2), above, is to provide booster pumps in the new fire water pump suction line from the ESW intake structure. These booster pumps could be sized to meet the NPSH and flow requirements of the fire water pumps. The impact of these changes on the fire protection system would have to be evaluated in detail.

With these design changes, the fire water system could be aligned to provide flow in the ESW system, as illustrated in Figure 5.15.1. The connection with the ESW system would be the same as used in damage control measure #13. With this system realignment, the diesel engine-driven fire water pump and the jockey pumps are still available for fire protection service.

Leaving the fire water pumps aligned to their normal water source is not considered to be a viable alternative when the system is crossconnected to the ESW system. The increased fire water pump capacity would rapidly deplete the available onsite water sources and leave the plant without a source of fire water, without a backup source of water for reactor core cooling (e.g., for PWR auxiliary feedwater systems and BWR isolation condenser systems), and without further ESW cooling.

Even if ESW flow can be adequately restored by the modified fire water system, there will still be a variety of operational problems associated with the CCW system in PWR plants. These problems are discussed in the evaluation of damage control measure #14.

5.15.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #15

There are many obvious technical problems associated with attempting to restore ESW flow by crossconnecting with the fire water system. Without significant system redesign, it is doubtful that a fire water system could serve in the role postulated in this damage control measure. In addition to these technical problems, there are regulatory impediments that also need to be considered.

USNRC Standard Review Plan 9.5.1 (Ref. 2) requires that "the fire main system piping should be separate from service or sanitary water system piping," except when necessary to provide fire water to standpipes and hose connections for manual fire fighting in areas containing equipment required for safe plant shutdown in the event of a Safe Shutdown Earthquake (SSE). The reason for this exception is to allow for system crossconnections which provide fire water from a Seismic Category 1 system to the fire water system. Use of a significant portion of the pumping capacity of the fire water system as a substitute for the ESW pumps conflicts with the guidance in SRP 9.5.1.

The NRC does allow the fire water system to serve as a backup water source for some safety-related systems such as: (1) PWR auxiliary feedwater system and (2) BWR isolation condenser system. In these cases, required makeup rates from the fire water system are in the order of several hundred gallons per minute; a fraction of the system pumping capacity. Use of the fire water system as proposed in this damage control measure could eliminate the fire water system as a backup water source for core cooling purposes.

Any electrical interconnections between the normal AC and the Class 1E distribution system would require particular attention to assure that the Class 1E system was not degraded because of the interconnection. See damage control measure #19 for additional information.

5.15.6 Conclusions and Recommendations Regarding Damage Control Measure #15

Without substantial upgrade, it is unlikely that the firewater system could serve as an effective replacement for the ESW pumps. Significant regulatory concerns exist if the capacity of the entire firewater system is required for this purpose. Only limited time is available to restore ESW flow if that system provides direct diesel generator cooling. This operational constraint may further limit the practicality of this damage control measure.

5.15.7 Section 5.15 References

1. "Lobner, P., et al., "The Boiling Water Reactor - A Review of a Typical General Electric BWR/6 Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

2. USNRC Standard Review Plan 9.5.1, "Fire Protection Program," NUREG-0800, U. S. Nuclear Regulatory Commission, July 1981.

3. "238 Nuclear Steam Supply System-GESSAR," Docket STN-50550, General Electric Company.

4. Ericson, D. M. and Varnado, G.B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

5.16 DAMAGE CONTROL MEASURE #16 - PWR

The purpose of a damage control measure #16 is to use the essential service water (ESW) system to supply water directly to components cooled by the component cooling water (CCW) system in the event that the CCW system pumps are inoperable because of sabotage action.

5.16.1 Sabotage Scenario

Loss of offsite power occurs and the main turbine generator trips on loss of load. The emergency diesel generators operate to supply AC power to the Class 1E buses. The CCW pumps have been sabotaged. Other components of the component cooling water system remain operable.

5.16.2 System Descriptions

5.16.2.1 Essential Service Water System

See Section 5.13.

5.16.2.2 Component Cooling Water System

A component cooling water (CCW) system forms an intermediate heat transfer loop between selected plant systems and components and an essential service water (ESW) system. Representative PWR systems and components that may be served by a CCW system are listed in Section 5.13. Note that diesels are not always supplied by a CCW system. In some plants, diesel cooling is provided directly by the ESW system. Other plants may provide an independent diesel cooling system such as a water-to-air radiator. In these plants, the heat loads on the CCW system are significantly reduced.

An example of a CCW system is illustrated in Figure 5.16.1. This system has two independent, critical cooling loops, A and B, which serve safety-related components. In addition there is a noncritical cooling loop, which is supplied by either CCW loop, to serve nonsafety-related components.

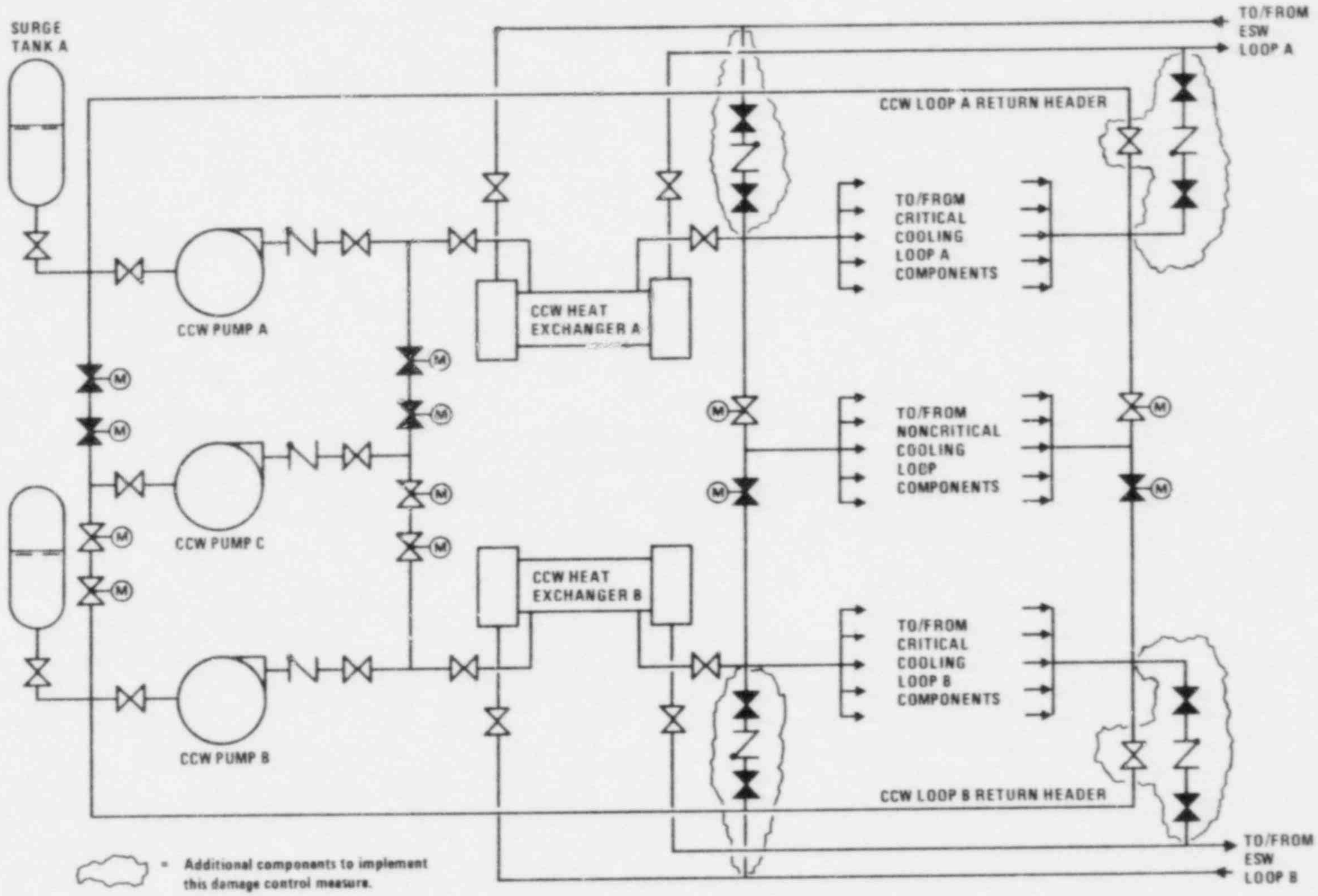


Figure 5.16.1. Component Cooling Water System.

During normal operation, a single CCW pump is operating to supply cooling water to the noncritical loop and any operating components in the associated critical loop. The other CCW loop is in standby. During emergencies, the noncritical loop is automatically isolated and the standby CCW loop is placed in operation. If necessary, CCW flow can be manually restored to components in the noncritical loop following automatic isolation.

A third CCW pump (pump C in Figure 5.16.1) serves as an installed spare that can be aligned to replace either pump A or pump B. CCW pump C is considered to be a third-of-a-kind load and its electric power supply and other auxiliaries (e.g., room cooling, control power and actuation) can be selected to be the same as the pump which is being replaced.

The CCW system is powered from the Class 1E electrical system and is automatically actuated by an Engineered Safety Feature Actuation System.

Relatively small diameter piping directs cooling water from CCW headers to the individual components. Line sizes range from 1.5 to 3 inches for safety-related pumps, up to 8 to 12 inches for large heat exchangers (e.g., shutdown cooling, CVCS letdown, or containment emergency coolers). The CCW system is supplied with makeup water from a high quality source such as a demineralized water system. There are usually no filters or strainers in the CCW system piping.

5.16.3 System Conditions During Sabotage Scenario

The CCW system pumps are inoperable because of sabotage actions and there is no flow in the CCW system. Components served by the CCW system are heating up. The most critical components will most likely be the diesel generators (if served by the CCW system). Some large safety-related pumps in operation following loss of offsite power (e.g., auxiliary feedwater and ESW pumps) are cooled by water diverted from their own discharge and are not limited directly by the unavailability of the CCW system. All motor-driven pumps and other AC-powered equipment will be unavailable if the diesel generators fail due to inadequate cooling. Only about five minutes are available to restore CCW cooling water flow if this system provides cooling for diesel generators (see Section 5.27).

5.16.4 System Alignment Necessary to Restore CCW Flow with a Crossconnected ESW Pump

Table 5.16.1 presents a comparison of typical ESW and CCW pumps characteristics. Flow rates are roughly comparable, however, the discharge head of the ESW pump is somewhat less than that of the CCW pump.

The ESW system could be aligned to provide direct cooling to components served by the CCW system. The required crossconnections, illustrated in Figure 5.16.1, include series isolation valves that are normally locked closed to preclude inadvertent contamination of the CCW system with lower quality essential service water. The alternate cooling water path to individual components is established by: (1) shutting the heat exchanger CCW outlet valves and the new CCW return header isolation valves, (2) shutting the heat exchanger ESW supply or return line isolation valve, and (3) opening the series manual valves in the ESW/CCW crossconnect supply and return lines. Cooling water from the ESW system then can flow directly to the CCW supply header, to the components requiring cooling and finally back to the ESW outfall (return) line. Much of the CCW system has been isolated (e.g., the pumps, heat exchanger, the noncritical loop and the CCW return headers) thereby minimizing the flushing and cleanup requirements following use of the ESW system in this crossconnected configuration.

Many of the components served by the CCW system are located at or near grade level (e.g., safety-related pumps, shutdown heat exchanger) and would be cooled adequately by the crossconnected ESW system. Some components, however, may be located at a high elevation in the plant with respect to the elevation of the ESW pumps (e.g., containment fan cooler units). The capability of providing alternate cooling water to such components using the ESW system is limited by the shutoff head of the ESW pumps. The adequacy of cooling for such components must be evaluated on an individual case basis. If necessary, ESW pumps could be replaced with units having a higher shutoff head.

Table 5.16.1. Comparison of Typical ESW and CCW Pump Characteristics.

	ESW Pump	CCW Pump
Type	Vertical Turbine	Horizontal Single-Stage Centrifugal
Flowrate	17,000 gpm	14,000 gpm
Design Head	80 feet	140 feet
Horsepower	400	600

Depending on the nature of the ultimate heat sink, the quality of the essential service water may range from reasonably good quality cooling pond or cooling tower water to highly saline ocean water. The potential effects of essential service water use in the CCW system must be considered on an individual plant basis. Of particular concern is the introduction of salt water into stainless steel systems and the blockage of small diameter CCW piping by foreign material that passes through the ESW trash screens from ocean, lake or river sources.

A radiation monitoring capability (e.g., gross gamma monitoring) should be provided in the crossconnect line between the CCW system and the ESW return header to detect any leakage from the shutdown cooling or letdown heat exchangers.

5.16.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #16

Use of essential service water in the CCW system may have an adverse effect on the CCW system by accelerating general corrosion, causing certain types of localized corrosion that are not normally encountered in the CCW system (e.g., chloride stress corrosion), or plugging small diameter piping with foreign material. Adequate flushing and inspection programs following use of service water in the CCW system must be developed, commensurate with service water quality.

5.16.6 Conclusions and Recommendations Regarding Damage Control Measure #16

This damage control measure appears to be technically feasible. If the diesels are served by the CCW system, only limited time is available to implement this measure. Additional time for operator action would be available if the diesels are not cooled by the CCW system.

5.17 DAMAGE CONTROL MEASURE #17 - PWR

The purpose of damage control measure #17 is to provide local pressurizer and steam generator water level indication in the event that all normal level indication has been disabled through sabotage action.

5.17.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with successful sabotage of the instrumentation which provides indication of pressurizer and steam generator water level to the control room or to other remote locations. With the loss of offsite power, reactor core cooling is accomplished by the auxiliary feedwater (AFW) system and reactor coolant inventory control is accomplished by the charging system or high pressure safety injection (HPSI) system. Because of the loss of key instrumentation through sabotage actions, it may be difficult to assess the safety status of the plant and to properly operate the AFW, HPSI and charging systems.

5.17.2 Description of Steam Generator and Pressurizer Level Instrumentation

PWR plants may have two, three or four steam generators but only one pressurizer. Steam generator and pressurizer level indications are derived from differential pressure sensor/transmitter units located inside containment. Signal cables from these units pass through containment electrical penetrations and are connected to a variety of safety, and nonsafety-related instrumentation and control systems as described below.

5.17.2.1 Steam Generator Level Instrumentation

Safety-related steam generator level instrumentation may provide inputs to the following:

- Reactor Protection System (for reactor trip on steam generator low level)

- Auxiliary Feedwater System (automatic actuation logic)

- Safety-related display instrumentation in the control room and other locations (analog meters, recorders, high/low level alarms)

There are typically three to six independent safety-related channels monitoring steam generator water level (e.g., three or four narrow range channels plus two wide range channels). Level indication is available for each channel. The RPS and AFW actuation logic both use coincidence logic to compare multiple steam generator water level channels and determine the need for protective actions. Each narrow range channel has an independent sensor/transmitter unit that is powered from an independent Class 1E electrical division (e.g., 125 VDC or 120 VAC). Physical separation is maintained between the sensor/transmitter units and sensing lines to ensure that a single event (e.g., pipe break inside containment) does not disable all level indication. Physical and electrical separation of the signal cables, signal processing equipment and power supplies is also maintained. Similar separation is maintained between the wide range channels, if provided.

The safety-related logic systems (e.g., the RPS) that monitor steam generator level may provide an output to nonsafety-related systems by means of suitable isolation devices (e.g., optical isolators or isolation amplifiers). These signals typically are derived from two-out-of-three or two-out-of-four output logic, and are used to initiate main turbine trip, main feedwater pump trip and feedwater valve closure if a high-high water level condition exists in a steam generator.

The feedwater control system also monitors steam generator level. The level signal origin for this control system is different than that which is used to generate the low level reactor trip. Typically, the feedwater control system utilizes a single nonsafety-related instrument channel. Indication of the level of each steam generator is usually provided at the feedwater control panel.

5.17.2.2 Pressurizer level Instrumentation

Safety-related pressurizer level instrumentation may provide inputs to the following:

- Reactor Protection System (high-pressurizer level trip)
- Safety-related display instrumentation in the control room and other locations (analog meters, recorders, high/low level alarms)

There are typically three independent safety-related channels monitoring pressurizer level. Level indication is available for each channel. Each channel is physically and electrically separated as described previously. Pressurizer level information may be provided to nonsafety-related instrumentation and control systems via suitable isolation devices (e.g., optical isolators or isolation amplifiers). Nonsafety-related systems that require pressurizer level information include the following:

- Pressurizer Heater Control System (low level interlock for heater protection)
- Chemical and Volume Control System (for automatic control of charging pumps and letdown line flow)

5.17.3 System Conditions During Sabotage Scenario

The plant is in a post-accident condition without some primary indications required for the operator to assess the adequacy of core cooling and coolant inventory control. The impact of the loss of level instrumentation on associated control systems may vary, depending on the details of level instrument and control system design.

If the pressurizer level instruments are sabotaged in a manner that causes the indication to fail low, the pressurizer heaters would be deenergized by their control system. Pressurizer heaters will likely be required for maintaining primary coolant system pressure control at some time during the post-accident sequence. It will not be possible to remotely reenergize these heaters without first bypassing the low pressurizer level interlock provided for heater protection. Local operation of the heaters at their electrical switchgear is not affected by the low pressurizer level interlock.

If steam generator level instruments are sabotaged such that the indications fail high, the main turbine and main feedwater pump will trip, the main feedwater control valves will close, and the auxiliary feedwater system will not automatically start. Remote-manual AFW system actuation can still be accomplished.

Rapidly disabling all steam generator and pressurizer level indication would not be accomplished by sabotaging the sensor/transmitter units inside containment. The specific sabotage actions may entail disabling the station batteries (Class 1E and Nonclass 1E), major instrument cable runs or instrument cabinets. Such actions will likely affect far more than just the level instrumentation.

5.17.4 Level Indication System Alterations to Provide Local Indication of Steam Generator and Pressurizer Level

There are three basic approaches that can be taken for providing a capability to determine steam generator and pressurizer level when all normal indication has been disabled. These approaches are: (1) provide level gauges inside containment, (2) provide level gauges outside containment, or (3) provide portable, self-powered, calibrated level instruments that can be connected to signal cables from selected level transmitters. Each approach will be described separately below.

5.17.4.1 Level Gauges Inside Containment

Level transmitters with local gauge indicators, similar to the Yarway transmitters used in BWR plants (see Figure 5.17.1, from Ref. 1), or simple level gauges could be provided at some suitable location inside containment. If possible, location of these gauges in the immediate vicinity of an airlock may permit an operator to read the instruments through an airlock view port, without actually having to enter containment. Auxiliary lighting may be required to enable an operator to read the gauges in a darkened containment.

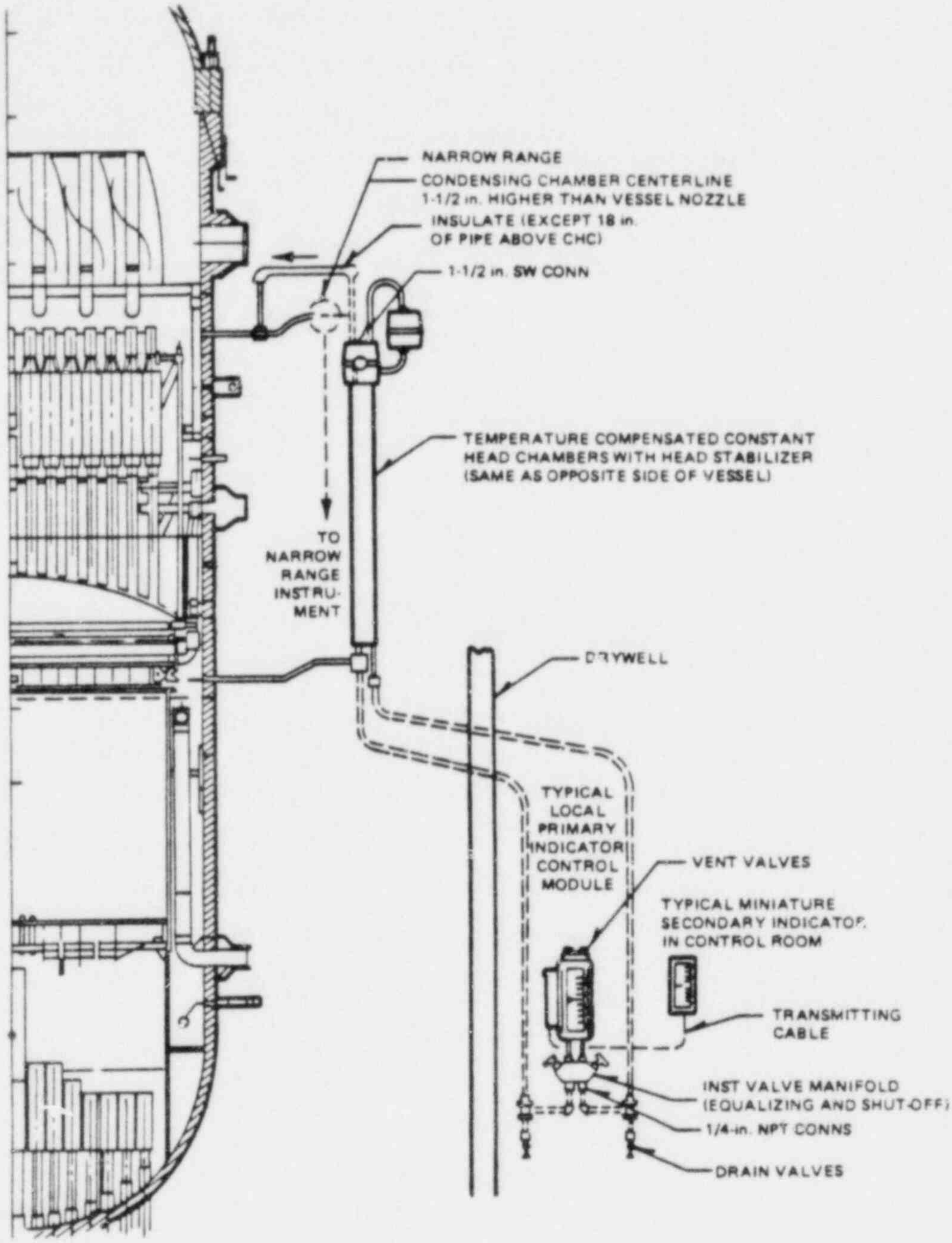


Figure 5.17.1. Typical 210 Inch Yarway Piping Arrangement (From NUREG-0626).

The instrument piping typically is sloped down from the steam generators and pressurizer to the level sensors. This is necessary to avoid traps for noncondensable gases and to provide for simple high point venting of the water-filled instrument sensing lines. The elevation of the main airlock (e.g., at the operating floor level) with respect to the lower sensing line taps on the steam generators and pressurizer may preclude locating the gauges near the main airlock. The need for providing missile and jet impingement protection for the new sensing lines and gauges should be considered.

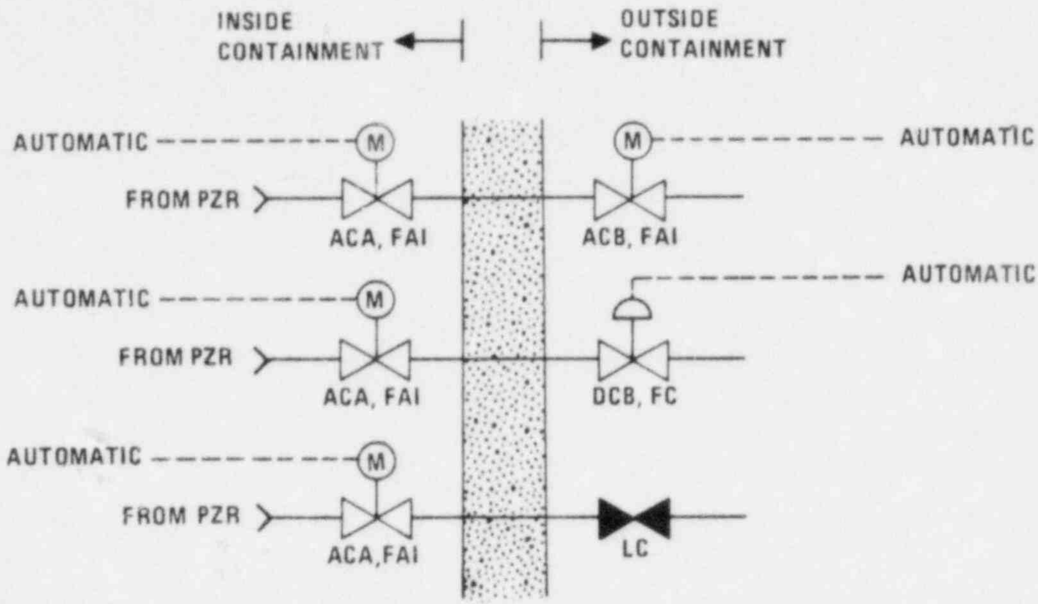
The normal radiological controls typically implemented during containment entry when the plant is at power (e.g., essentially the formation of a two-person team) would likely provide adequate protection against sabotage for the new level gauges.

5.17.4.2 Level Gauges Outside Containment

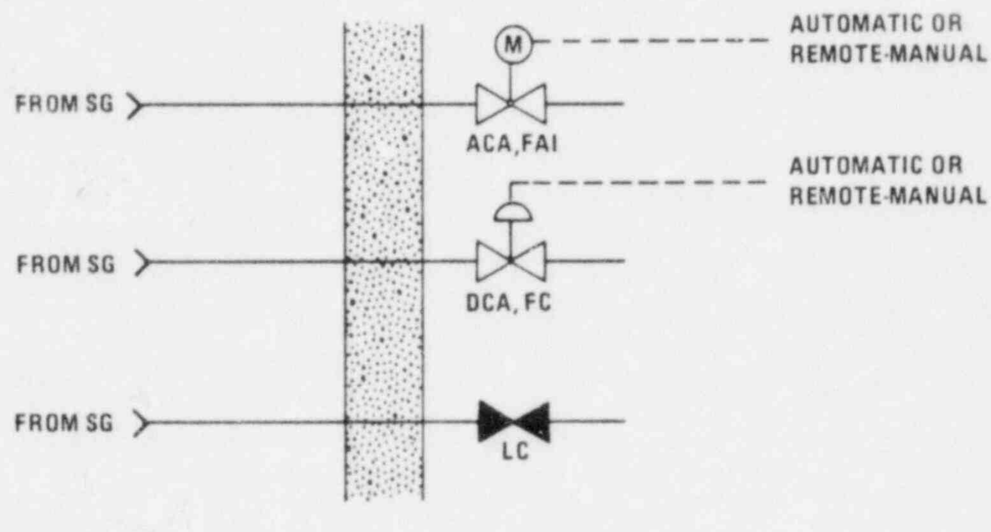
Level transmitters with local gauge indicators, or simple level gauges could be provided outside containment. Because of containment isolation requirements for the instrument sensing lines, the design requirements for this approach are more complex than if the gauges remained inside containment. The benefit of placing the gauges outside containment is a higher assurance that the gauges will be accessible when required. Communications with other plant personnel also may be simplified.

The pressurizer level instrument sensing lines are part of the reactor coolant pressure boundary and are subject to the basic containment isolation requirements of NRC General Design Criterion 55 (Ref. 2). Three possible sensing line isolation valve arrangements suitable for a pressurizer level instrument are illustrated in Figure 5.17.2. If the pressurizer level gauge is to be normally on-line and available with a minimum of effort, the first isolation valve arrangement in Figure 5.17.2 would be the likely choice (e.g., two motor-operated valves, one inside and one outside containment).

The steam generator level instrument sensing lines are part of a closed secondary coolant system and are subject to the basic containment isolation requirements of NRC General Design Criterion 57 (Ref. 3). Three possible sensing



PRESSURIZER LEVEL INSTRUMENT LINES



STEAM GENERATOR LEVEL INSTRUMENT LINES

NOTES: (1) VALVE POWER SOURCES ARE IDENTIFIED BY AC OR DC POWER AND BY ELECTRICAL DIVISION (A OR B).

(2) VALVE FAILURE MODES ARE LISTED AS FOLLOWS:
FAI = FAIL AS-IS; FC = FAIL CLOSED; LC = LOCKED CLOSED.

(3) VALVE ACTUATION IS LISTED AS AUTOMATIC (e.g., BY A CONTAINMENT ISOLATION SYSTEM) OR REMOTE-MANUAL (e.g., BY A CONTROL ROOM HAND SWITCH).

Figure 5.17.2. Examples of Containment Isolation Provisions for Instrument Lines.

line isolation valve arrangements for this level instrument are also illustrated in Figure 5.17.2. If the steam generator level gauge is to be normally on-line, and available with a minimum of effort, the first isolation valve arrangement in Figure 5.17.2 would be the likely choice (e.g., a single motor-operated valve outside containment).

The sensing lines for these new gauges may require missile and jet impingement protection inside containment. Physical protection for the new gauges outside containment would be required.

5.17.4.3 Portable, Self-Powered, Calibrated Level Instruments

Portable, calibrated level instrument packages with self-contained DC power supplies and appropriate leads could be connected to steam generator and pressurizer sensor terminals in instrumentation cabinets or control boards. These packages would simulate the normal instrument power supply and signal processing circuitry. Depending on the location of the instrument cabinets (many are located in the vicinity of the control room), it may be possible to use long leads and place the level instrument packages at some convenient location remote from the instrument cabinets (e.g., in the control room). Sabotage of the sensor/transmitter units, sensing lines, or signal cables would render this method ineffective. Only the signal cables are vulnerable outside containment, and would therefore require physical protection.

5.17.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #17

Containment entry with the plant in a post-accident condition may involve significant hazard to personnel and is likely to run contrary to plant radiological health programs. Furthermore, the time required to adequately prepare for a containment entry would not be compatible with the need to restore steam generator and pressurizer level indication in a timely manner. These considerations may be significant impediments for implementation of Approach 1.

There are no technical or regulatory impediments to Approaches 2 or 3.

5.17.6 Conclusions and Recommendations Regarding Damage Control Measures #17

If the required level gauges cannot be placed inside containment in a location readily visible from an airlock viewing port, Approach 1 would not be a viable alternative for locally monitoring steam generator and pressurizer level.

Approach 2 may require new containment penetrations and interfaces with the containment isolation and Class 1E power systems. It is therefore likely to be the most costly to implement.

Approach 3 is the simplest to implement. The relatively large number of steam generator and pressurizer level transmitters should provide a high level of assurance that a basic level monitoring capability can be reestablished with this technique.

5.17.7 Section 5.17 References

1. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

2. 10CFR50, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 55, "Reactor Coolant Pressure Boundary Penetrating Containment."

3. 10CFR50, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 57, "Closed System Isolation Valves."

5.18 DAMAGE CONTROL MEASURE #18 - PWR

The purpose of damage control measure #18 is to provide local readouts for steam generator pressure when this indication is lost in the control room and at the emergency shutdown panel because of sabotage action.

5.18.1 Sabotage Scenario

It is assumed that offsite power is lost. Instrumentation systems, receiving Class 1E power, such as the reactor protection system (RPS), engineered safety feature actuation system (ESFAS), and safety-related display instrumentation, function normally except that all steam generator pressure indication and indication of main steam line pressure on the steam generator side of the main steam isolation valves (MSIVs) has been disabled by sabotage action.

5.18.2 Description of Steam Generator Pressure Indication

Typical steam generator pressure instrumentation is illustrated in Figure 5.18.1. Sensors and transmitters for directly measuring steam generator pressure are located inside containment. A signal cable penetrating containment provides the necessary communication link with instrumentation systems (e.g., RPS, ESFAS), indicators, recorders and the plant computer system, and with the DC power supply for the sensor channel. Other pressure sensors monitor main steam line pressure and are located outside the containment, but before the MSIVs. These sensors would also provide a good indication of steam generator pressure.

A typical pressure sensor is illustrated in Figure 5.18.2 (from Ref. 1). Installation details for this sensor are shown in Figure 5.18.3 (from Ref. 1).

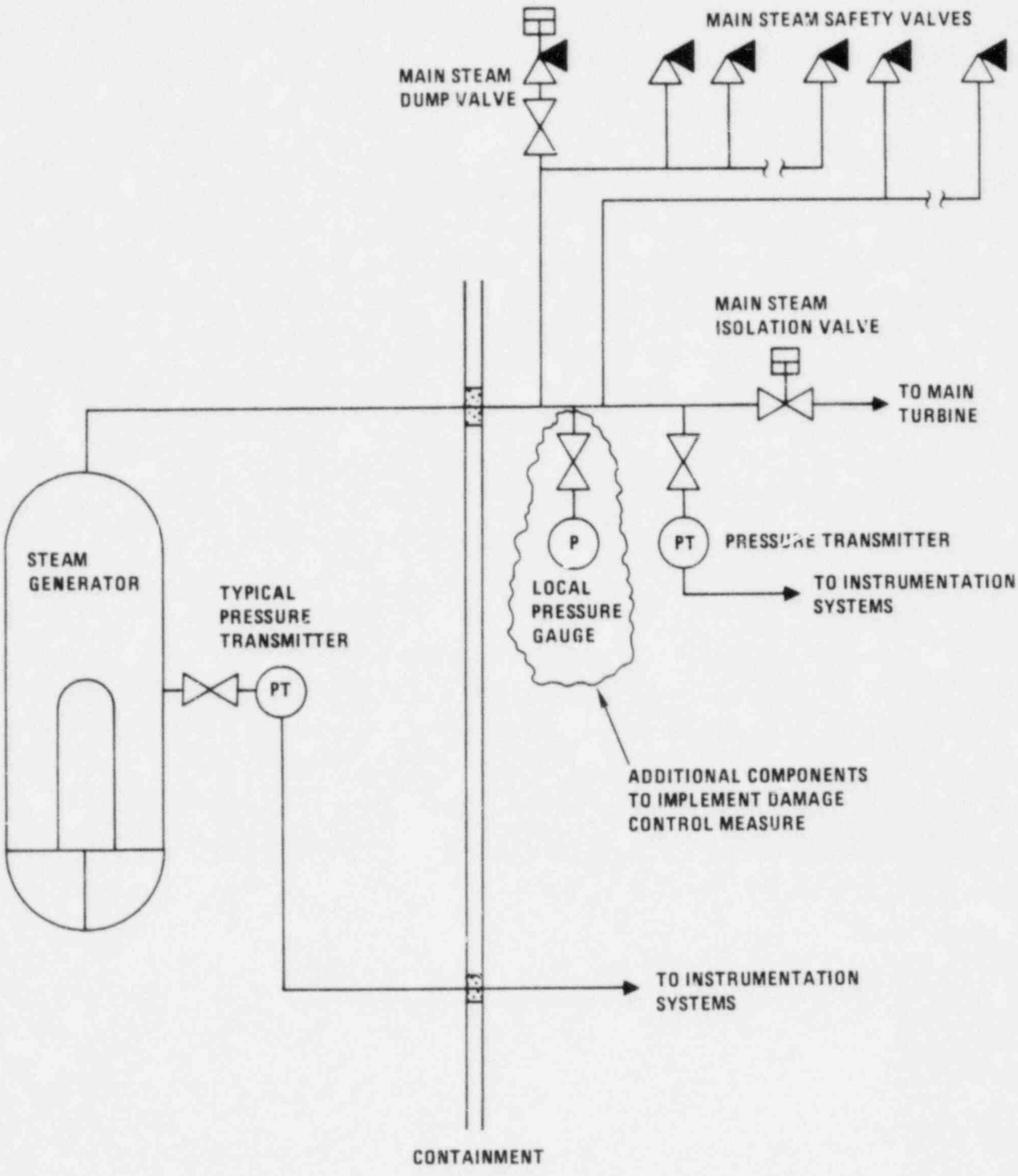


Figure 5.18.1. Typical Steam Generator Pressure Instrumentation.

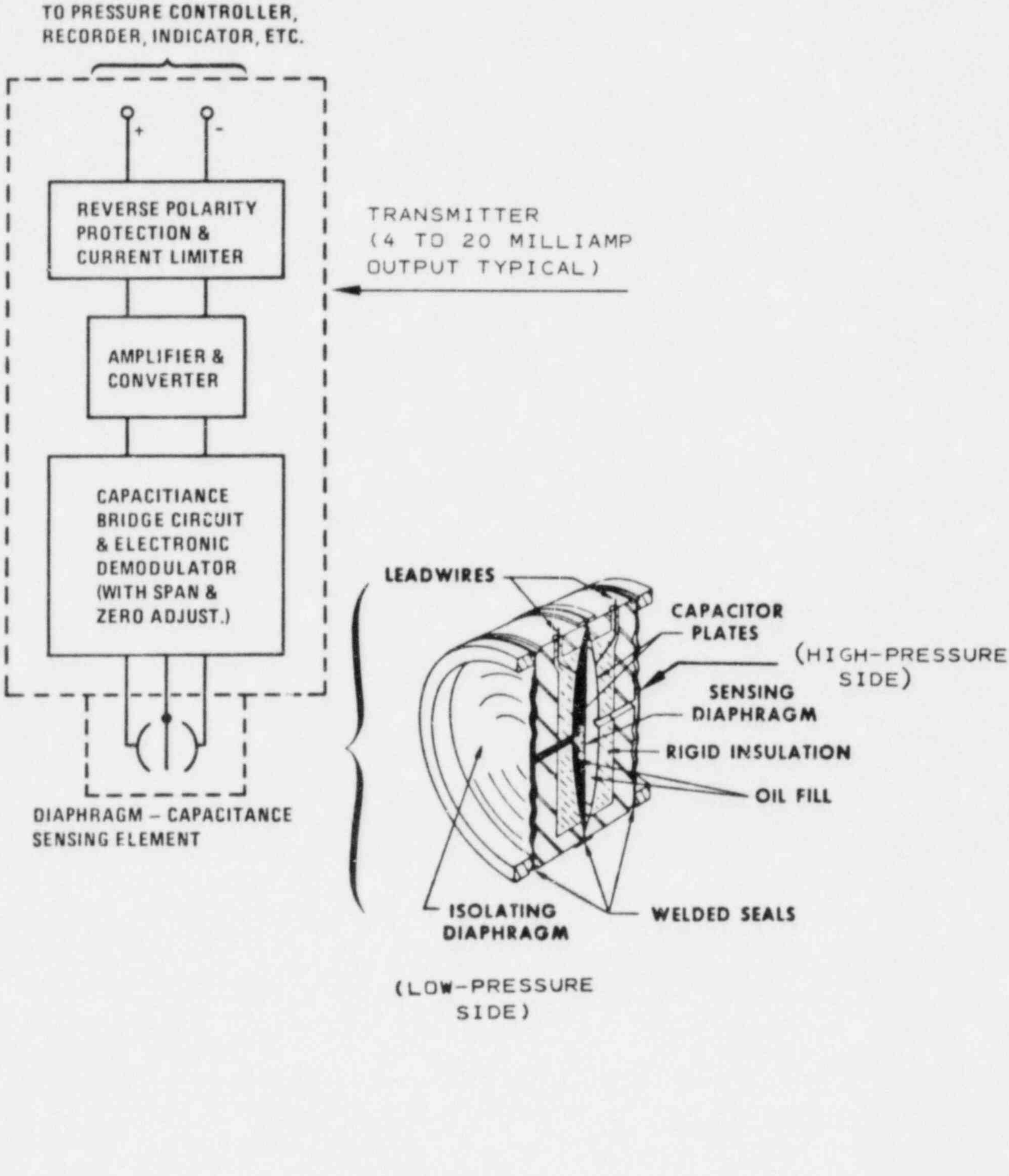


Figure 5.18.2. Typical Pressure Sensor and Transmitter Circuit, With Detail of Diaphragm-Capacitance Sensing Element (from SAI01379-585LJ).

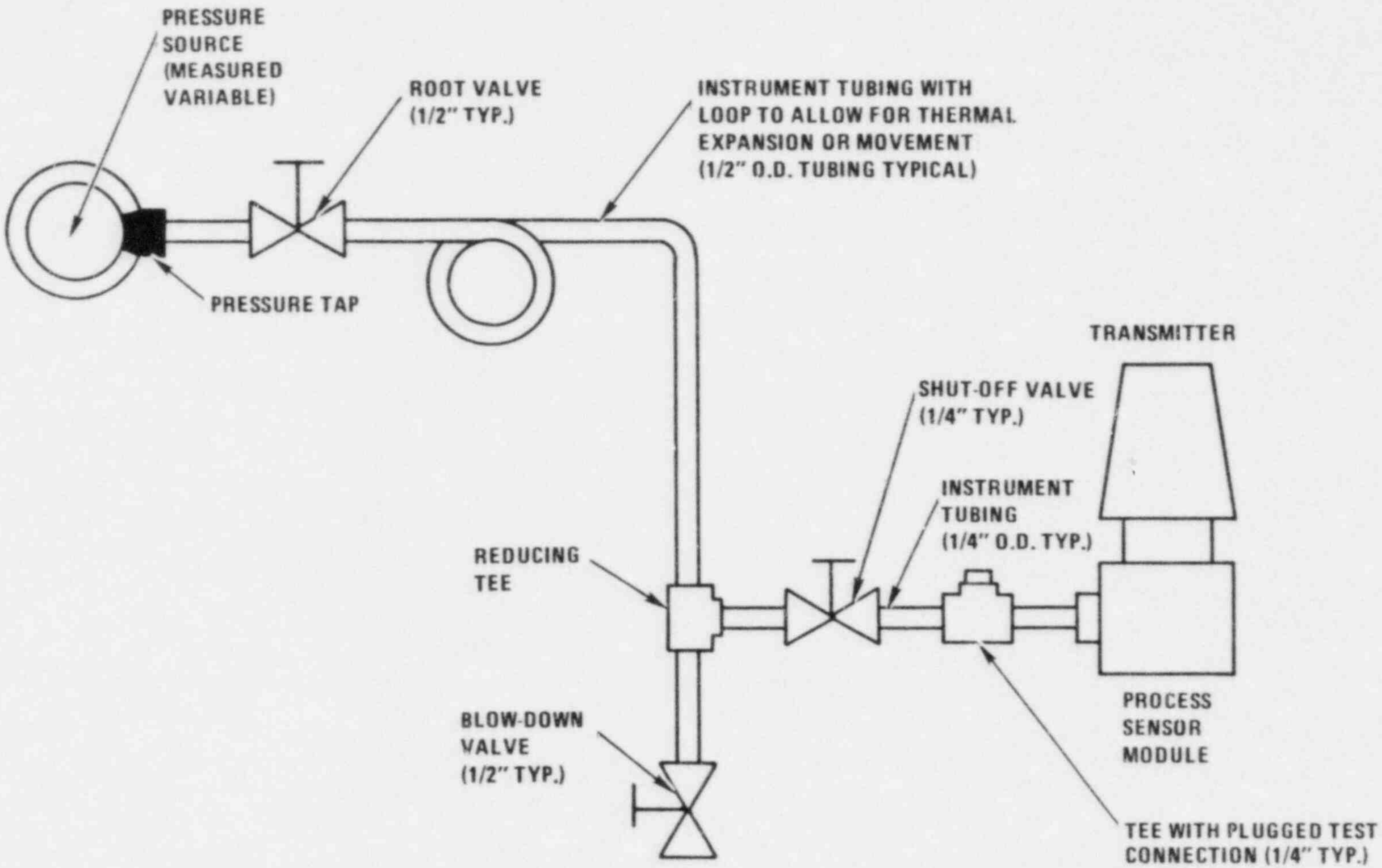


Figure 5.18.3. Typical Pressure Sensor and Transmitter Installation Details (from SAI01379-585LJ).

5.18.3 Plant Conditions During Sabotage Scenario

The plant is in a post-accident phase following some initiating event. All steam generator pressure indication and indication of main steam line pressure on the steam generator side of the MSIVs has been lost due to sabotage action.

5.18.4 Measures For Providing Local Indication of Steam Generator Pressure

There are four basic approaches for providing local indication of steam generator pressure. These include the following:

A. Replace existing main steam line sensor/transmitter units with a sensor/transmitter unit with a local indicator gauge. A unit of this type is illustrated in Figure 5.18.4 (from Ref. 1). Sabotage of the main steam line sensor/transmitter units, the sensing lines or the valves in the instrument lines would also render this method ineffective. Physical protection of these items would be necessary.

B. Provide a portable calibrated gauge that can be connected to a pressure sensing line (e.g., at the blowdown valve in Figure 5.18.3) for a main steam line pressure sensor. A disabled sensor/transmitter unit could be isolated by closing its shut-off valve. Sabotage of the sensing line (e.g, crimping) or the root valve (e.g., disabled closed) would also render this method ineffective. Physical protection of these items would be necessary.

C. Provide a portable, calibrated pressure instrument package with a self-contained DC power supply and appropriate leads that can be connected to steam generator or main steam line pressure sensor terminals in instrumentation cabinets or control boards. This package would simulate the normal instrument power supply and signal processing circuitry. Depending on the location of the instrument cabinets (many are located in the vicinity of the control room) it may be possible to use long leads and place the portable pressure instrument package at some convenient location remote from the instrument cabinets (e.g., in the control room). Sabotage of the sensor/transmitter units, sensing lines, isolation valves or signal cables would render this method ineffective. Physical protection of these items would be required.

D. Install separate local pressure gauges to measure main steam line pressure as illustrated in Figure 5.18.1. Physical protection of the gauge and associated sensing line and isolation valves would be necessary.

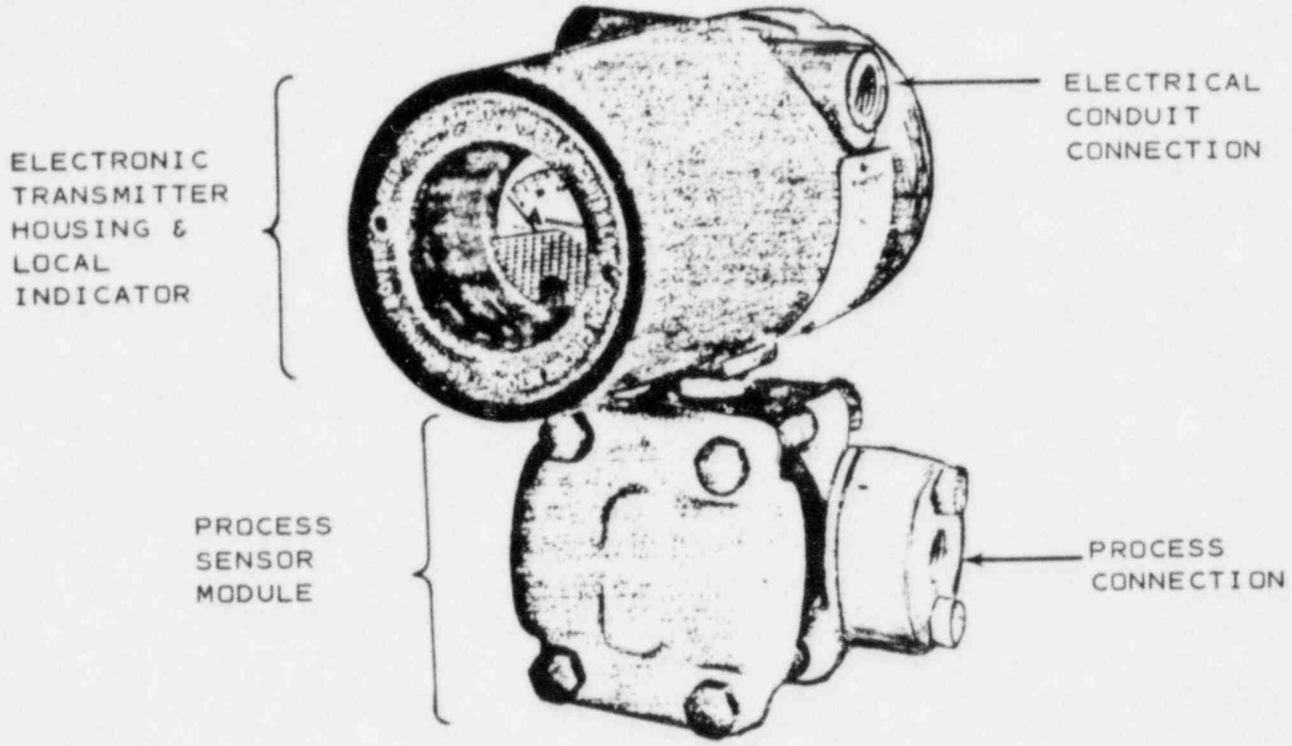


Figure 5.18.4. Typical Pressure Sensor and Electronic Transmitter (with Local Indicator) (from SAI01379-585LJ).

Each of these approaches (with the possible exception of C) may require the assignment of a person to remain at the field-mounted gauge or pressure readout and communicate steam generator pressure to the control room via the plant interior communications system.

5.18.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #13

None

5.18.6 Conclusions and Recommendations Regarding Damage Control Measure #13

All four alternatives for providing local indication of steam generator pressure are technically feasible. All of these measures complicate the sabotage actions that the saboteur must perform to eliminate all indication of steam generator pressure. Some require more items to be physically protected than others to ensure that some capability to measure steam generator pressure can be restored. A clear selection among these alternatives cannot readily be made.

5.18.7 Section 5.18 References

1. Lobner, P., et al., "Nuclear System Components - A Review of Typical Design and Operating Characteristics of Components Used in Nuclear Power Plant Systems," SAI01379-585LJ, Science Applications, Inc., March 21, 1979.

5.19 DAMAGE CONTROL MEASURE #19 - BWR AND PWR

The purpose of damage control measure #19 is to provide emergency AC electrical power to nonsafety-related components or systems that could be used in emergencies as a substitute for safety-related equipment disabled by sabotage action.

5.19.1 Sabotage Scenarios

Loss of offsite power occurs coincidentally with the sabotage of some safety-related systems required for maintaining the plant in a safe condition. The main turbine generator trips on loss of load. Nonsafety-related systems capable of maintaining the plant in a safe condition have not been sabotaged, but are unavailable because of the loss of Nonclass 1E AC power. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.19.2 Onsite AC Electric Power System Description

There is great variety in the design of onsite electrical power systems. An example of an onsite electric power system is illustrated in Figure 5.19.1 (from Ref. 1). This system is divided into two major parts; a Nonclass 1E part which supplies nonsafety-related equipment and a Class 1E part, which supplies safety-related equipment, and in some cases, selected nonsafety-related equipment. IEEE Standard 384 (Ref. 2) and Regulatory Guide 1.75 (Ref. 3) establish guidelines that define the electrical isolation and physical separation that must be achieved between the Class 1E and Nonclass 1E portions of the onsite electric power system. Electrical isolation is achieved by means of Class 1E isolation devices (e.g., suitable circuit breakers or current transformers), shielding and wiring techniques. Physical separation is achieved by means of spacing and safety class physical barriers. The intent of these separation requirements is to create an independent Class 1E electrical system that can provide necessary power to safety-related systems irrespective of faults in, or unavailability of the Nonclass 1E electrical system.

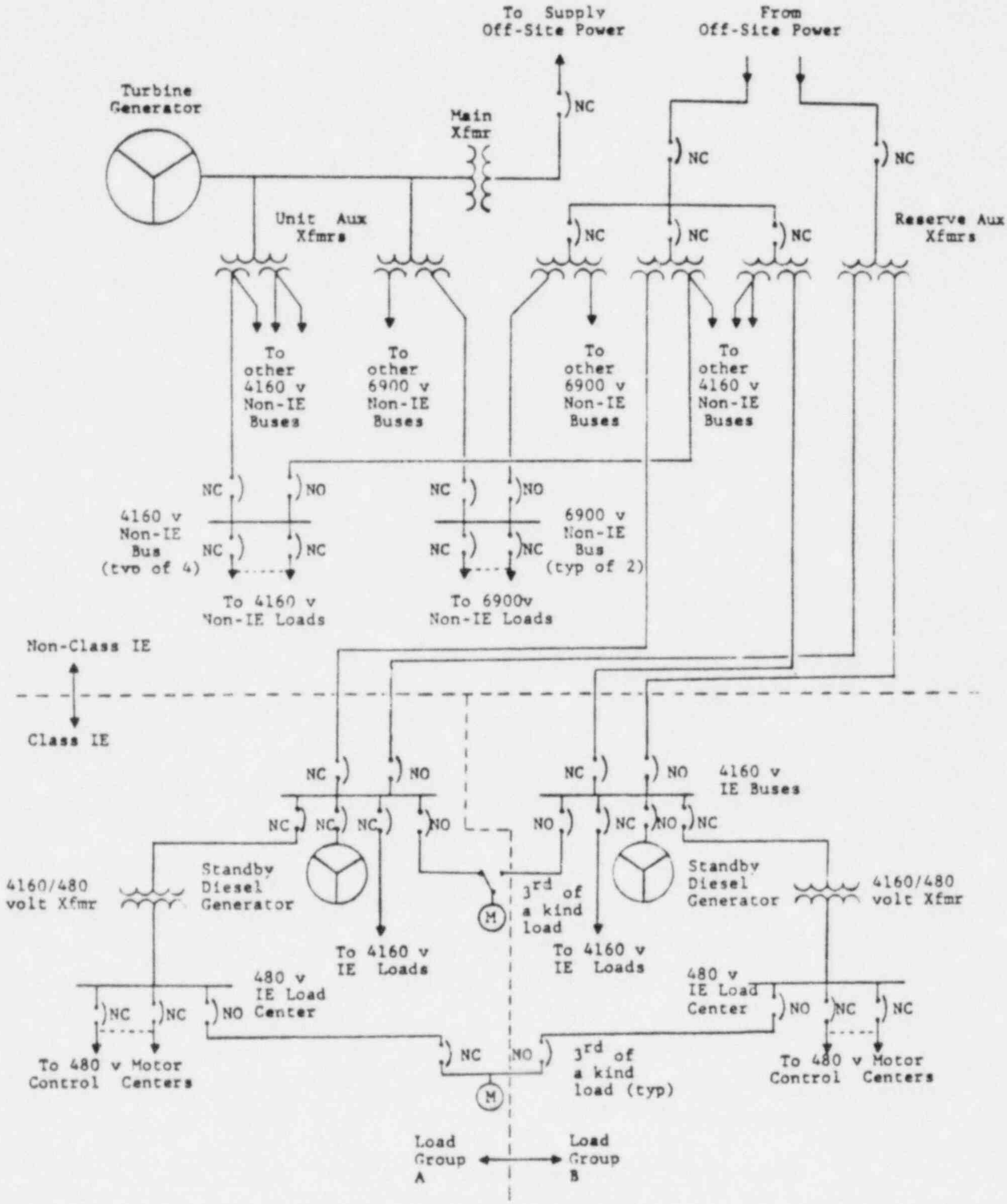


Figure 5.19.1. Example of an Onsite AC Electric Power System.

5.19.2.1 Nonclass 1E AC Electric Power System

During normal power operation, electric power to the Nonclass 1E system is supplied from the main turbine generator via auxiliary transformers. During unit startup or shutdown, when the main turbine is not operating, electric power can be supplied from the offsite grid via the reserve auxiliary (or startup) transformers.

5.19.2.2 Class 1E AC Electric Power System

Separation and redundancy is provided within the Class 1E system to ensure that a single failure will not result in a loss of ability to maintain the plant in a safe shutdown condition. This additional separation results in the formation of independent Class 1E electrical divisions or load groups. Typically, there are two or three Class 1E AC divisions (6900, 4160 or 480 VAC), and two, three or four Class 1E DC and 120 VAC divisions. A summary of PWR and BWR Class 1E AC electric power system configurations is presented in Tables 5.19.1 and 5.19.2, respectively (data abstracted from Ref. 4).

The preferred source of power for the Class 1E system may consist of two or more circuits from the offsite transmission network. One feeder is selected as the normal feeder, and the other serves as a backup, or alternate feeder. The normal supply for the Class 1E system is the main turbine generator in some plants. Alternate feeders from the offsite grid are also provided. Independent standby onsite power supplies (e.g., a diesel generator and station batteries) are provided for each Class 1E electrical division. Guidance on sizing the standby diesel generator to adequately support safety-related loads is provided in IEEE Standard 387 (Ref. 5).

Nonclass 1E loads may be supplied from the Class 1E system when proper isolation provisions are made. The following guidance for such interconnections is provided in USNRC Standard Review Plan 8.3.1 (Ref. 6).

> "In ensuring that the interconnections between non-Class 1E loads and Class 1E buses will not result in the degradation of the Class 1E system, the isolation device through which standby power is supplied to the non-Class 1E load, including control circuits and connections to the Class 1E bus, must be designed to meet Class 1E requirements. Should the standby power supplies have not been sized to accommodate

Table 5.19.1. Summary of PWR Class 1E AC Electric Power System Configurations[a].

Plant	Number of Diesels Per Unit(b)	Continuous Load Rating (KW)	Number of AC Divisions Per Unit	Ties Between Divisions	Ties Between Units
ANO 1	1D+1S	2750	2	Yes	Yes
ANO 2	1D+1S	2850	2	Yes	Yes
Beaver Valley 1	2D	2600	2	Yes	-
Calvert Cliffs 1 and 2	2S(c)+1SW	2500	2	No	Yes
Cook 1 and 2	2	3500	2	No	No
Crystal River 3	2D	2750	2	No	-
Davis - Besse 1	2D	2600	2	Yes	-
Farley 1 and 2	1D+3S	4000(D) 2600(S)	6	Yes	Yes
Fort Calhoun 1	2D	2500	2	Yes	-
Ginna	2D	1950	2	Yes	-
Haddam Neck	2D	2850	2	No	-
Indian Point 2 and 3	3D	1750	3	Yes	Yes
Kewanee	2D	2850	2	Yes	-
Maine Yankee	2D	2500	2	No	-
Millstone 2	2D	2750	2	Yes	(?)
North Anna 1 and 2	2D	2750	2	Yes	Yes
Oconee 1, 2 and 3	Hydro(d)	-	3	Yes	Yes
Palisades	2D	2500	2	Yes	-
Point Beach 1 and 2	2S(c)	2850	2	Yes	Yes
Prairie Island 1 and 2	2S(c)	2750	2	Yes	Yes

Figure 5.19.1. Summary of PWR Class 1E AC Electric Power System Configurations[a] (Continued).

Plant	Number of Diesels Per Unit(b)	Continuous Load Rating (KW)	Number of AC Divisions Per Unit	Ties Between Divisions	Ties Between Units
Rancho Seco	2D	2750	2	Yes	-
Robinson 2	2D	2500	2	Yes	-
Salem 1 and 2	3D(e)	2600	3	Yes	No
San Onofre 1	2D	600	2	Yes	No
San Onofre 2 and 3	2D	4700	2	No	No
St. Lucie 1 and 2	2D	3500	2	Yes	No
Surry 1 and 2	1D+1S	2850	2	Yes	Yes
Three Mile Island 1	2D	2600	2	No	No
Three Mile Island 2	2D	3000	2	Yes	No
Trojan	2D	4418	2	Yes	-
Turkey Point 3 and 4	2S(c)	2500	2	Yes	No
Zion 1 and 2	2D+1S	4000	3	Yes	Yes

Notes: (a) Data abstracted from NUREG/CR-2069, "Summary Report on a Survey of Light Water Reactor Safety Systems"
(b) D = dedicated to one unit, S = shared between units, SW - swing diesel, can be aligned to either unit
(c) Each diesel supplies a bus in each unit
(d) No diesels, two hydroelectric generators serve all units
(e) Plus 40 MW gas turbine generator

Table 5.19.2. Summary of BWR Class 1E AC Electric Power System Configurations.[a]

Plant	Number of Diesels per Unit[b]	Continuous Load Rating (KW)	Number of AC Divisions Per Unit	Ties Between Divisions	Ties Between Units
Arnold	2D	2850	2	Yes	-
Browns Ferry 1 and 2	4S	2600	2	No	Yes
Browns Ferry 3	4D	2600	2	No	Yes
Brunswick 1 and 2	2D	3500	2	Yes	Yes
Cooper 1	2D	4000	2	Yes	-
Dresden 2 and 3	1D + 1S	2850	2	Yes	Yes
Fitzpatrick	4D	2600	2	Yes	-
Hatch 1 and 2	2D + 1S	2850	3	Yes	Yes
Millstone 1	1D[c]	3000	7	Yes	-
Monticello	2D	2500	2	Yes	-
Nine Mile Point	2D	2560	2	Yes	(?)
Oyster Creek	3D	2500	2	Yes	-
Peach Bottom 2 and 3	4S	2600	2	Yes	Yes
Pilgrim 1	2D	2600	2	Yes	-
Quad Cities 1 and 2	1D + 1S	2850	2	Yes	Yes
Vermont Yankee	2D	3000	2	Yes	-

Notes: (a) Data abstracted from NUREG/CR-2069, "Summary Report on a Survey of Light Water Reactor Safety Systems".

(b) D = dedicated to one unit, S = shared between units.

(c) Plus 12 MW gas turbine generator.

the added non-Class 1E loads during emergency conditions, the design must provide for the automatic disconnection of those non-Class 1E loads upon the detection of the emergency condition. This action must be accomplished whether or not the load was already connected to the power supply. Further, the design must also prevent the automatic or manual connection of these loads during the transient stabilization period subsequent to this event."

5.19.3 Plant Conditions During Sabotage Scenario

Loss of offsite power is assumed to cause a trip of the main turbine generator. This effectively eliminates the sources of Nonclass 1E power to plant systems. Although Class 1E power is available, some safety system(s) have been sabotaged (e.g., auxiliary feedwater, component cooling water, high pressure injection, suppression pool cooling, etc.) and the plant is tending toward an unsafe condition. If electric power could be restored to some selected nonsafety systems, they could be substituted for the sabotaged safety systems and the plant could be maintained in a safe condition. Other damage control measures describe the specific system substitutions or realignments that have been considered.

5.19.4 Electric Power System Features to Facilitate Energizing Selected Nonclass 1E Components from the Class 1E Buses

The following three basic approaches for reenergizing nonsafety-related equipment from the Class 1E system are discussed below:

- Running temporary three-phase cables between Class 1E distribution load centers and selected Nonclass 1E switchgear or motor control centers.
- Providing permanent interconnections to align selected components to either a normal Nonclass 1E bus or, during emergencies, to a Class 1E bus.
- Providing normal power to selected Nonclass 1E components from Class 1E buses and providing the isolation capabilities recommended in References 2, 3, and 6.

Running temporary power cables would be a difficult damage control concept to implement. Long power cables will likely be required because of: (1) separation requirements implemented in plant design and, (2) Nonclass 1E switchgear and motor control centers are distributed throughout the plant, usually in the vicinity of the components they serve. This approach is further complicated by the weight of the temporary cables, available manpower, and in some cases, short time constaints. No further consideration will be given to this approach.

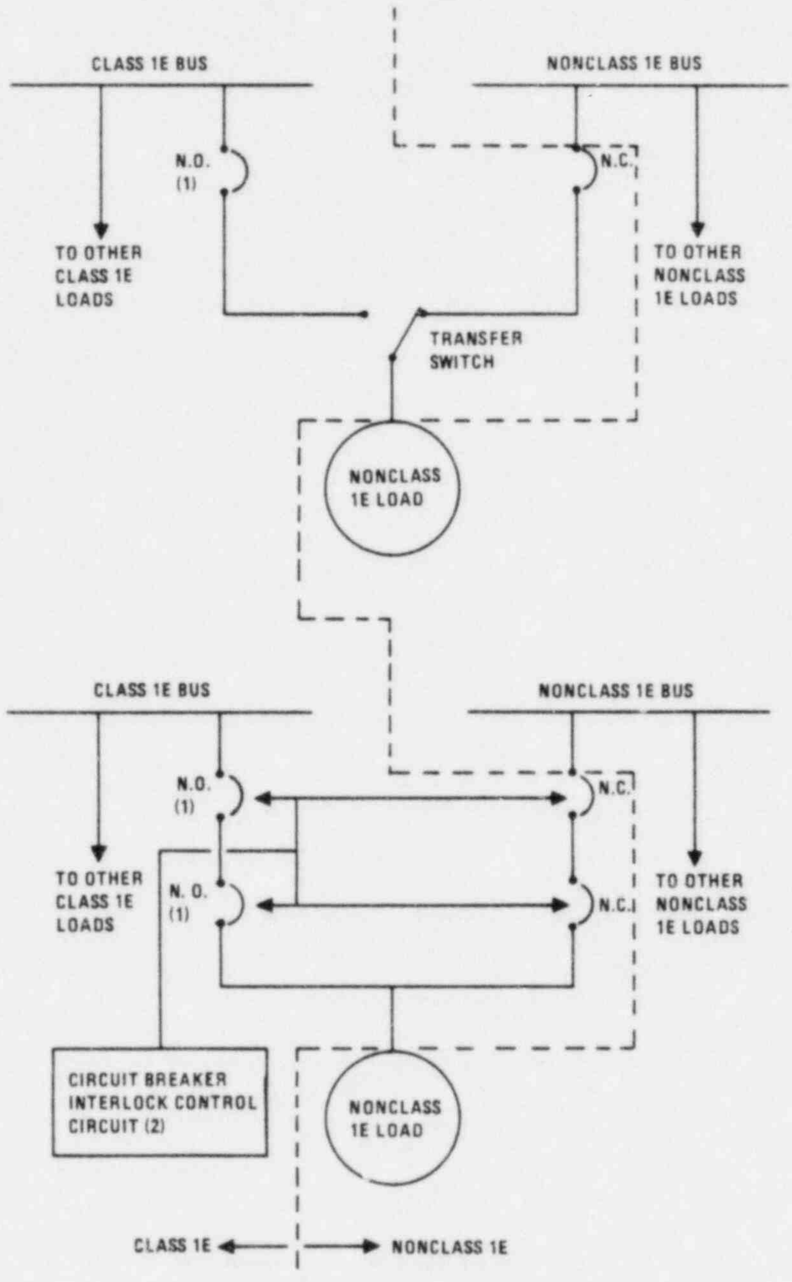
It is assumed that the nonsafety-related equipment of concern is normally powered from the Nonclass 1E electrical system. Reenergizing this equipment from the Class 1E system is therefore a significantly different concern than reenergizing Nonclass 1E equipment that is normally connected to the Class 1E system. Guidance for this latter case has been described References 2, 3, and 6.

Two possible approaches for connecting a Nonclass 1E component to either a Nonclass 1E bus or a Class 1E bus are illustrated in Figure 5.19.2. These circuit configurations are similar to those provided for third-of-a-kind loads in Figure 5.19.1. The normal power source is the Nonclass 1E bus. Circuit design and/or Class 1E interlocks prevent energizing the component from both sources simultaneously. Some of the loads that may be realigned to the Class 1E system are quite large (e.g., condensate or main circulating water pump) and may therefore, introduce the possibility of overloading the diesel generator through operator error. Emergency procedures must be available to describe manual load shedding requirements before large Nonclass 1E loads can be started on the Class 1E system. The rated diesel generator output for many operating plants is listed in Tables 5.19.1 and 5.19.2.

A simpler solution may be to provide normal power to the selected Nonclass 1E components via a Class 1E bus. The available guidance in References 2, 3, and 6 describe how these interconnections should be made. As discussed previously, emergency procedures procedures may be required.

5.19.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #19

Design provisions for reenergizing Nonclass 1E equipment from the Class 1E system can be made. Emergency operating procedures would likely be required to ensure that this capability does not degrade the reliability of the Class 1E



NOTES: (1) THESE CIRCUIT BREAKERS MUST AUTOMATICALLY RECEIVE AN "OPEN" COMMAND UPON DETECTION OF AN EMERGENCY CONDITION, AND MUST BE PREVENTED FROM BEING CLOSED DURING THE TRANSIENT STABILIZATION PERIOD FOLLOWING THE EVENT.

(2) INTERLOCK PREVENTS ENERGIZING LOAD FROM BOTH SOURCES SIMULTANEOUSLY

(3) N.O. = NORMALLY OPEN, N.C. = NORMALLY CLOSED

Figure 5.19.2. Possible Approaches for Connecting Nonclass 1E Loads to Nonclass 1E or Class 1E Systems.

system, either by overloading the diesel generators or by improperly interconnecting Nonclass 1E equipment to the Class 1E system.

NRC concern over connecting Nonclass 1E equipment to the Class 1E system is described in NUREG-0410 (Ref. 7) as Category A technical activity task A-25. Category A issues include generic technical issues judged by the NRC staff to warrant priority attention to attain early resolution. Current resolution of this task is reflected in USNRC Regulatory Guide 1.75 (Ref. 3) and Standard Review Plan 8.3.1 (Ref. 6). Some interconnections that may be required by this damage control measure appear to go beyond the scope of currently available design guidelines. It is likely that this damage control measure would introduce significant new licensing concerns.

5.19.6 Conclusions and Recommendations Regarding Damage Control Measure #19

Although technically feasible approaches have been identified, this damage control measure may adversely affect the reliability of the Class 1E electrical system. Significant licensing concerns could arise if this damage control measure were implemented.

An alternative approach would be to provide onsite Nonclass 1E standby generators to power selected nonsafety-related equipment. Such generators could be sized as necessary to support the operation of a significant amount of nonsafety equipment. Separation between Class 1E and Nonclass 1E systems would be maintained. The plant may even have a black start capability with these additional generators (see damage control measure #26).

5.19.7 Section 5.19 References

1. Lobner, P., et al., "The Pressurized Water Reactor-A Review of a Typical Combustion Engineering PWR Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

2. IEEE 384-1977, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers.

3. USNRC Regulatory Guide 1.75, "Physical Independence of Electrical Systems."

4. Heddleson, F. A., "Summary Report on a Survey of Light Water Reactor Safety Systems," NUREG/CR-2069, Oak Ridge National Laboratory, Nuclear Safety Information Center, October 1981.

5. IEEE 387-1977, "IEEE Standard Criteria for Diesel Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations."

6. USNRC Standard Review Plan 8.3.1, "A-C Power System (Onsite)," NUREG-0800, U. S. Nuclear Regulatory Commission, July 1981.

7. NUREG-0410, "NRC Program for the Resolution of Generic Issues Related to Nuclear Power Plants," U. S. Nuclear Regulatory Commission, January 1, 1978.

5.20 DAMAGE CONTROL MEASURE #20 - BWR AND PWR

The purpose of damage control measure #20 is to provide cross connections between Class 1E DC load groups in PWR and BWR plants to permit reenergizing a load group in the event that its Class 1E battery is disabled by sabotage action.

5.20.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the sabotage of one or more Class 1E DC load groups. The emergency diesel generators which receive control power from operable Class 1E DC load groups operate and provide Class 1E AC power to safety-related systems.

5.20.2 Onsite DC and 120 VAC Vital Instrumentation Power System Description

DC power systems provide 125 or 250 VDC to equipment requiring uninterruptable power. During normal operation, battery chargers supplied from an AC bus (typically 480 VAC) maintain the batteries charged and supply all loads on the DC power system. When this normal AC source is unavailable, all loads on the DC power system are supplied directly from the station batteries.

There is wide variety in the design of DC power systems. There may be two, three or four Class 1E DC electrical load groups (or divisions) to supply safety-related loads. In addition, there may be Nonclass 1E batteries for switchyard circuit breaker control, turbine generator emergency auxiliary systems (e.g., coast-down lube oil pumps) or for other control functions related to the balance-of-plant (BOP). A summary of PWR and BWR DC electric power system configurations is presented in Tables 5.20.1 and 5.20.2, respectively (data abstracted from Ref. 1). Typical loads on DC power systems are listed in Table 5.20.3. Among these loads are 120 VAC vital instrumentation and control power systems which are supplied via inverters.

Table 5.20.1. Summary of PWR DC Electric Power System Configurations[a].

Plant	Voltage	Number of Batteries Per Unit	Number of DC Divisions Per Unit	Number of Battery Chargers Per Unit	Ties Between Divisions	Ties Between Units	Other Batteries
ANO 1	125	2	2	3	Yes	No	Switchyard BT
ANO 2	125	2	2	3	Yes	No	Emergency TG Aux. BT (125 V)
Beaver Valley 1	125	4	2	4	Yes	-	(2) Switchyard BT (125 V)
Calvert Cliffs 1 and 2	125	2	2	4	No	Yes	Diesel field flash BT
Cook 1 and 2	250	2	2	4	Yes	No	Substation control BT
	250[b]	1	1	2	(?)		
Crystal River 3	250/125	2	2	6	Yes	-	None
Davis-Besse 1	250/125	4	2	6	Yes	-	Switchyard BT (125 V)
Farley 1 and 2	125	2	2	3	(?)	(?)	(3) Service water, cooling tower, relay BT (125 V)
Fort Calhoun 1	125	2	2	3	No	-	None
Ginna	125	2	2	2	Yes	-	None
Haddam Neck	125	2	2	2	Yes	-	None
Indian Point 2	125	2	2	2	Yes	No	(2) Switchyard BT (125 V)
Indian Point 3	125	3	3	3	Yes	No	None
Kewaunee	125	2	2	3	Yes	No	Switchyard BT
Maine Yankee	125	4	2	4	Yes	-	Switchyard BT
Millstone 2	125	2	2	3	Yes	(?)	Emergency TG Aux. BT (125 V)
North Anna 1 and 2	125	4	4	6	No	No	None
Oconee 1, 2 and 3	125	2	2	3	Yes	Yes	None
Palisades	125	2	2	4	No	-	Switchyard BT (125 V)
Point Beach 1 and 2	125	2[c]	2[c]	3[c]	Yes	Yes	Switchyard BT (125 V)
Prairie Island 1 and 2	125	2	2	2	Yes	No	Switchyard BT
Rancho Seco	125	4	6	6	Yes	-	
Robinson 2	125	2	2	2	Yes	-	Diesel field flash BT
Salem 1 and 2	250	1	1	1	Yes	No	(2) Control BT (28 V)
	125	3	3	6			

Table 5.20.1. Summary of PWR DC Electric Power System Configurations[a] (Continued).

Plant	Voltage	Number of Batteries Per Unit	Number of DC Divisions Per Unit	Number of Battery Chargers Per Unit	Ties Between Divisions	Ties Between Units	Other Batteries
San Onofre 1	125	1	1	2	-	-	Switchyard BT
San Onofre 2 and 3	125	4	4	4	No	No	(2) Switchyard, Emerg. TG Aux. BT
St. Lucie 1 and 2	125	2	2	3	Yes	-	(2) Switchyard BT
Surry 1 and 2	125	2	2	4	Yes	(?)	Diesel field flash BT, Switchyard BT
Three Mile Island 1	125/250	2	2	6	Yes	No	Switchyard BT
Three Mile Island 2	125/250	2	2	4	Yes	No	None
Trojan	250	1	1	1	No	-	Switchyard BT
	125	2	2	4			
Turkey Point 3 and 4	125	2	2	3	Yes	No	Switchyard BT
Zion 1 and 2	125	2.5	2	5	No	Yes	None

Notes: (a) Data abstracted from NUREG/CR-2069, "Summary Report on a Survey of Light Water Reactor Safety Systems".

(b) Auxiliary Feedwater system control only.

(c) Shared between units.

Table 5.20.2. Summary of BWR DC Electric Power System Configuations.

Plant	Voltage	Number of Batteries Per Unit	Number of DC Divisions Per Unit	Number of Battery Chargers Per Unit	Ties Between Divisions	Ties Between Units	Other Batteries
Arnold	250 125	1 2	1 2	2 3	Yes	-	(2) Nuclear instruments, switchyard BT (24V)
Browns Ferry 1, 2 & 3	250	2	2	2	No	Yes	Diesel field flash BT, monitoring + switchyard BT (24V)
Brunswick 1 & 2	125/250	2	2	4	Yes	Yes	None
Cooper 1	250 125	2 2	2 2	2 2	Yes	-	Switchyard BT
Dresden 2 & 3	250 125	1 1	1 1	1 1(b)	Yes	Yes	Switchyard BT
Fitzpatrick	125	2	2	2	No	-	Monitoring BT (24V)
Grand Gulf 1 & 2(c)	125	3	3	6	No	No	(2)BOP batteries (125/250V)
Hatch 1 & 2	125/250	2	2	6	No	No	Diesel field flash BT, switchyard BT
Millstone 1	125	2	2	3	Yes	(?)	Switchyard BT
Monticello	250 125	1 2	1 2	2 3	Yes	-	Switchyard BT
Nine Mile Point	125	2	2	2	Yes	-	None
Oyster Creek	125	1	2	2	Yes	-	Diesel field flash BT, switchyard BT
Peach Bottom 2 & 3	125/250	4	2	4	No	No	Emergency TG Aux. BT (250V), switchyard BT
Pilgrim 1	250 125	1 2	1 2	2 3	Yes	No	Switchyard BT
Quad Cities 1 & 2	250 125	1 1	1 1	2 2	Yes	Yes	None
Vermont Yankee	125	2	2	3	Yes	-	Switchyard BT

Notes: (a) Data abstracted from NUREG/CR-2069, "Summary Report on a Survey of Light Water Reactor Safety Systems"

(b) Third battery charger is shared between units.

(c) From Grand Gulf FSAR, Docket 50416, Mississippi Power and Light

Table 5.20.3. Composite List of Typical Loads on DC Power Systems.

125 VDC Class 1E System

Class 1E DC instrumentation and control systems
Class 1E DC valve actuators
Class 1E switchgear DC control power
Diesel generator control, field flashing and DC auxiliary pump power
Inverters for the 120 VAC vital instrumentation buses
Auxiliary feedwater (AFW) system turbine-driven pump control and DC valve power (PWRs)
Reactor core isolation cooling (RCIC) system control, DC valve and DC auxiliary pump power (BWRs)
High pressure coolant injection (HPCI) system control, DC valve and some DC auxiliary pump power (BWRs)
Backup scram valves (BWRs)
Scram circuit breaker control power (PWRs)

250 VDC Class 1E System

High pressure coolant injection (HPCI) system auxiliary lube oil pumps (BWRs)

125 VDC Nonclass 1E System

Nonclass 1E DC instrumentation and control systems
Nonclass 1E DC valve actuators
Nonclass 1E switchgear DC control power
Inverters for some plant computer systems
Some emergency lighting

250 VDC Nonclass 1E System

Main turbine emergency bearing lube oil pump
Main generator emergency hydrogen seal oil pump
Main feedwater turbine emergency lube oil pumps
Inverters for some plant computer systems

A "minimum" DC power system, illustrated in Figure 5.20.1 (from Ref. 2), is physically and electrically separated into two redundant, independent load groups, each being fed by one battery and one battery charger. The nuclear plant can achieve and maintain a safe shutdown condition following th loss of either DC load group. Each load group in the "minimum" DC power system supplies Class 1E and Nonclass 1E DC loads as well as 120 VAC vital instrumentation loads (via an inverter). A manually-operated bus tie circuit breaker is provided for parallel operation of the two load groups when either battery or battery charger is out of service for maintenance. This system has been reviewed in detail in NUREG-0666 (Ref. 2).

A more comprehensive Class 1E 125 VDC and 120 VAC power system is illustrated in Figure 5.20.2 (from Ref. 3). The Class 1E system is physically and electrically separated into four redundant, independent load groups. The loss of any single load group does not adversely affect the performance of the remaining load groups. In addition to the Class 1E DC electric power system in Figure 5.20.2, separate Nonclass 1E 250 VDC and/or 125 VDC systems are provided for nonsafety-related DC loads.

Common design practices for ensuring independence of the DC load groups include the following (Ref. 4):

- The standby source (e.g., battery) of one load group should not be automatically paralleled with the standby source of another load group under accident conditions;
- No provisions should exist for automatically connecting one load group to another load group;
- No provisions should exist for automatically transferring loads between redundant power sources; and
- If means exist for manually connecting redundant load groups together, at least one interlock should be provided to prevent an operator error that would parallel their standby power sources.

The following further guidance regarding the independence of DC load groups is provided in USNRC Standard Review Plan 8.3.2 (Ref. 5).

"The interconnections between redundant load centers through bus tie breakers and multi-feeder breakers used to connect

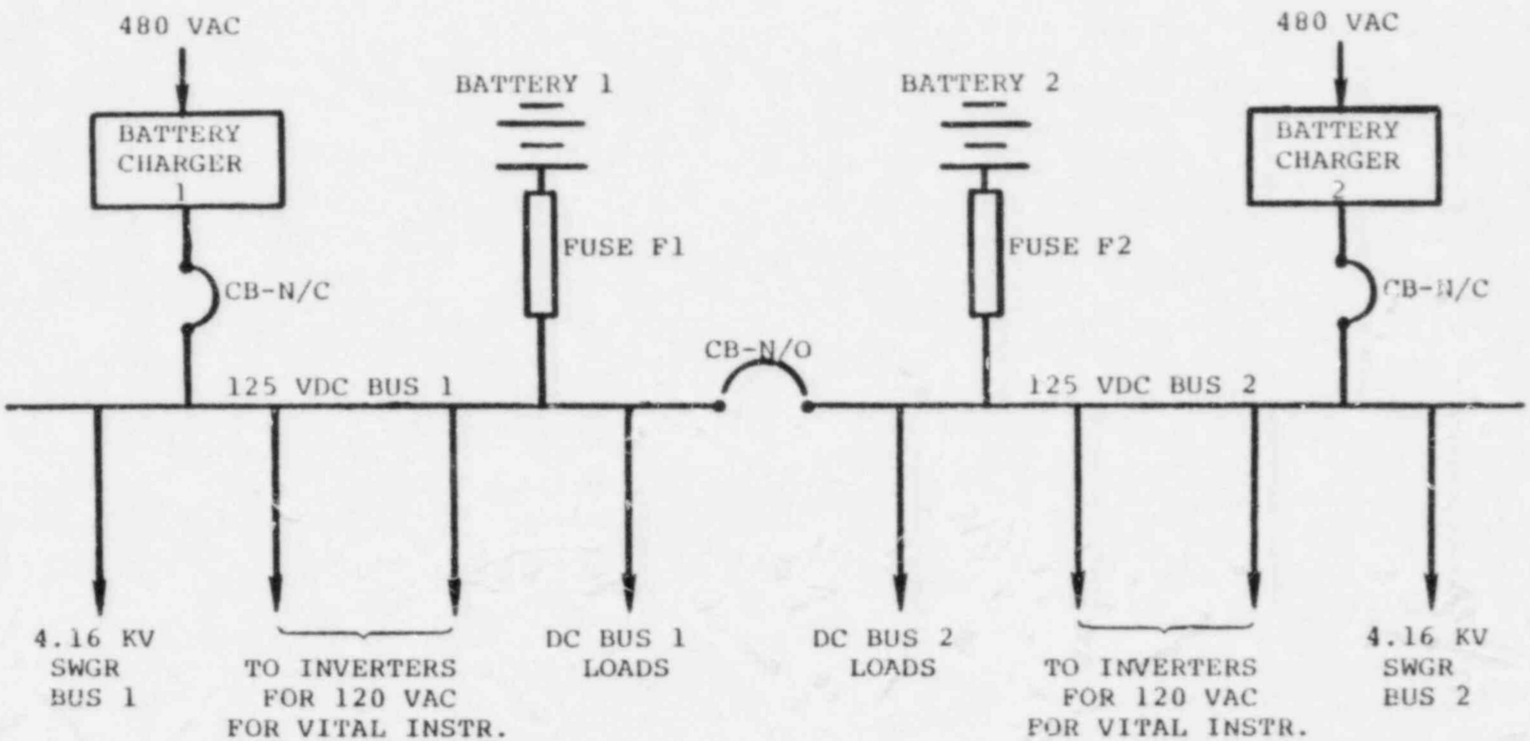


Figure 5.20.1. Simplified Schematic, Minimum DC Power System (from NUREG-0666).

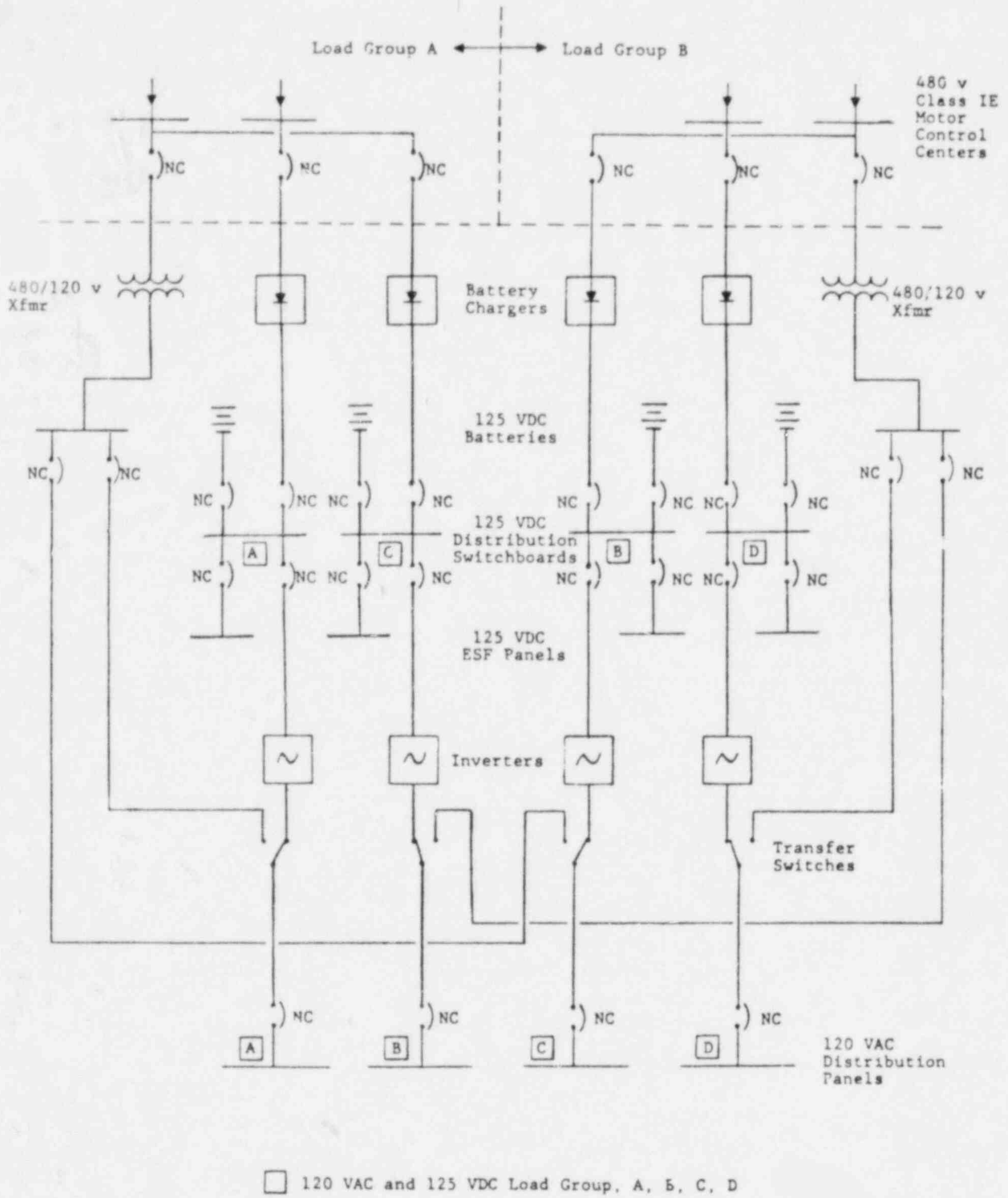


Figure 5.20.2. "Class 1E 125 VDC and 120 VAC Electric Power System with Four Load Groups (from SAI01379-626LJ)."

> extra redundant loads to either of the redundant distribution systems are examined (by the NRC) to assure that no single failure in the interconnections will cause the paralleling of the DC power supplies. To assure this, the control circuits of the bus tie breakers or multi-feeder breakers must preclude automatic transferring of load centers or loads from the designated supply to the redundant counterpart upon loss of the designated supply. Regarding the interconnections through bus tie breakers, an acceptable design will provide for two tie breakers connected in series and physically separated from each other in accordance with the acceptance criteria for separation of safety-related systems. Further, the interconnection of redundant load centers must be accomplished only manually."

Interconnections between redundant load groups are frequently provided in nuclear plants to allow a battery or battery charger to be removed from service (see Tables 5.20.1 and 5.20.2). The typical bus tie circuit includes two series circuit breakers, as described above. During normal operations, these circuit breakers are both normally open, and in some plants, the circuit breakers are racked-out as well. The NRC is considering the recommendation made in NUREG-0666 (Ref. 2) that bus ties be eliminated in the minimum DC power system, or at least preclude their use during normal power operation so as not to compromise divisional independence of the DC power supplies required for operation of decay heat removal systems (Ref. 2).

A single-train safety system requiring DC power would be disabled by the loss of its respective DC load group. The BWR reactor core isolation cooling (RCIC) system and high pressure coolant injection (HPCI) system are both single-train systems that together provide a redundant high pressure coolant injection capability. Each system is supplied from a different DC load group, therefore, loss of a single DC load group does not eliminate the capability to provide core coolant makeup at high pressure. Comparable electrical separation is provided for multiple-train safety systems. Loss of a single DC load group generally affects only a single train of each system. Adequate system capability exists to perform required safety functions with the remaining trains.

Loss of a single 125 VDC load group may also disable its respective 120 VAC vital instrumentation load group. Redundancy of safety-related instrumentation (e.g., multiple, independent channels monitoring important plant parameters) ensures that adequate status monitoring, actuation and control capability exists following loss of a 125 VDC load group and its respective 120 VAC load group.

5.20.3 Plant Conditions During Sabotage Scenario

Following the loss of one Class 1E DC load group, one channel of safety-related instrumentation, one train of some multi-train safety systems, some single-train systems, and one standby diesel generator may be inoperable. By design, the nuclear power plant can be maintained in a safe shutdown condition with the remaining DC load group(s) and operable safety systems.

Some plants only have two Class 1E DC load groups. Loss of the second load group in such a plant will likely result in a loss of capability to provide adequate decay heat removal. If the diesel generators have not been started before DC power was lost, this event would correspond to a station blackout plus loss of DC power.

Plants having three or four DC load groups may be capable of withstanding the loss of more than one load group. The specific plant response would be highly dependent on the safety systems that remained operable.

The specific sabotage actions that resulted in the loss of DC load groups have not been specified. Depending on the sabotage actions, various approaches may be available to reenergize selected safety-related systems. If a Class 1E battery was the target, the protective electrical relaying in the DC power distribution system would likely disconnect the affected battery from its respective DC bus. If this has not occurred, manual actions could be taken to disconnect the battery (e.g., by manually opening the circuit breaker or disconnect links). After it has been determined that no faults exist on the affected DC bus, it would be possible to reenergize that load group by crossconnecting to: (1) another Class 1E load group, or (2) an available Nonclass 1E DC power system. The first approach is discussed in this section. Damage control measure #21 describes the implementation of the second approach.

If a fault remains on the DC bus following sabotage actions, it would not be possible to simply reenergize the affected load group by either of the two previously described methods. Crossconnecting to a faulted bus may result in the loss of another load group. An alternate approach for reenergizing designated DC loads would be to provide individual components with multiple DC feeders and a capability to select any one DC feeder to supply the component. Damage control measure #22 describes this approach.

5.20.4 Design Features to Crossconnect Class 1E DC Load Groups

Considering the guidance for DC load group independence described previously, bus ties between Class 1E DC load groups are not recommended in "minimum" DC power systems (e.g., two independent DC load groups). Use of bus ties may be permissible in DC power systems having three or four independent load groups, and should have the following features:

- Each bus tie circuit between redundant load groups should provide two tie breakers connected in series and physically separated from each other. These circuit breakers should be normally open.
- The crossconnection of load groups should be accomplished manually
- At least one interlock should be provided to prevent an operator error that would parallel two batteries.
- Use of bus ties should not adversely affect the reliability and availability of the Class 1E DC power system.

A bus tie circuit incorporating these features is illustrated in Figure 5.20.3. Each load group would have the capability of being crossconnected to any other load group. Plants with two, three and four DC load groups would respectively require one, three and six bus tie circuits. Each bus tie circuit has series, interlocked manual circuit breakers. A separate interlock circuit is provided for each DC load group. Each interlock permits only one bus tie breaker to be closed when power is available at the bus (and to the interlock circuit). If a bus is dead. its interlock would not be active, and all bus tie breakers could be closed. Once a bus tie circuit has been completed, the interlock circuit on the previously "dead" bus side is reenergized. That interlock would allow the circuit breaker in the established bus tie to remain closed. Other bus

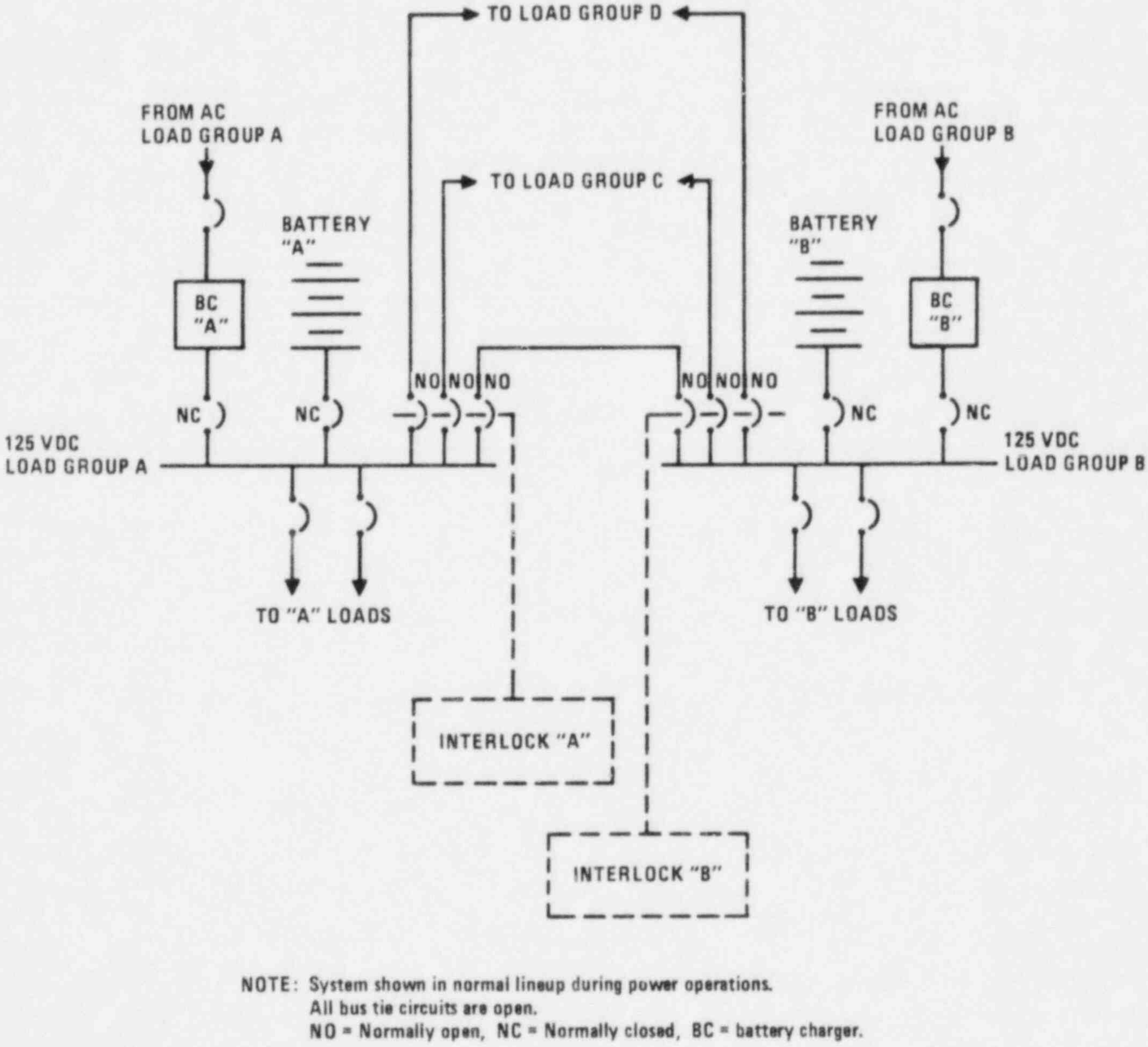


Figure 5.20.3. Approach for Crossconnecting Redundant Class 1E DC Load Groups.

tie circuit breakers would be immediately tripped open if they had been closed. The series bus tie circuit breaker arrangement requires two deliberate operator actions in different locations to establish a crossconnection between DC load groups. This feature should adequately guard against operator errors that would parallel two batteries. It may be possible to eliminate the interlocks by leaving all bus tie circuit breakers racked out. Four deliberate operator actions (e.g., rack in and close two circuit breakers) in two locations would be required to establish a bus tie under those conditions. Operating procedures would be required to clearly specify the conditions under which this DC bus tie capability may be used.

An operating strategy that might be adopted in conjunction with this damage control measure is to establish a crossconnection to a "dead" load group, start the diesel generator in the affected load group, and then disestablish the crossconnection once DC power is available via the battery charger in the affected load group. This approach provides for rapid restoration of DC load group independence.

5.20.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #20

The use of bus ties may adversely affect the reliability of DC power systems and the ability to provide adequate decay heat removal when required. The NRC is considering the recommendation made in NUREG-0666 (Ref. 2) that the use of bus ties in a "minimum" DC power system having two independent load groups be eliminated, or at least precluded during normal power operation. Acceptability of bus ties in other DC power system configurations should be determined on an individual case basis. Existing guidance (Refs. 4 and 5) establishes a basis for design of an acceptable bus tie capability.

5.20.6 Conclusions and Recommendations Regarding Damage Control Measure #20

This damage control measure is technically feasible. Unless additional sabotage actions are involved, the inherent redundancy of nuclear plant systems do not warrant the use of this damage control measure when only a single DC load group is affected. When required, this damage control measure would allow a Class 1E DC load group to be reenergized when the faults resulting from sabotage actions are limited to the battery, and these faults can be isolated from the remainder of the load group by opening the battery circuit breaker or disconnect links. In conjunction with operating procedures, this damage control measure provides a means for starting a diesel generator following loss of its normal DC control power supply and restoring operation of a Class 1E load group (DC and AC) that would otherwise be unavailable.

5.20.7 Section 5.20 References

1. Heddleson, F. A., "Summary Report on a Survey of Light Water Reactor Safety Systems," NUREG/CR-2069, Oak Ridge National Laboratory, Nuclear Safety Information Center, October 1981.

2. NUREG-0666, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," U. S. Nuclear Regulatory Commission, April 1981.

3. Lobner, P., et al., "The Pressurized Water Reactor - A Review of a Typical Combustion Engineering PWR Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

4. USNRC Regulatory Guide 1.6, "Independence Between Redundant Standby (Onsite) Power Soures and Between Their Distribution Systems."

5. USNRC Standard Review Plan 8.5.2, "DC Power Systems (Onsite)," NUREG-0800, U. S. Nuclear Regulatory Commission, July 1981.

5.21 DAMAGE CONTROL MEASURE #21 - BWR AND PWR

The purpose of damage control measure #21 is to provide cross connections between the Class 1E and the Nonclass 1E DC power systems in BWR and PWR plants to permit the Nonclass 1E batteries to supply DC power to safety-related systems when one or more Class 1E batteries are disabled through sabotage action.

5.21.1 Sabotage Scenario

See Section 5.20.

5.21.2 Onsite DC and 120 VAC Vital Instrumentation Power System Description

See Section 5.20.

5.21.3 Plant Conditions During Sabotage Scenario

See Section 5.20

5.21.4 Design Features to Supply the Class 1E DC System From a Nonclass 1E Station Battery

If a suitable Nonclass 1E DC system is available, a crossconnection to a Class 1E DC load group could be established as illustrated in Figure 5.21.1 (see Section 5.20 for a listing of other batteries that may be available for crossconnection to the Class 1E DC system). The number of bus tie circuits equals the number of Class 1E DC load groups. Bus tie circuits between Class 1E load groups require series, physically separated circuit breakers that are open during normal plant operations (Ref. 1). These features are included in Figure 5.21.1. To complete a Class 1E/Nonclass 1E bus tie circuit, additional disconnect links must be installed. Through administrative controls over the disconnect links, use of this Class 1E/Nonclass 1E bus tie capability can be effectively controlled. The boundary between the Class 1E and Nonclass 1E systems is illustrated in Figure 5.21.1.

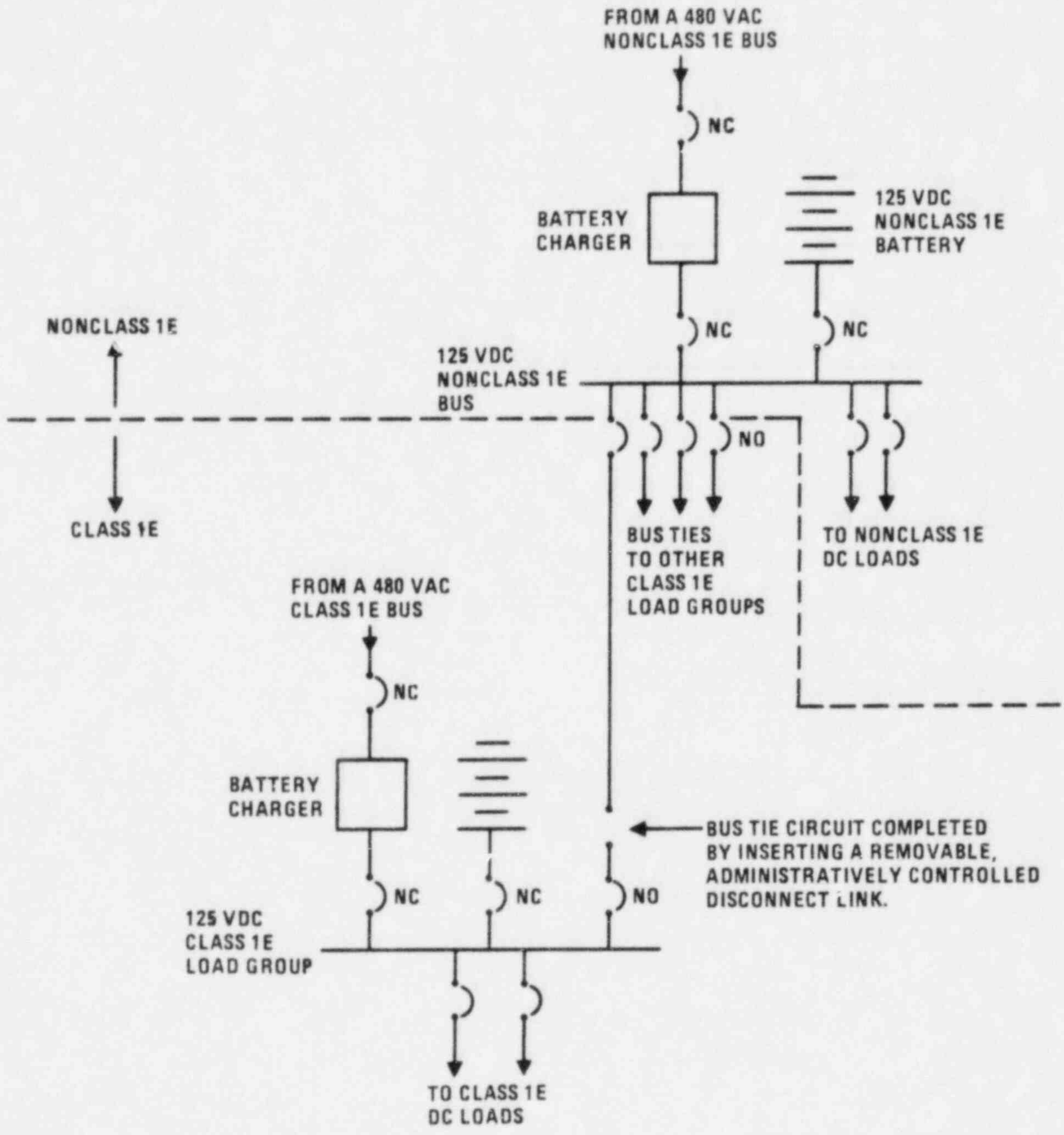


Figure 5.21.1. Approach for Establishing a Bus Tie Between Class 1E and Nonclass 1E DC Buses.

This damage control measure would be of use in reenergizing a single Class 1E DC load group following sabotage of its battery. With DC power restored to the Class 1E load group, its respective diesel generator could be started. Once Class 1E DC power is being supplied via the battery charger, the Class 1E/Nonclass 1E DC bus tie may be disestablished. If necessary, other Class 1E DC load groups could be reenergized in the same manner.

The bus tie illustrated in Figure 5.21.1 assumes that both the Class 1E and Nonclass 1E batteries are the same voltage (e.g., 125 VDC). Occassionally, 250 VDC batteries serve as sources for 250 VDC and 125 VDC systems. This is accomplished by providing additional battery terminals that essentially split the 250 VDC battery into two batteries for the purpose of supplying the 125 VDC systems. With such additional terminals, a 250 VDC Nonclass 1E station battery could be crossconnected to serve one, or perhaps two Class 1E DC load groups

5.21.5 Technical and Regulatory Impediments to Implementating Damage Control Measure #21

A bus tie capability between the Class 1E and Nonclass 1E DC power systems must be properly implemented and administratively controlled to ensure that separation and independence of the Class 1E DC system is maintained during all plant conditions when normal Class 1E DC power sources (battery and/or battery chargers) are available.

5.21.6 Conclusions and Recommendations Regarding Damage Control Measure #21

This damage control measure is technically feasible. It would allow a Class 1E DC load group to be reenergized when the faults resulting from sabotage action are limited to the battery, and these faults can be isolated from the remainder of the load group by opening the battery circuit breaker or disconnect links. This damage control measure does not reduce the separation and independence of Class 1E DC load groups from each other. In conjunction with operating procedures, this damage control measure provides a means for starting a diesel generator following loss of its normal DC supply, and restoring operation to a Class 1E load group (DC and AC) that would otherwise be unavailable.

5.21.7 Section 5.21 References

1. USNRC Standard Review Plan 8.3.2, "DC Power Systems (Onsite)," NUREG-0800, U. S. Nuclear Regulatory Commission, July 1981.

5.22 DAMAGE CONTROL MEASURE #22 - BWR AND PWR

The purpose of this damage control measure is to provide multiple selectable DC feeders to designated DC powered components to allow the components to be rapidly reenergized from an alternate feeder in the event that the original feeder is disabled by sabotage action.

5.22.1 Sabotage Scenario

See Section 5.20.

5.22.2 Onsite DC and 120 VAC Vital Instrumentation Power System Description

See Section 5.20.

5.22.3 Plant Conditions During Sabotage Scenario

See Section 5.20.

5.22.4 Design Features to Provide Selectable DC Feeders for Designated Components

Multiple DC feeders for selected equipment are occassionally provided in nuclear power plants. A principle requirement in the design of such multiple feeders is that no single failure in the interconnections will cause the paralleling of Class 1E DC power supplies (Ref. 1). To assure this, the control circuits of the multiple feeder circuit breakers and/or transfer switchs must not include provisions for automatically transferring loads between redundant power sources (Refs. 1 and 2).

Methods for establishing multiple feeder circuits for typical DC loads are illustrated in Figure 5.22.1. This type of transfer capability would permit selected loads to be reenergized when sabotage actions prevent restoring power to the DC bus itself via bus tie circuits (see damage control measures #20 and #21).

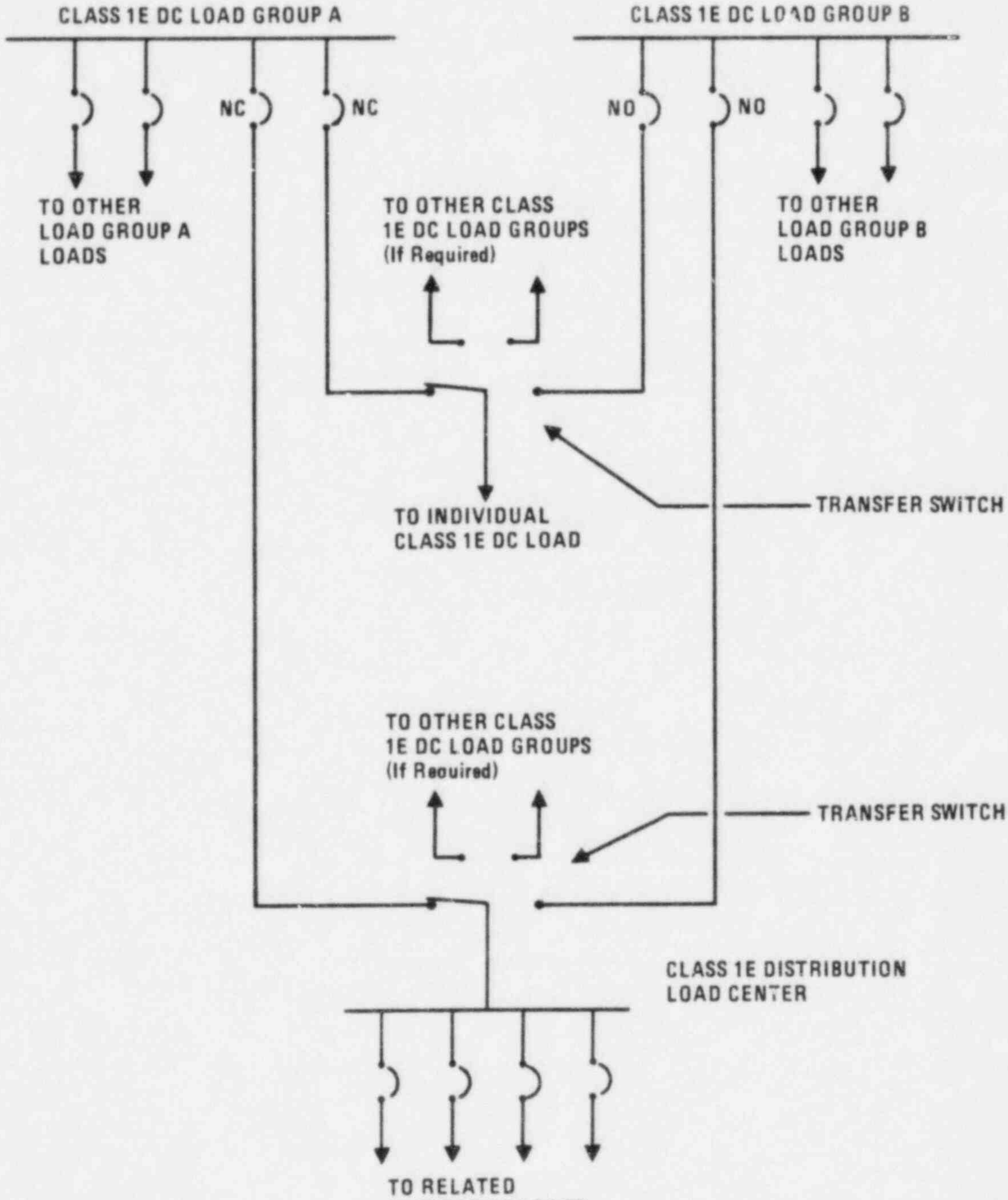


Figure 5.22.1. Approaches for Establishing a Multiple Feeder Circuit for Selected DC Loads.

The following DC loads are considered to be good candidates for multiple DC feeders:

- Components in a single-train safety system that would be inoperable following loss of its respective DC load group. Such systems include the BWR reactor core isolation cooling (RCIC) and high pressure coolant injection (HPCI) systems.

- Components in an individual train of a multi-train safety system that is designed to be operable when only DC power is available. An example is the PWR turbine-driven auxiliary feedwater (AFW) pump train.

- Inverters supplying 120 VAC vital instrumentation power systems from the DC system

- Diesel generator control systems.

- DC distribution load centers supplied from the battery bus.

The first two items in the above list generally involve multiple DC loads. In the case of the RCIC system, DC loads include the control system, gland seal vacuum and condensate pumps, DC motor-operated valves, and an inverter. Each of these loads may be supplied via an individual circuit from the DC bus. To simplify the implementation of this damage control measure, it would be advantageous to collect these related loads and supply them from a DC distribution load center which has a multiple feeder capability (see Figure 5.22.1). The potential impact of this design change on overall system reliability should be evaluated.

The time requirements to transfer selected loads to alternate load groups will likely be shorter than the time requirements to establish bus ties between Class 1E DC load groups or between a Class 1E DC load group and a Nonclass 1E DC system, as described in damage control measures #20 and #21.

5.22.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #22

Procedures have been established to verify that the capacity of the Class 1E DC system is adequate to power prescribed loads (Refs. 1 and 3). These procedures require that calculations be made to establish the combined load demand to be connected to each DC supply during the "worst" operating condition.

The potential impact of this damage control measure on battery capacity requirements has not been estimated.

5.22.6 Conclusions and Recommendations Regarding Damage Control Measure #22

This damage control measure is technically feasible. It would allow selected loads to be reenergized from an alternate load group under conditions that may preclude use of bus ties to restore power to an entire DC load group. This damage control measure may therefore be a useful complement to damage control measures #20 and/or #21. Impact of this damage control measure on system reliability and battery capacity requirements should be evaluated on an individual plant basis.

5.22.7 Section 5.22 References

1. USNRC Standard Review Plan 8.3.2, "DC Power Systems (Onsite)," NUREG-0800, U. S. Nuclear Regulatory Commission, July 1981.

2. USNRC Regulatory Guide 1.6, "Independence Between Redundant Standby (Onsite) Power Sources and Between Their Distribution Systems."

3. IEEE 485-1978, "IEEE Recommended Practice for Sizing Large Lead Storage Batteries for Generating Stations and Substations."

5.23 DAMAGE CONTROL MEASURE #23 - PWR

The purpose of damage control measure #23 is to provide alternative water sources to maintain reactor coolant inventory and to remove decay heat during hot shutdown in the event that the usual sources of water have been disabled through sabotage action.

5.23.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of the usual water sources for reactor coolant inventory control and decay heat removal. The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.23.2 Decay Heat Removal System Descriptions

Decay heat removal in a PWR is accomplished at high pressure by the auxiliary feedwater (AFW) system and at low pressure by the residual heat removal (RHR) or shutdown cooling (SDC) system.

5.23.2.1 Decay Heat Removal at High Pressure

The AFW system operates on an open cycle in which water is supplied to the steam generators to remove heat from the reactor coolant system (RCS) and steam is vented to the atmosphere as shown in Figure 5.23.1 (from Ref. 1). The AFW system requires a long-term source of water to provide the necessary makeup to the steam generators. The normal source of water for the AFW system is the condensate storage tank (CST). Water inventory in the CST is usually sized for RCS cooldown and timely transition to shutdown cooling system operation. Available AFW water sources at selected operating PWR plants are summarized in Table 5.23.1 (from Ref. 2).

AFW system makeup requirements for a 3390 MWt PWR are shown in Figure 5.23.2. It is notable that all of the plants listed in Table 5.23.1 have water supplies capable of supporting long-term operation of the AFW system.

Table 5.23.1. Sources of Auxiliary Feedwater for Cumbustion Engineering Operating Plants (from NUREG-0635).

	MAINE YANKEE	CALVERT CLIFFS (1 & 2)	ANO-2	FORT CALHOUN 1	MILLSTONE 2	PALISADES	ST. LUCIE
Condenser Hotwell				10^5 gal.			
Condensate Storate		7×10^5 gal. Available Per Unit	1.9×10^5 gal.	1.5×10^5 gal.	1.5×10^5 gal.	6×10^4 gal.	1.16×10^5 gal.
Demineralized Water	1.5×10^5 gal.	3.5×10^5 gal.		1×10^5 gal.			
Emergency Feedwater Storage Tank				5.5×10^4 gal.			
Primary Water Storage	1.61×10^5 gal.				1.5×10^5 gal.		
Primary Makeup Tank					7.5×10^4 gal.		
Pretreated Water storage Tanks		1×10^6 gal. Total					
Well Water		30 days supply					
Fire Protection System	3×10^6 gal.			unlimited	10^6 gal.	From Lake (unlimited)	
Public Water					Unlimited		6×10^5 gal. in tanks & 10^3 gpm indefinitely
Steam Generator Blowdown Monitor Tank							2×10^5 gal.
Service Water System			Lake (infinite)				
Primary Water Treatment Plant	3×10^6 gal.						

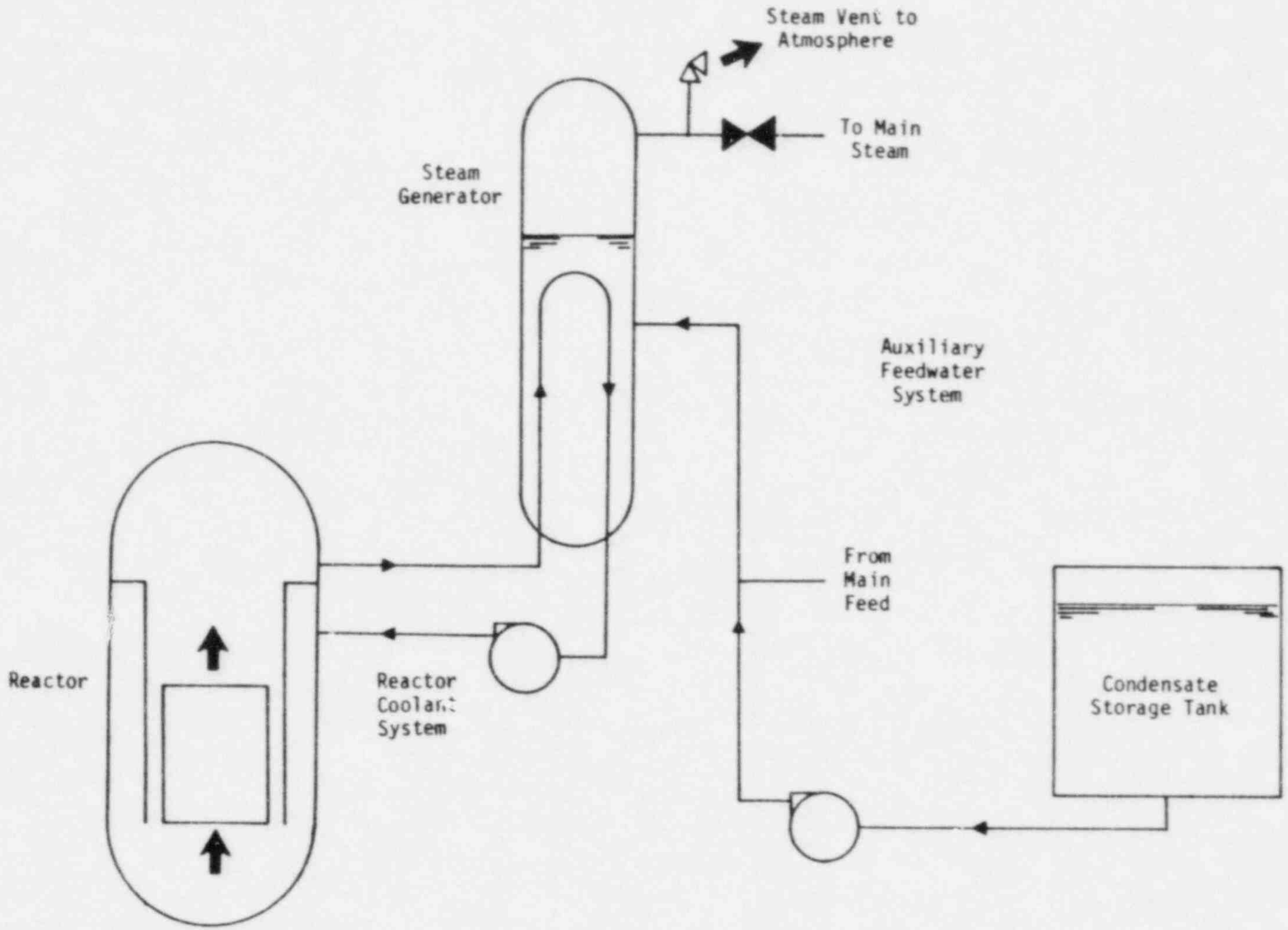


Figure 5.23.1. Residual Heat Removal Via The Auxiliary Feedwater System (from SAI01379-626LJ).

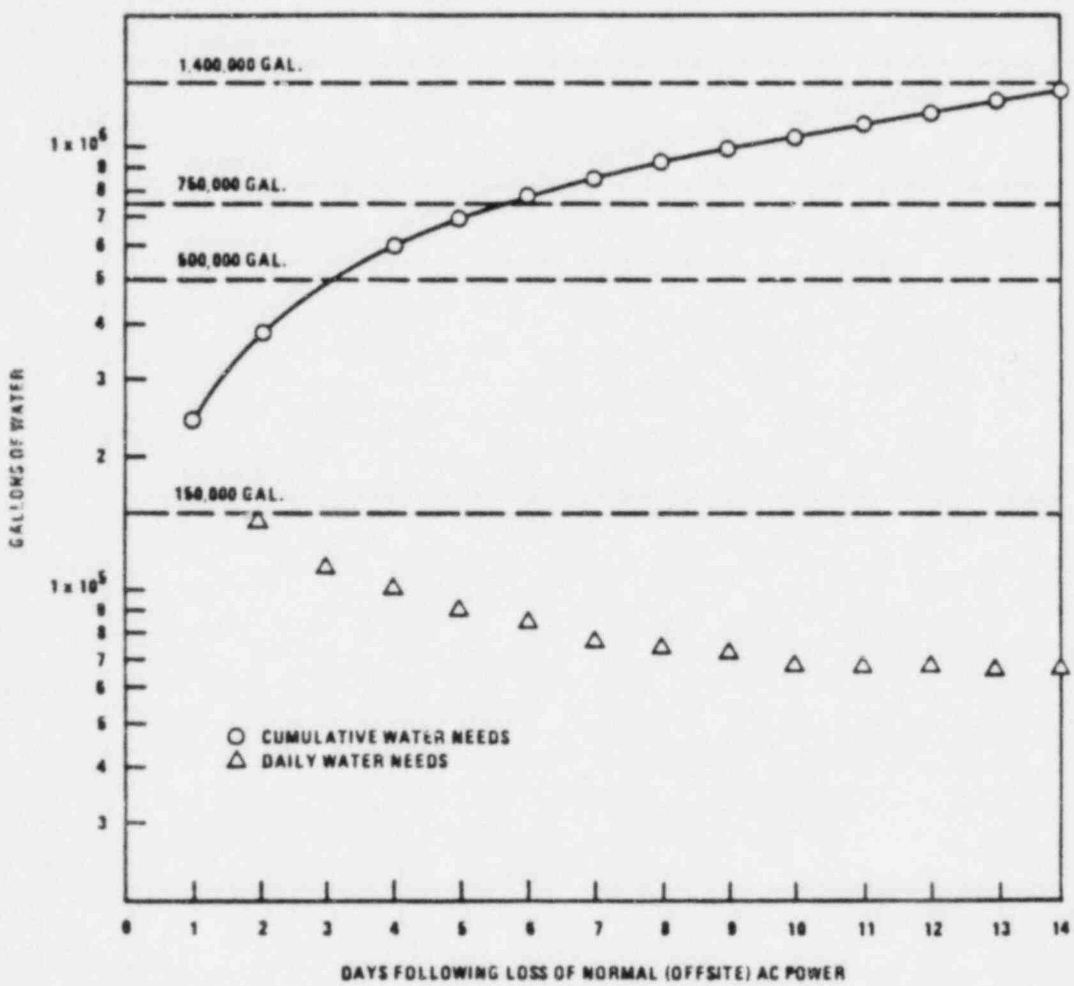


Figure 5.23.2. Steam Generator Feedwater Requirements to Achieve and Maintain Hot Shutdown Following a Loss of Offsite Power for a 1160 MWe (3390 MWt) PWR.

Additional makeup must be provided to maintain adequate reactor coolant inventory in hot shutdown. Inventory makeup requirements are dictated primarily by: (1) coolant volume reduction (e.g., "shrink") due to cooldown, and (2) main coolant pump seal leakage and any other "normal" leakage from the reactor coolant pressure boundary. Reactor coolant temperature can be controlled by modulating AFW system flow rate, thereby minimizing the effects of "shrink." Normal main coolant pump seal leakage during reactor operation is approximately 1 gpm per main coolant pump (Ref. 3). Assuming comparable leakage from a static reactor coolant pump seal at high pressure, at least 5760 gallons/day of makeup water would be required to maintain primary coolant system inventory in a hot shutdown condition. This is a small fraction of the AFW system makeup requirements and does not add significantly to the cumulative water needs indicated in Figure 5.23.2.

5.23.2.2 Decay Heat Removal at Low Pressure

The SDC system is placed in operation only when the RCS has been cooled and depressurized (e.g., to about 350°F and 350 psig) by other systems. When operating, the SDC system and the interfacing cooling systems illustrated in Figure 5.23.3 (from Ref. 1) form a complete heat transfer path from the RCS to the ultimate heat sink. The heat transfer path consists of a series of closed loop cooling systems (SDC and component cooling water systems) and a final open or closed-loop system that communicates directly with the ultimate heat sink.

The refueling water storage tank (RWST) is the normal source of RCS makeup water during cooldown and depressurization to a cold shutdown condition. After achieving cold shutdown, the makeup requirements for residual heat removal and coolant inventory control are significantly less than the requirements for long-term AFW system operation. Onsite water supplies are generally available for maintaining the plant in a cold shutdown condition for a period of at least 30 days (Ref. 4).

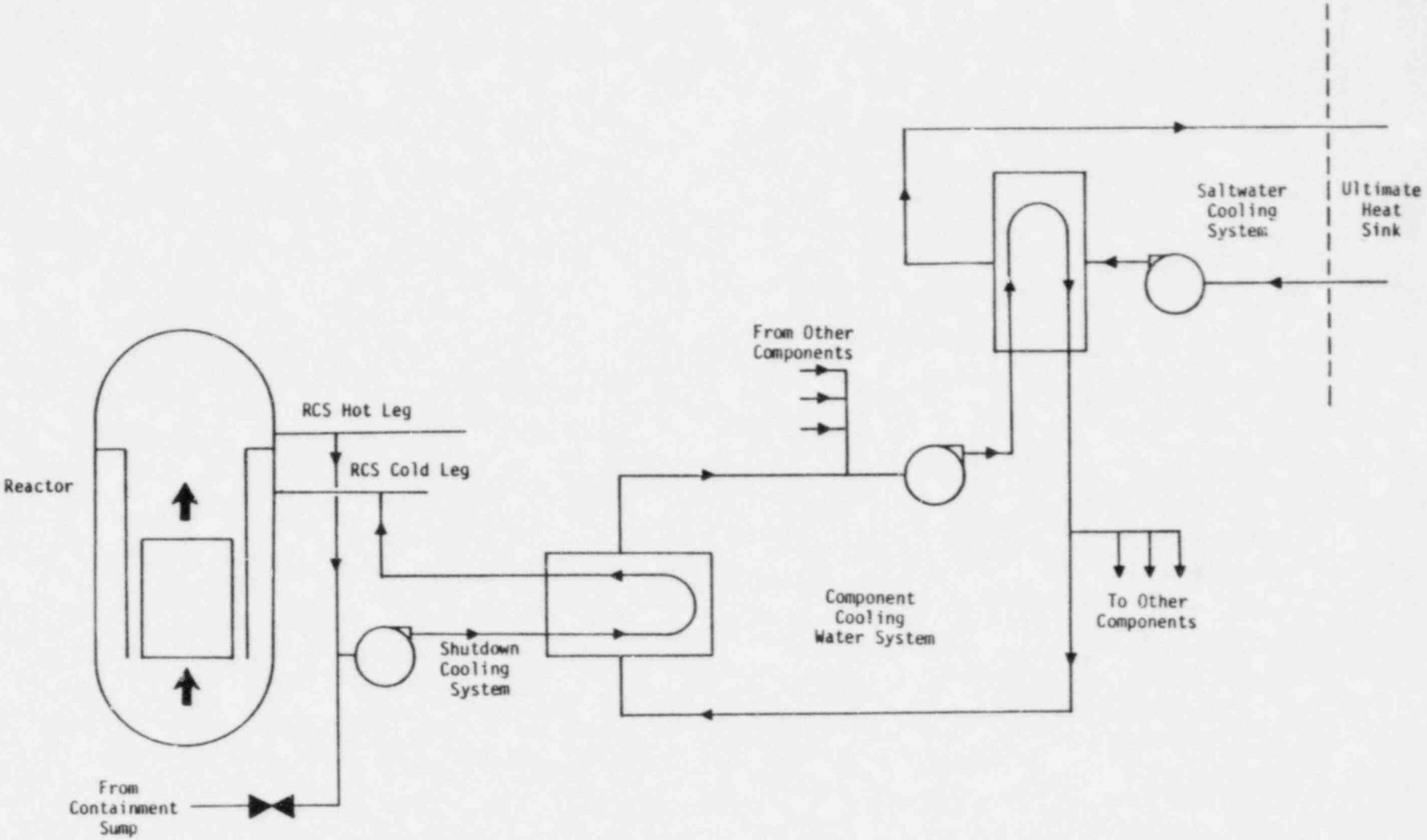


Figure 5.23.3. Residual Heat Removal Via the Shutdown Cooling System (from SAI01379-626LJ).

5.23.3 Plant Conditions During Sabotage Scenario

The steam and power conversion system is unavailable following loss of offsite power and turbine trip. Reactor core decay heat removal is being accomplished by the auxiliary feedwater system. Long-term decay heat removal with the plant in a hot shutdown condition can be accomplished by the AFW system. If the shutdown cooling system is available, the AFW system will be used to cool the RCS to the point where the SDC system can be placed in operation. This transition can usually be made three to four hours after reactor shutdown. The SDC system can establish cold shutdown conditions within 24 hours after reactor shutdown and can maintain these conditions indefinately.

5.23.4 Measures to Provide a Long-Term Water Supply for Decay Heat Removal

The NRC requires that nuclear plants have an ultimate heat sink that is capable of providing sufficient cooling for at least 30 days and that procedures exist for assuring a continued capability after 30 days. A cooling capacity less than 30 days may be acceptable if it can be demonstrated that replenishment or use of an alternate water supply can be effected to assure the continuous capability of the heat sink to perform its safety functions (Ref. 4). The determination of water requirements assumes that the plant will be placed in a cold shutdown condition.

Sabotage actions may prevent the PWR plant from transitioning to a closed-loop RHR system and achieving cold shutdown. Extended operation of the open-loop AFW system with the plant in a hot shutdown condition may therefore be necessary. Long-term maintenance of a hot shutdown condition may increase the ultimate heat sink water requirements. Recent reviews of available AFW system long-term water supplies by the NRC (Refs. 2 and 5) indicate that this concern is being addressed and that corrective actions will be taken if necessary.

Assuming that adequate water supplies are available onsite, the following general guidance should be considered when establishing the fluid system interconnections necessary to align water sources to decay heat removal systems:

- Interconnecting piping should be in-place to permit operating personnel to rapidly align alternate water sources when required. This approach maximizes operational flexibility in responding to a sabotage event without prejudging the targets that may be selected by a saboteur.

- Locked or protected isolation valves and suitable administrative controls will likely be required to prevent: (1) introduction of poor quality water during nonemergency conditions, (2) blockage of alternate makeup paths by sabotaging the isolation valves, or (3) diversion of necessary water away from a decay heat removal system by improper valve lineup.

- Pumps used to supply water from alternate sources should be capable of operating following loss of offsite power (e.g., such pumps should be powered from the Class 1E electrical system or they should be driven by a diesel engine).

- The available net positive suction head (NPSH) from an alternate water source should be compatible with the NPSH requirement of the pump utilizing the alternate water source. If necessary, a booster pump should be installed to increase the available NPSH at the main pump suction. Use of booster pumps should be minimized, as they introduce additional sabotage vulnerabilities.

- Water quality from an alternate source should be compatible with the intended use to the extent practical. Procedures should be established to segregate the alternate water sources based on expected usage for decay heat removal or reactor coolant inventory control. "Good" quality water sources for each purpose should be used first and "poor" quality water sources should be used only when other "good" quality alternate sources are not available.

5.23.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #23

None

5.23.6 Conclusions and Recommendations Regarding Damage Control Measure #23

Existing PWR plant design features provide significant long-term water sources for decay heat removal. Specific system requirements for connecting decay heat removal systems (or reactor coolant inventory control systems) to alternate water sources should be determined on an individual plant basis considering the general guidelines described in this damage control measure.

5.23.7 Section 5.23 References

1. Lobner, P., et al., "The Pressurized Water Reactor - A Review of a Typical Combustion Engineering PWR Plant," SAI01379-626LJ, Science Applications, Inc., March 23, 1979.

2. NUREG-0653, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

3. "System 80 PSAR-CESSAR," Docket STN-50470, Combustion Engineering.

4. USNRC Regulatory Guide 1.27, "Ultimate Heat Sink for Nuclear Power Plants."

5. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant-Accidents in Westinghouse-Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5.24 DAMAGE CONTROL MEASURE #24 - BWR

The purpose of damage control measure #24 is to provide alternative water sources to maintain reactor coolant inventory and to remove decay heat in the event that the normal water sources have been disabled through sabotage action.

5.24.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of the usual water sources for reactor coolant inventory control and decay heat removal. The main turbine generator trips on loss of load. The emergency diesel generators operate and supply AC power to the Class 1E buses.

5.24.2 BWR Decay Heat Removal

BWR plants have multiple decay heat removal systems capable of establishing: (1) a direct heat transfer path from the reactor core to the ultimate heat sink, or (2) an indirect heat transfer path from the reactor core to the suppression pool and finally to the ultimate heat sink. Either approach is an effective means for decay heat removal. The complement of decay heat removal systems at BWR plants is summarized in Section 5.11. These systems and their coolant makeup requirements are briefly discussed in this section.

5.24.2.1 Systems for Direct Transfer of Decay Heat to the Ultimate Heat Sink

There are four BWR decay heat removal systems that are capable of establishing a direct heat transfer path from the reactor core to the ultimate heat sink. These include:

- Main turbine bypass system (TBS)
- Isolation condenser system (ICS)
- Reactor core isolation cooling (RCIC) system operating in the steam-condensing mode
- Residual heat removal (RHR) system

The main turbine bypass system is the normal system for decay heat removal following reactor shutdown. The TBS is not available following loss of offsite power, however, and will not be discussed further. The other systems and their makeup water requirements are discussed below.

A. Isolation Condenser System

The isolation condenser system (ICS) forms a closed-loop natural circulation flow path between the reactor vessel and a condensing heat exchanger which transfers decay heat directly to the atmosphere in the form of steam which is vented from the secondary side of the condensing heat exchanger. The ICS provides for removal of decay heat following reactor shutdown when the TBS is not available and reactor coolant system (RCS) temperature is above the point at which the RHR system can be placed in operation. As indicated in Section 5.11, the isolation condenser system is found at BWR/1, BWR/2 and at some BWR/3 plants. A representative isolation condenser system is illustrated in Figure 5.24.1 (from Ref. 1).

There are two basic versions of the isolation condenser system. The more complex version has redundant isolation condenser loops, each with a heat removal capability equivalent to the decay heat level a few minutes after reactor shutdown following extended operation at full power (e.g., about 2 to 4 percent of full power). BWR/2 plants such as Oyster Creek and Nine Mile Point 1 have this type of system. Either isolation condenser loop may fail without reducing the system residual heat removal capability below required levels.

The simpler system is nonredundant, with a single condenser. It is essentially equivalent to a single loop of the redundant isolation condenser system described above. BWR/3 plants such as Millstone 1 and Dresden 2 and 3 have this type of system. If the TBS and this single isolation condenser loop are both unavailable, the core is cooled by operation of the nuclear system safety/relief valves and makeup provided by the high pressure coolant injection (HPCI) system. In this mode of core cooling, containment spray system operation would also be required to limit suppression pool temperature and containment pressure resulting from the extended blowdown from the safety/relief valves.

During power operation, the isolation condenser system is in standby with valves 1, 2 and 4 open and valve 3 closed to block flow through the system (see Figure 5.24.1). This system is actuated automatically by a reactor vessel high pressure condition (e.g., due to an inadvertent closure of the main steam isolation valves at power). A time delay of approximately 10 to 15 seconds in the actuating logic prevents brief transient high pressure conditions from spuriously actuating the system. The system may also be actuated manually from the control room or locally by opening valve 3. Only DC electric power is required by the actuation logic and by the motor-operated valves outside the drywell (valves 2 and 3). The normally open inner

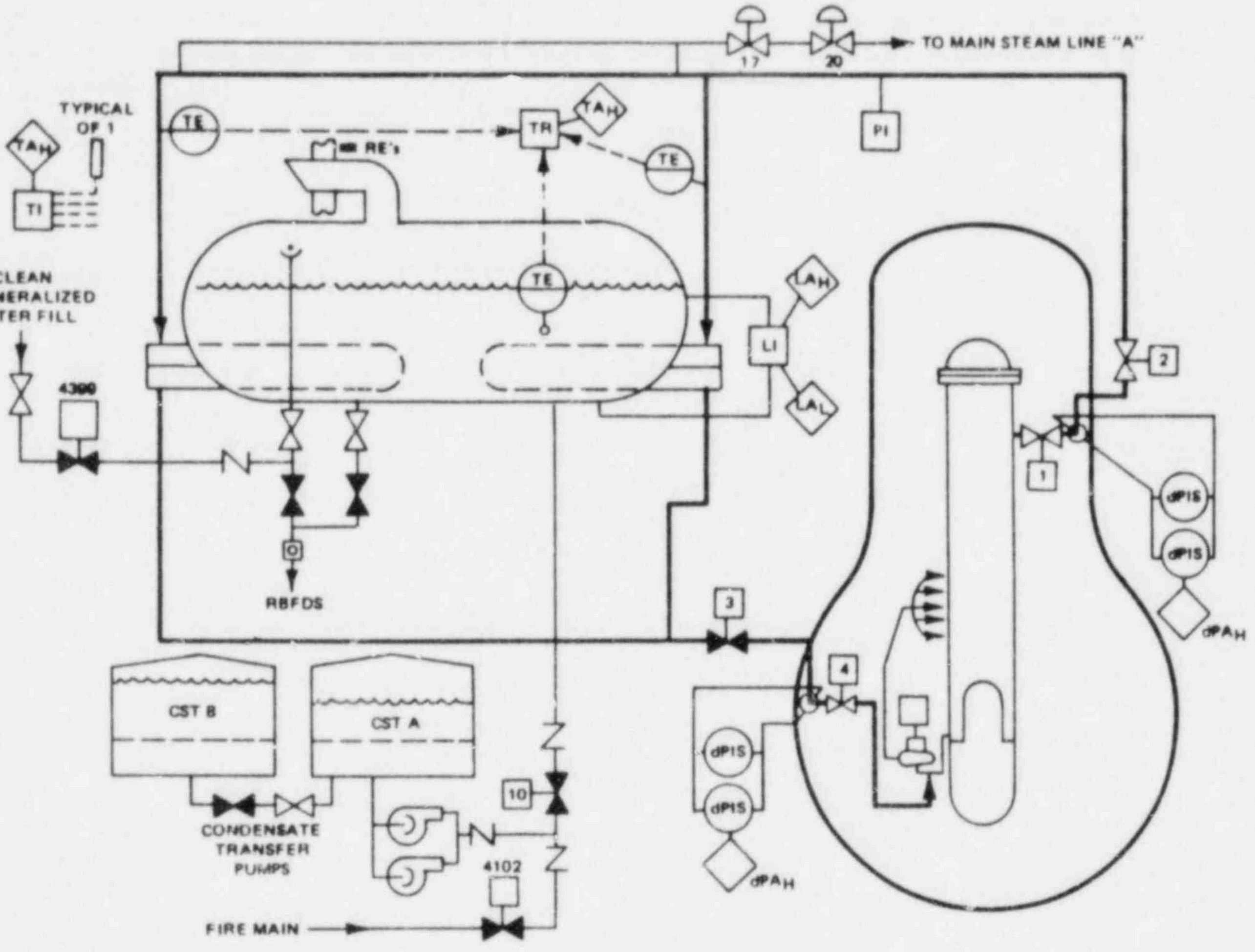


Figure 5.24.1. Isolation Condenser System (from NUREG-0626).

containment isolation valves are AC-powered. When the system is placed in operation, DC-powered valve 3 opens, establishing a natural circulation flow path for reactor cooling. Steam generated in the reactor vessel passes through containment isolation valves 1 and 2 and rises through 12 to 16 inches piping to the isolation condenser located high in the secondary containment building (e.g., about 55 to 65 feet above the core mid-plane).

In the isolation condenser, steam from the reactor vessel is condensed on the tube-side of the heat exchanger and is returned by gravity to the reactor through 6 to 8 inches piping and containment isolation valves 3 and 4. The shell-side of the isolation condenser contains a large volve (e.g., 22,000 gallons) of water, sufficient for absorbing at least 40 minutes (Ref. 1) of core decay heat by boiling at atmospheric pressure and venting to the atmosphere. After 40 minutes, additional water from any of a variety of sources (e.g., condensate system, fire water system, makeup tanks inside containment) must be provided to ensure a continuing capability for cooling the core with the isolation condenser. The maximum isolation condenser makeup rate for a 2000 MWt BWR is approximately 275 gpm. Approximately 65,000 gallons of makeup water are required for seven hours of isolation condenser operation (Ref. 2).

B. Steam-Condensing RCIC System

BWR/5 and BWR/6 plants have multi-mode RCIC systems that can be used in conjunction with the RHR heat exchangers to form a high pressure decay heat removal system. An RCIC system aligned for steam-condensing operation is illustrated in Figure 5.24.2.

Approximately one-half hour after reactor shutdown, a dual-mode RCIC system may be manually placed in the steam-condensing mode of operation. Both RHR heat exchangers are initially required for steam condensing. First the RHR heat exchangers are isolated from their previous sytem alignment (e.g., suppression pool cooling). Reactor steam is supplied to the RHR heat exchangers through pressure reducing regulating valves and the essential service water system removes heat from the RHR heat exchangers to complete the heat transfer path to the ultimate heat sink. The RCIC pump suction is realigned to draw condensate from the RHR heat exchangers and the previous water source for the pump (condensate storage tank or suppression pool) is isolated.

When core cooling has been established in the steam-consensing mode of RCIC operation, the nuclear system safety-relief valves should no longer cycle to limit primary system pressure. The rate of temperature rise in the suppression pool is therefore limited to that caused by the continuing steam exhaust from the RCIC pump turbine drive. This will result in about a $3^{0}F/hr$ heatup of the suppression pool (Ref. 3). Approximately 90 minutes after reactor shutdown, only one RHR heat exchanger is required to support steam-condensing RCIC operation. The other RHR heat exchanger may then be aligned to provide suppression pool cooling.

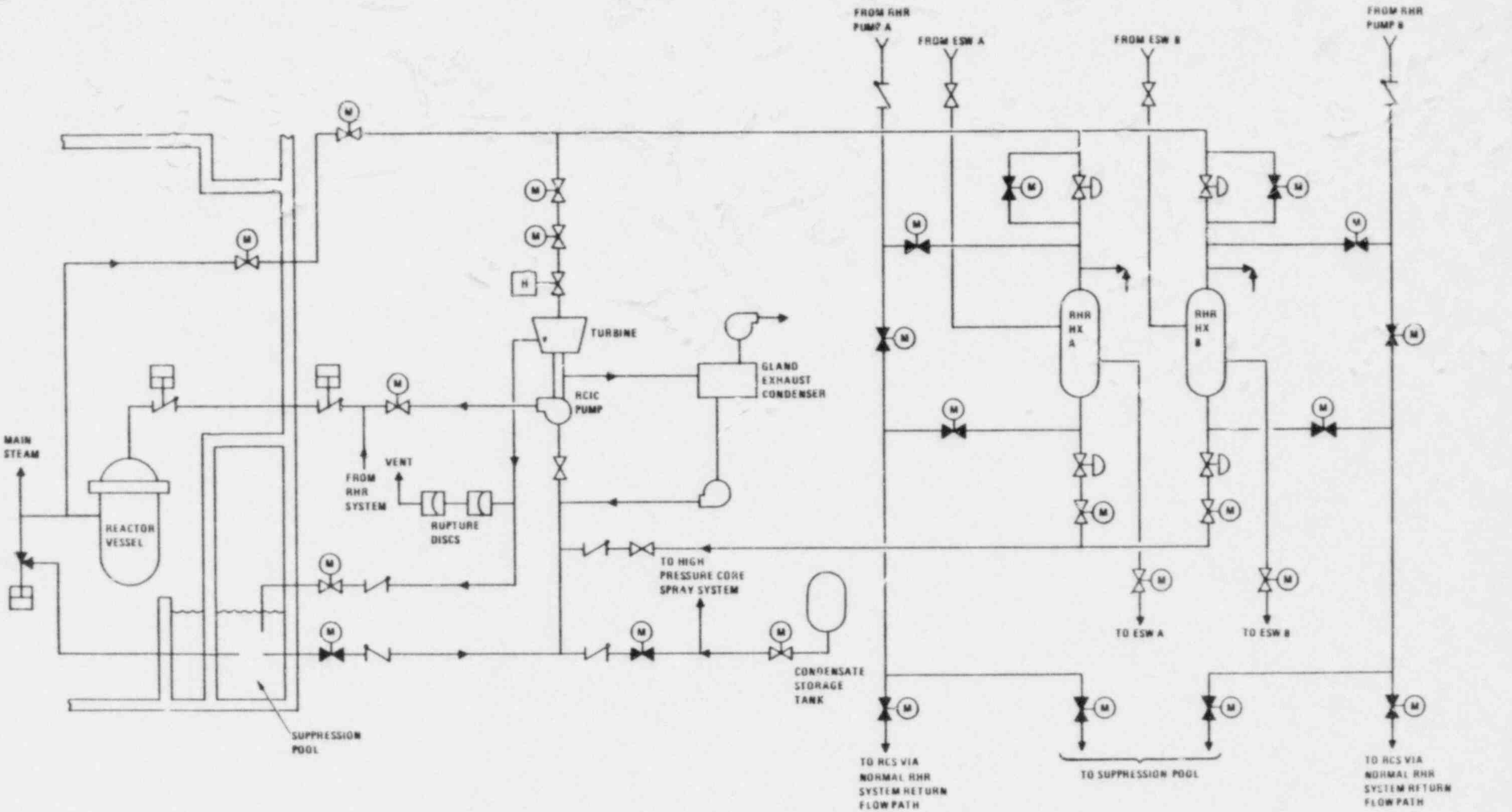


Figure 5.24.2. RCIC System Aligned for Steam-Condensing Operation (High-Pressure Decay Heat Removal).

There are no significant makeup requirements associated with the operation of a steam-condensing RCIC system. Ultimate heat sinks associated with the RHR heat exchangers (e.g., cooling towers or spray ponds) may, however, have makeup requirements that should be considered on an individual plant basis.

C. Residual Heat Removal Systems

The RHR system is described in Section 5.11. This is a closed-loop system that does not have significant makeup requirements. Ultimate heat sinks associated with the RHR heat exchangers (e.g., cooling towers or spray ponds) may have makeup requirements that should be considered on an individual plant basis.

5.24.2.2 Transfer of Decay Heat to the Ultimate Heat Sink via the Suppression Pool

This method of decay heat removal requires the availability of a high or low pressure injection system for core coolant inventory control and a heat transfer system for containment cooling. These systems may include:

- High pressure injection
  - High pressure coolant injection (HPCI) system
  - Hign pressure core spray (HPCS) system
  - Reactor core isolation cooling (RCIC) system
  - Feedwater coolant injection (FWCI) system
  - Control rod drive hydraulic system (CRDHS)
- Low pressure injection
  - Low pressure coolant injection (LPCI) system
  - Low pressure core spray (LPCS) system
  - Multi-mode residual heat removal (RHR) system operating in the injection mode
- Containment cooling
  - Containment spray system
  - Multi-mode system operating in the containment spray or suppression pool cooling mode (e.g., RHR system)
  - Suppression pool feed-and-bleed cooling

A. High and Low Pressure Coolant Injection Systems

The RCIC, HPCS and HPCI systems are described in Section 5.6. The CRDHS is described in Section 5.11 and the FWCI system is briefly discussed in Section 5.12. The LPCS and LPCI systems are discussed in Sections 5.11 and 5.12. The condensate storage tank (CST) is the normal water source for most high pressure injection systems. In some plants, the CST is also the normal water source for the LPCS system. In safety analyses, credit for the water in CST is not taken (Ref. 4), and the suppression pool is assumed to be the primary water source. The suppression pool is the normal water source for most low pressure injection systems. Available suppression pool water volumes and in-containment makeup sources are discussed in Section 5.2.

An essentially unlimited quantity of water is available for reactor coolant inventory control because of the closed loop formed by the reactor coolant system and the suppression pool (e.g., feed in from and blowdown to the suppression pool). Therefore, the availability of alternate sources of water for coolant inventory control purposes is not a significant concern.

B. Suppression Pool Cooling Systems

Systems for cooling the suppression pool are described in Section 5.2. There are no significant makeup requirements associated with conventional suppression pool cooling systems. Ultimate heat sinks associated with the system heat exchangers (e.g., cooling towers of spray ponds) may, however, have makeup requirements that should be considered on an individual plant basis. Suppression pool feed-and-bleed cooling (damage control measure #2) does have significant makeup water requirements, on the order of 75,000 gallons per hour as discussed in Section 5.2.

5.24.3 Plant Conditions During Sabotage Scenario

Following loss of offsite power and reactor scram, core decay heat is being removed by one of the systems described in Section 5.24.2. Plants with isolation condenser systems may require makeup water in approximately 40 minutes. If suppression pool feed-and-bleed is to be implemented as a damage control measure, makeup water must be available approximately 3 hours after reactor shutdown (see Section 5.2). Other BWR plants do not have significant short-term makeup water requirement beyond the water available inside containment (e.g., in the suppression pool or upper containment pool).

5.24.4 Measures to Provide a Long-Term Water Supply for Decay Heat Removal

The NRC requires that nuclear plants have an ultimate heat sink that is capable of providing sufficient cooling for at least 30 days and that procedures exist for assuring a continued capabiity after 30 days. A cooling capacity less than 30 days may be acceptable if it can be demonstrated that replenishment or use of an alternate water supply can be effected to assure the continuous capability of the heat sink to perform its safety functions (Ref. 5).

The large volume of water inside the containment of BWR plants minimizes their dependency on other makeup water sources for coolant inventory control. With the exception of the isolation condenser system, all BWR decay heat removal systems operate in a closed loop, further reducing makeup water needs. Assuming that adequate water supplies are available onsite, the general guidance in Section 5.23 should be considered when establishing the fluid system interconnections necessary to align alternate water sources to decay heat removal systems.

5.24.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #24

None

5.24.6 Conclusions and Recommendations Regarding Damage Control Measure #24

Existing BWR plant design features provide significant long-term water sources for decay heat removal. When alternate makeup water sources are required for decay heat removal, the design of system interconnections to supply the required water should consider the general guidelines in Section 5.23.

5.24.7 Section 5.24 References

1. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

2. Millstone 1 Final Safety Analysis Report, Docket 50245, Millstone Point Company.

3. "238 Nuclear Steam Supply System - GESSAR," Docket STN-50550, General Electric Company.

4. NUREG-0123, Rev. 3, "Standard Technical Specifications for General Electric Boiling Water Reactors," Section 3/4.5 (Bases), U. S. Nuclear Regulatory Commission, Fall 1980.

5. USNRC Regulatory Guide 1.27, "Ultimate Heat Sink for Nuclear Power Plants."

5.25 DAMAGE CONTROL MEASURE #25 - BWR AND PWR

The purpose of damage control measure #25 is to provide for operation of steam turbine-driven pumps such as the auxiliary feed water (AFW) pump in PWRs and the high pressure coolant injection (HPCI) and the reactor core isolation cooling (RCIC) pumps in BWRs following a loss of 125 VDC/120 VAC control power to the turbine control system. In fact, loss of control power will affect more than just the AFW, RCIC or HPCI turbine control systems. Table 5.25.1 lists the components in the turbine-driven AFW pump train and in the RCIC and HPCI systems that require 125 VDC/120 VAC power. The ability of the turbine-driven AFW pump train and the RCIC and HPCI systems to operate without DC power must therefore be addressed on a system level.

5.25.1 Sabotage Scenario

Loss of offsite power occurs coincidentally with the successful sabotage of the Class 1E DC electrical division serving the turbine-driven AFW train (PWR) and the RCIC and HPCI system (BWR). The main turbine generator trips on loss of load. The emergency diesel generators operate and supply Class 1E AC power. In addition, the motor-driven AFW train (PWR) and the feedwater coolant injection or high pressure core spray systems (BWR) are assumed to be unavailable. Their availability would preclude the need to restore the turbine-driven pumps to operation.

5.25.2 Turbine-Driven Auxiliary Feedwater Train Evaluation

5.25.2.1 Description of Auxiliary Feedwater System Operation With a Turbine-Driven AFW Pump

The AFW system provides for heat removal from the primary system via the steam generators when the main feedwater system is not available. It is capable of maint[illegible]ing the plant in a hot shutdown condition or of cooling the reactor coolant [illegible] (RCS) to the point where the residual heat removal (RHR) system can be [illegible] in operation (e.g., about 350°F and 350 psig). Normal RCS cooldown rat[illegible]he AFW system is about 75°F/hr. The switch from AFW cooling

Table 5.25.1. AFW, RCIC, and HPCI System Components Requiring DC Power.(1)

AFW	RCIC	HPCI
AFW Power-Operated Valves (motor-operated, pneumatic or hydraulic)	RCIC Motor-Operated Valves	HPCI Motor-Operated Valves
AFW Control System	RCIC Control System	HPCI Control System
AFW Auxiliary Lube Oil Pump	RCIC Inverter	HPCI Inverter
	RCIC Gland Seal Vacuum Pump	HPCI Gland Seal Vacuum Pump
	RCIC Gland Seal Condensate Pump	HPCI Gland Seal Condensate Pump
		HPCI Auxiliary Lube Oil Pump

Note: (1)Class 1E DC power is assumed to be the normal source of Class 1E 120 VAC instrumentation power (e.g., via an inverter). Loss of DC power also causes loss of 120 VAC power.

to RHR cooling can usually be made 3.5 to 5 hours after reactor shutdown. The AFW system can also be used to provide feedwater to the steam generators during normal plant startup and shutdown conditions.

The AFW system also plays an important role in mitigating some small break loss-of-coolant accidents (LOCAs). Small break LOCAs traditionally are considered to include breaks with an equivalent diameter up to six inches. Within this class of LOCAs, there are two distinctly different plant responses. Analysis predicts that PWR LOCA sizes greater than approximately two inches in diameter have the capacity to remove energy from the primary system at a rate greater than that introduced by the core decay heat source, independent of heat removal from the steam generators (Refs. 1, 2, and 3). As a result, RCS depressurization occurs, and coolant makeup can be provided by the high pressure portion of the emergency core cooling system (ECCS) or by the ECCS accumulators. Breaks smaller than two inches equivalent diameter are dependent for a portion of the heat removal function on the steam generators to depressurize the RCS. Without heat removal via the steam generators, the RCS will remain at high pressure. In this condition, many plants will be unable to provide coolant makeup with the ECCS system because reactor pressure exceeds the shutoff head of the high pressure injection pumps (see damage control measure #9).

There is wide variety in the design of AFW systems. Many of these designs are described in References 1, 2, and 4. The pump complement found in AFW systems is summarized in Table 5.25.2. As indicated in this table, the turbine-driven AFW pump is invariably rated at 100 percent capacity, and is therefore capable of delivering rated system flow to the steam generators when required. A representative AFW system is illustrated in Figure 5.2_.1.

In most PWR plants, the turbine-driven AFW pump and associated portions of the AFW system are operable on DC power alone (e.g., following loss of offsite and onsite AC power). The NRC has recommended that all plants be capable of providing the required AFW flow for at least two hours from one AFW pump train, independent of any AC power source (Recommendation GS-5 in Refs. 1 and 2).

Table 5.25.2. Summary of PWR Auxiliary Feedwater System Pump Complement.

Plant	Type(1)	Auxiliary Feedwater Pumps(2) Steam-Driven	Motor-Driven	Other(3)	Remarks
San Onofre 1	W	1(100%)	1(100%)	-	
Yankee-Rowe	W	1(100%)	-	(3)	charging & safety injection backup
Prairie Island 1 & 2	W	1(100%)	1(100%)	-	
Trojan	W	1(100%)	-	1(100%)	diesel engine-driven pump
Salem 1	W	1(100%)	2(50%)	-	
Ginna	W	1(100%)	2+2(50%)	-	2 normal + 2 standby AFW pumps
North Anna 1 & 2	W	1(100%)	2(50%)	-	per unit
Point Beach 1 & 2	W	1(100%)	1(50%)	-	per unit, motor pumps supply both units
Kewaunee	W	1(100%)	2(100%)	-	
D.C. Cook 1 & 2	W	1(100%)	1(50%)	-	per unit, motor pumps supply both units
Farley 1 & 2	W	1(100%)	2(50%)	-	per unit
H.B. Robinson	W	1(100%)	2(50%)	-	
Zion 1 & 2	W	1(100%)	2(50%)	-	per unit
Haddam Neck	W	2(100%)	-	-	
Indian Point 2 & 3	W	1(100%)	2(50%)	-	
Beaver Valley	W	1(100%)	2(50%)	-	
Turkey Point 3 & 4	W	3(100%)	-	-	3 pumps for 2 units
Surry 1 & 2	W	1(100%)	2(50%)	-	
Arkansas Nuclear One-2	C-E	1(100%)	1(100%)	-	
Calvert Cliffs 1 & 2	C-E	2(100%)	-	-	per unit
Fort Calhoun	C-E	1(100%)	1(100%)	-	
Maine Yankee	C-E	1(100%)	2(100%)	-	
Millstone 2	C-E	1(100%)	2(50%)	-	
Palisades	C-E	1(100%)	1(100%)	-	
Saint Lucie 1	C-E	1(100%)	2(50%)	-	
Three Mile Island 1 & 2	B&W	1(100%)	2(50%)	-	per unit
Crystal River	B&W	1(100%)	1(100%)	-	
Oconne 1, 2 & 3	B&W	1(100%)	-	-	per unit, 3 total
Rancho Seco	B&W	-	1(100%)	1(100%)	motor & turbine tandem
Davis Besse	B&W	2(100%)	-	-	
Arkansas Nuclear One-1	B&W	1(100%)	1(100%)	-	

Notes:

(1) W = Westinghouse, C-E = Combustion Engineering, B&W = Babcock & Wilcox

(2) Data includes number of pumps and, in parentheses, the pump capacity as a percentage of rated system flow.

(3) See remarks

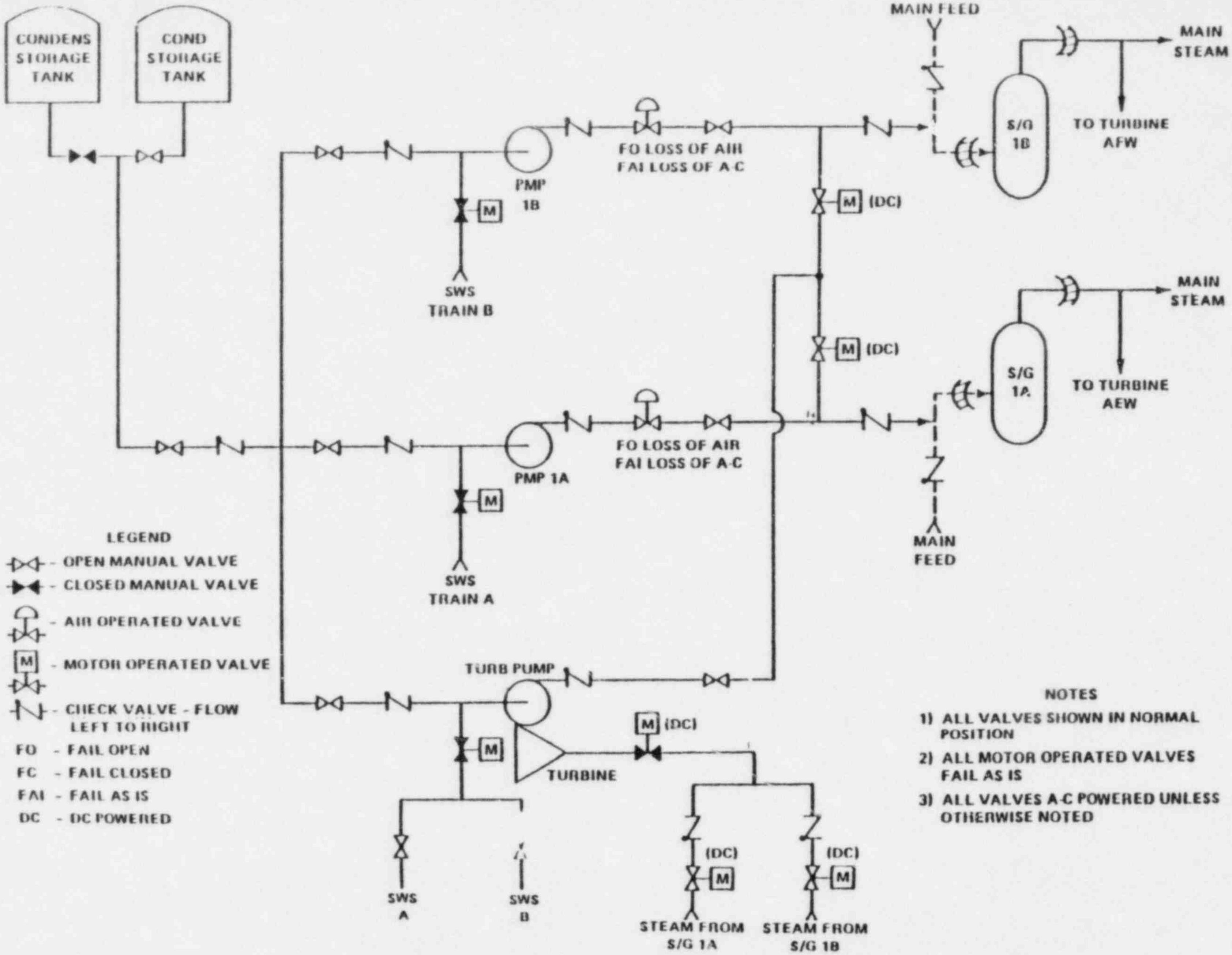


Figure 5.25.1. Auxiliary Feedwater System, Kewaunee Nuclear Plant (from NUREG-0611).

To actuate the turbine-driven AFW train, all that is required in many plants is to open one or more valves in: (1) the turbine steam supply line, and (2) each makeup path from the turbine-driven pump to the steam generators. There currently is no safety requirement that the turbine-driven train of the AFW system be operable following loss of DC power. None of the turbine-driven trains of the AFW systems described in References 1, 2, and 4 appear to be capable of operation in the absence of DC power. The features that preclude operation of the turbine-driven AFW train without DC power may include one or more of the following:

- Loss of power to the turbine control system, preventing turbine startup.
- Valve(s) in turbine steam supply line fail in the closed position preventing turbine startup.
  - Normally closed AC or DC motor-operated valve fails as-is when electric power is lost
  - Normally open or closed pneumatic or hydraulic valve fails losed when DC power is lost
- Valve(s) in the pump discharge line fail in the closed position preventing proper alignment of the pump discharge.
- Loss of DC power to an auxiliary lube oil pump required for turbine-driven pump startup (e.g., to open trip/throttle or governor valve and/or for tilting-pad thrust bearing pressure lubrication). Most AFW pumps and turbines do not require a pressure lubrication system for startup.

Other features that may preclude effective operation of a turbine-driven AFW pump train without AC or DC power include the following:

- Loss of turbine and/or pump cooling water from a separate system (e.g., a component cooling water system) following loss of AC power. Most AFW pumps are cooled by water diverted from their own discharge.
- Loss of AFW pump room ventilation and cooling following loss of AC power may limit long-term operability of the AFW system.
- Inability to operate the main steam dump valves without DC power.
- Lack of local indication of steam generator level and AFW flow rate.
- Lack of adequate illumination to facilitate local manual operations in the AFW pump room (e.g., AFW flow throttling, AFW pump start/stop).

- Lack of personnel training and emergency operating procedures for operation of the AFW system in this mode (e.g., without AC or DC power).

5.25.2.2 AFW System Conditions During Sabotage Scenario

The AFW system is inoperable. Steam generator pressure is at its safety valve setpoint, and the steam generators are boiling down as heat is being removed from the RCS. The steam generators have been calculated to boil dry in 14 to 43 minutes (Refs. 1 and 2) following loss of normal feedwater with no makeup from the AFW system. The reactor core may be uncovered to its midplane in approximately 120 minutes following loss of feedwater and no coolant makeup to the RCS (Ref. 5).

5.25.2.3 AFW System Alignment Necessary for Operatory Without AC or DC Power

To provide effective AFW system operation without AC or DC power, system design features must circumvent the failure modes and operational difficulties described previously. A turbine-driven AFW train incorporating design features to permit operation following loss of AC and DC power is illustrated in Figure 5.25.2. Specific design features include the following:

- Governor and turbine speed control system failure mode permits turbine startup without DC power.
  - The failure mode of electric-hydraulic and electronic governors on loss of control power should allow the turbine to startup and run on the backup ballhead governor alone.
  - Mechanical-hydraulic governors do not require electric power, except for a speed setting motor and a shutdown solenoid, if provided. Speed setting can be accomplished manually at the governor. The shutdown solenoid should be "energize-to-shutdown."
- All turbine protective trips (e.g., overspeed) are mechanically actuated.
- Valves in the AFW turbine steam supply line have the following characteristics:
  - Turbine governor and trip/throttle valves are normally open. The trip/throttle valve, which may be reset (reopened) remotely with a DC motor, fails as-is upon loss of DC power

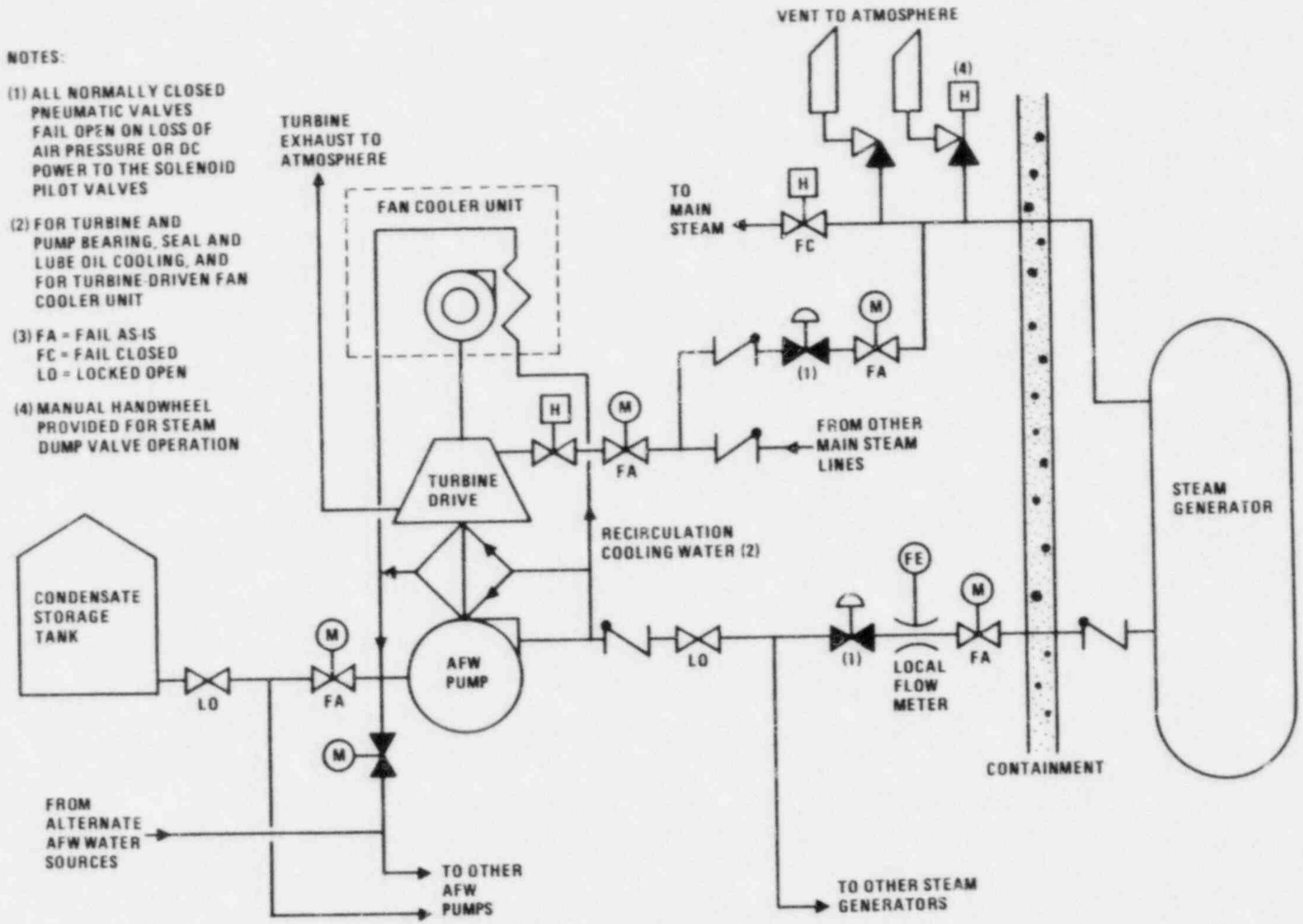


Figure 5.25.2. Turbine-Driven AFW Pump Train Designed for Operation Without AC or DC Power.

- A normally closed pneumatic steam line shutoff valve fails open upon loss of DC power. This valve is upstream of the trip/throttle and governor valves.

- A normally open AC motor-operated containment isolation valve fails as-is on loss of AC power.

- Valves in the AFW pump discharge line have the following characteristics:

  - A normally closed pneumatic flow control valve fails open on loss of DC power

  - A normally open AC motor-operated containment isolation valve fails as-is on loss of AC power.

- A pressure lube oil system is not required by the pump or turbine (e.g., a ring-oil or gear driven lubrication system is provided, ball-type thrust bearing is used).

- The AFW pump and turbine are cooled by water diverted from the pump discharge, and returned to the pump suction. Water for the AFW system would be supplied from the condensate storage tank or other source which would be at or near ambient temperature.

- Required pump room cooling is provided by a mechanically-driven fan cooler unit. The fan is driven by the AFW turbine (e.g., direct or belt drive) and the radiator is cooled by water diverted from the pump discharge and returned to the pump suction (see Figure 5.25.2). This capability may not be required if heat input to the pump room can be sufficiently reduced by measure such as:

  - Increased insulation of turbine steam supply and exhaust lines and valves.

  - Piping the turbine gland seal drains to a location outside the AFW pump room.

- Steam dump valves are provided with a local-manual operation capability (see damage control measure #5).

- Local indication of steam generator level is provided (either in the AFW pump room, or at some other location which can communicate with an operator in the AFW pump room, see damage control measure #17). Local indication of AFW flow rate is provided.

- Emergency DC lighting, independent of the Class 1E DC power system, is provided in the AFW pump room (e.g., small battery powered lanterns).

In addition, an adequate communications system (e.g., hand-held radios) and emergency operating procedures must be available.

An inadvertent actuation of the AFW system during normal power operation will occur following a loss of the Class 1E DC division which powers components in a turbine-driven AFW train having the design features described in this section. With AC power available, the AC motor-operated valves in the steam supply and pump discharge lines can be closed to terminate this unintended actuation of the AFW system.

If inadvertent AFW makeup to the steam generators following loss of a DC division is unacceptable, one or more valves in the turbine steam supply line should be designed to fail closed. Timely operator response will be necessary, however, the remaining AFW design changes should minimize the number and complexity of operator actions necessary to manually place the AFW system in operation.

5.25.3 Reactor Core Isolation Cooling System Evaluation

5.25.3.1 Description of Reactor Core Isolation Cooling System Operation

The RCIC system (found in BWR/3 to BWR/6 plants) is normally in standby. During power operation, reactor coolant inventory control is maintained by the feedwater system, with some minor additional makeup from normal control rod drive hydraulic system leakage into the reactor coolant system. The RCIC system is actuated automatically on reactor vessel low water level. The single, 100 percent capacity, turbine-driven RCIC pump is intended to provide adequate core cooling when the reactor vessel is isolated from the main condenser (e.g., the main steam isolation valves are closed) and normal feedwater flow is lost. In this condition, the reactor coolant system will be at high pressure, with energy being removed by blowdown through the safety valves to the suppression pool. Continued RCIC system operation in the injection mode will cause a fairly rapid heatup of the suppression pool, necessitating the actuation of suppression pool cooling systems or the changeover to the closed-loop steam-condensing mode of RCIC system operation (found in BWR/5 and BWR/6 plants). In this mode of RCIC operation, energy is removed from the reactor coolant system via the residual heat removal (RHR) heat exchangers operating in the steam-condensing mode. The safety valves will close, and suppression pool heatup rate will be reduced to approximately $3^{O}F/hr$ from RCIC turbine exhaust. Requirements for suppression pool cooling can thereby be postponed. The RCIC system is not considered as part of the emergency core cooling system (ECCS). A typical RCIC system is illustrated in Figure 5.25.3. BWR plants having an RCIC system are listed in Table 5.25.3.

The RCIC system operates independently of AC power, plant service air and external cooling water systems. Cooling water for the pump, turbine, lube oil cooler, and gland seal barometric condenser is supplied from the discharge of the pump. System valves and auxiliary pumps (e.g., condensate and vacuum pumps for the gland seal barometric condenser) operate on DC power. The RCIC pump room space cooling system does, however, require AC power for operation. Long-term operation of the RCIC system may require space cooling to maintain pump room temperatures within allowable limits (Ref. 6). The NRC has recommended that the RCIC system should be designed to withstand a complete loss of AC power to its support systems, including he space cooler system, for at least two hours (Recommendation B.3 in Ref. 6).

To place an RCIC system in operation, normally closed DC motor-operated valves in the steam supply, pump discharge and pump recirculation lines must be opened and DC-powered condensate and vacuum pumps for the gland seal barometric condenser must be started. In this lineup, the system is drawing a suction on the condensate storage tank which can typically support about eight hours of RCIC system operation. The suppression pool is the alternate source of water for the RCIC system. The RCIC system is not designed to be operable following loss of DC power to the system (e.g., loss of Class 1E C Division 1). System features that preclude operation without DC power may include one or more of the following:

- Loss of power to the turbine control system, preventing turbine startup.
- Normally closed DC motor-operated valves in the RCIC steam supply line and pump discharge line fail as-is (closed) when DC power is lost, preventing turbine startup and proper alignment of the pump discharge.
- Normally closed DC motor-operated valve in the RCIC cooling water recirculation line fails as-is (closed) when DC power is lost, preventing cooling water from reaching the lube oil cooler.

Table 5.25.3. BWR High Pressure Coolant Injection Systems.(1)

	BWR Type	RCIC	HPCI	HPCS	FWCI
Dresden 1	1	-	(2)	-	-
Humboldt Bay	1	-	-	-	X
Big Rock Point	1	-	-	-	-
Oyster Creek	2	-	-	-	-
Nine Mile Point	2	-	-	-	X
Millstone 1	3	-	-	-	X
Dresden 2 & 3	3	-	X	-	-
Pilgrim	3	X	X	-	-
Monticello	3	X	X	-	-
Quad Cities 1 & 2	3	X	X	-	-
Hatch 1 & 2	4	X	X	-	-
Browns Ferry 1, 2 & 3	4	X	X	-	-
Vermont Yankee	4	X	X	-	-
Peach Bottom 2 & 3	4	X	X	-	-
Cooper	4	X	X	-	-
Duane Arnold	4	X	X	-	-
Fitzpatrick	4	X	X	-	-
Brunswick 1 & 2	4	X	X	-	-
Shoreham	4	X	X	-	-
Fermi 2	4	X	X	-	-
Susquehanna 1 & 2	4	X	X	-	-
LaSalle 1 & 2	5	X	-	X	-
Zimmer	5	X	-	X	-
Handford 2	5	X	-	X	-
Grand Gulf 1 & 2	6	X	-	X	-
Other BWR/5 & /6		X	-	X	-

Note: (1)RCIC = reactor core isolation cooling system; HPCI = high pressure coolant injection system; HPCS = high pressure core spray system; FWCI = feedwater coolant injection system.

(2)Being installed

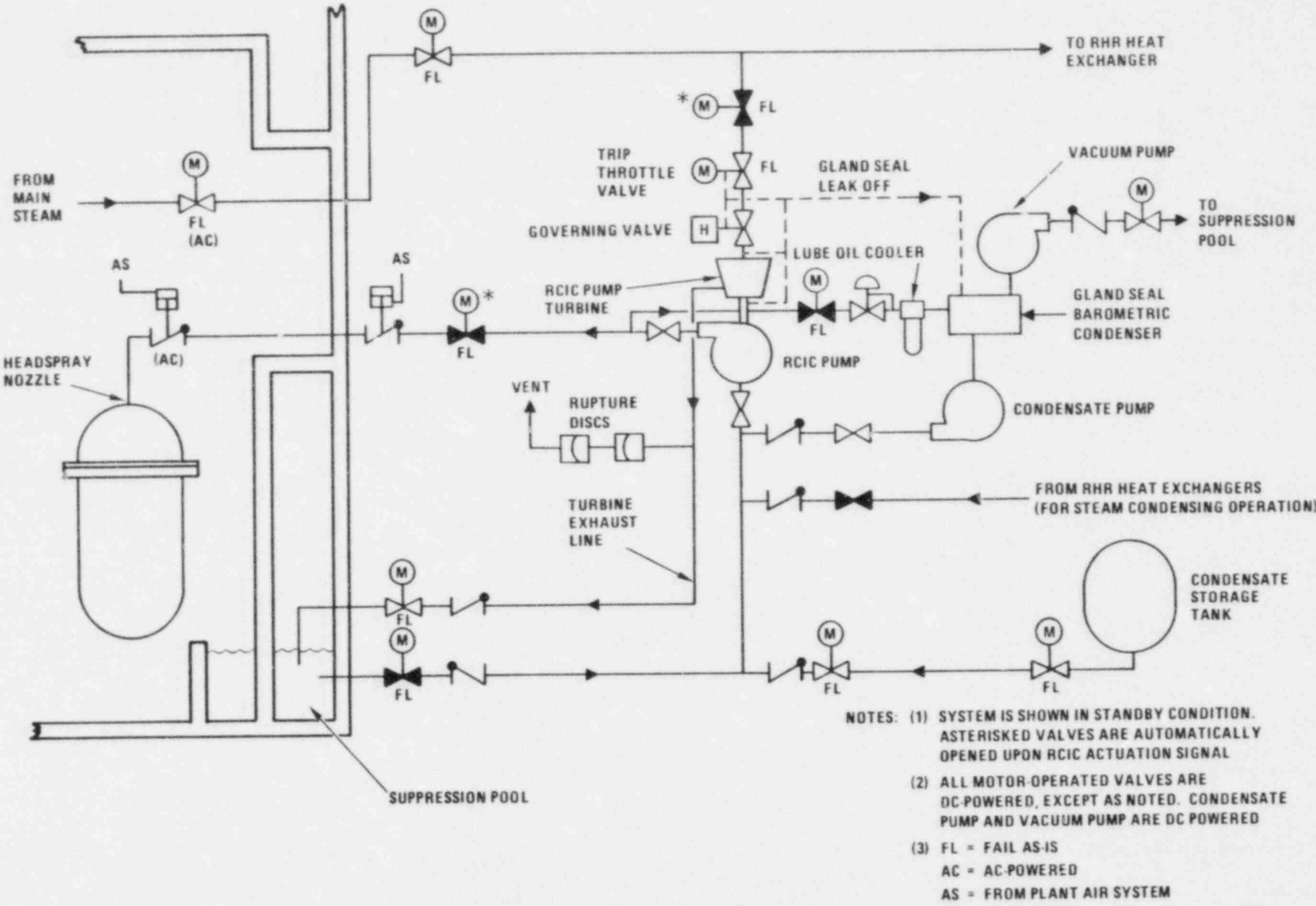


Figure 5.25.3. Typical RCIC System.

Other features that may preclude effective operation of an RCIC pump without AC and DC power include the following:

- Loss of DC-powered condensate and vacuum pumps for the gland seal barometric condenser may result in the RCIC pump room being uninhabitable because of steam (and consequently, airborne radioactivity) leakage into the pump room from the gland seals of the RCIC turbine and its governing and trip throttle valves.

- High radiation level in the RCIC pump room during system operation may limit occupancy.

- Loss of room ventilation and cooling following loss of AC power may limit long-term operability of the RCIC system.

- Lack of appropriately positioned local indication of reactor vessel level and RCIC flow rate.

- Lack of adequate illumination, communications and emergency procedures, as described previously.

5.25.3.2 RCIC System Conditions During Sabotage Scenario

The RCIC system is inoperable following loss of DC power to the system. As a minimum, Class 1E DC Division 1 is assumed to be unavailable. If loss 1E electrical Division 3 has not also been sabotaged, the high pressure injection portion of the emergency core cooling system (ECCS) (e.g., the HPCI or the high pressure core spray system) would be available and would provide adequate core cooling without restoring the RCIC system to operation. These systems are also assumed to be unavailable.

Reactor vessel water level will be dropping rapidly. When level drops to approximately 1.5 feet above the top of the core (e.g., Level 1), the automatic depressurization system (ADS) normally would be actuated and makeup would be provided by the low pressure injection systems. The ADS or the low pressure injection systems are assumed to fail, thus forcing reliance on the RCIC system. This scenario is comparable to plant conditions resulting from a station blackout (e.g., loss of offsite and onsite AC power). It has been estimated that, under these circumstances, the reactor coolant level will drop to the core midplane in approximately 1.4 hours (Ref. 5).

5.25.3.3 RCIC System Alignment Necessary for Operation Without AC or DC Power

To provide effective RCIC system operation without AC or DC power, system design features must circumvent the failure modes and operational difficulties described previously. An RCIC system incorporating design features to permit operation following loss of AC and DC power is shown in Figure 5.25.4. Specific design features include the following:

- The failure mode of the governor and turbine speed control system on loss of control power should permit the turbine to startup and run on the back-up ballhead mechanical governor.

- All turbine protective trips (e.g., overspeed, high exhaust backpressure) are mechanically actuated.

- Normally closed DC motor-operated valves in the turbine steam supply line, pump discharge line and pump recirculation line are replaced with normally closed, fail open pneumatic valves.

    - A suitable accumulator air supply system could be provided to prevent unintended RCIC startups following loss of the normal air system used for valve operation (see Figure 5.25.4).

    - A manual handwheel capability for the new steam line shutoff and the pump discharge pneumatic valves is provided to permit manual stop/start of the pump and manual throttling of the pump discharge from outside the RCIC pump room following loss of DC power. This will minimize radiation exposure to personnel during local RCIC system operation. These handwheels would require physical protection. If the handwheels were inadvertently moved to the closed position while the valves were in their normally closed position (e.g., air pressure is holding them closed), the fail safe mode of the valves (e.g., fail open) would be defeated.

- The condensate and vacuum pumps for the gland seal barometric condenser are directly driven by the RCIC turbine.

- Required pump room cooling is provided by a mechanically-driven fan cooler unit as described previously for the AFW system. Adequate room cooling can be provided while the system is being supplied by the condensate storage tank. An alternative approach for room cooling would be required when the system takes a suction on the suppression pool which may be at a significantly higher temperature than the condensate storage tank.

- Local indication of reactor vessel level and RCIC flow are provided outside the RCIC pump room, near the manual handwheels for the turbine steam supply and pump discharge valves.

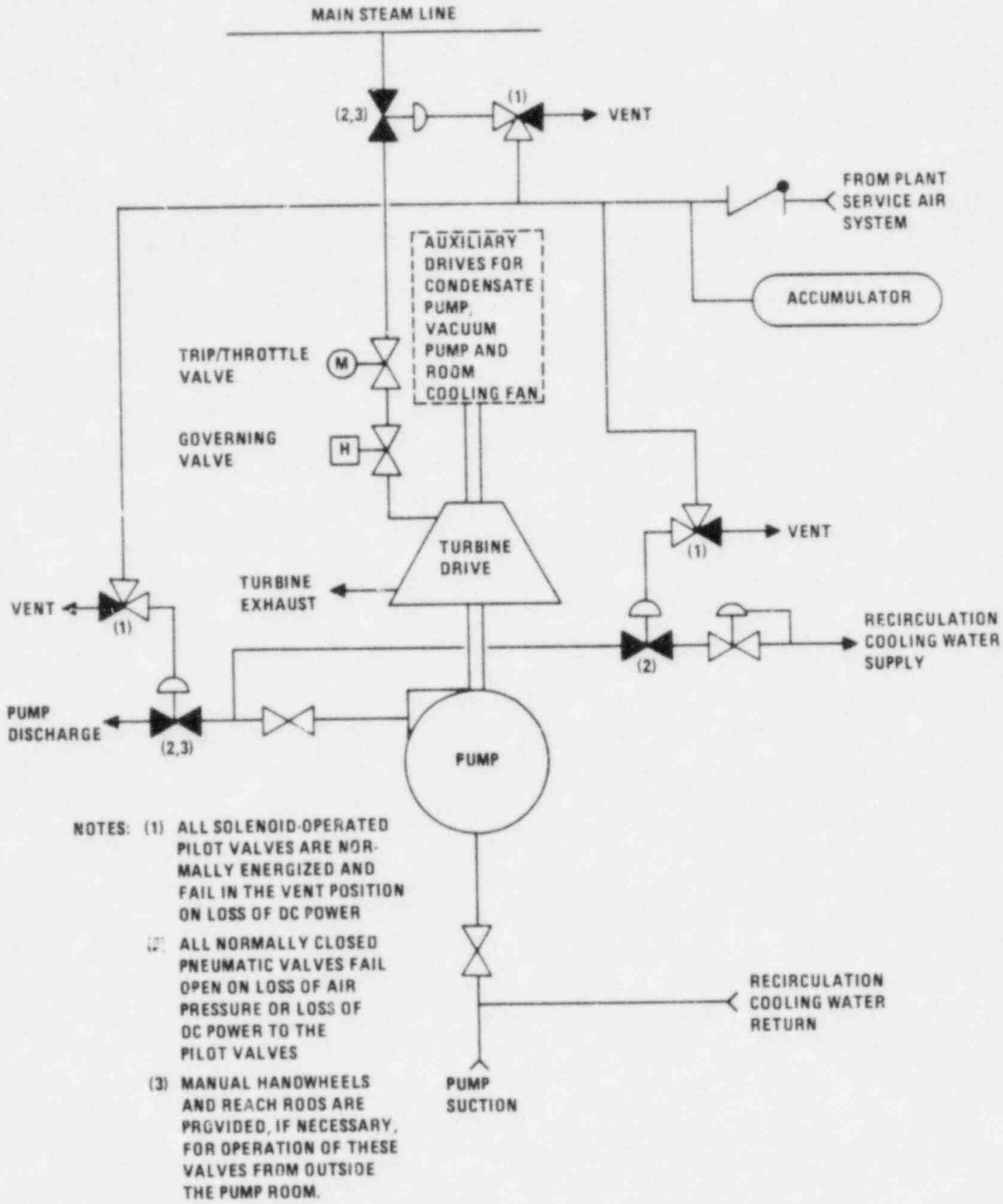


Figure 5.25.4. Some of the Design Changes Required For Operation of RCIC and HPCI Systems Without AC or DC Power.

- Emergency DC lighting, adequate communications and emergency operating procedures are provided

During normal power operation, a spurious loss of Class 1E DC Division 1 will cause an unintended startup of an RCIC system with these design features. With AC power available, containment isolation valves in the steam supply and pump discharge lines can be closed to terminate this unintended actuation of the RCIC system.

If inadvertent RCIC makeup to the RCS following loss of DC Division 1 is unacceptable, one or more valves in the turbine steam supply line should be designed to fail closed. Timely operator response will be necessary, however, the remaining RCIC design changes should minimize the number and complexity of operator actions necessary to manually place the RCIC system in operation.

5.25.4 High Pressure Coolant Injection System Evaluation

5.25.4.1 Description of High Pressure Coolant Injection System Operation

The HPCI system (found in BWR/3 and BWR/4 plants) is normally in standby. This system is part of the ECCS, and is automatically actuated on either reactor vessel low water level or high drywell pressure. The single, 100 percent capacity, turbine-driven HPCI pump is intended to provide adequate coolant inventory in the reactor vessel for a spectrum of LOCA conditions that do not result in rapid depressurization of the reactor coolant system. By design, the system also serves as a backup to the injection mode of the RCIC system. HPCI flow rate is approximately five to eight times that of the RCIC system at comparable pump head (e.g., 1130 psid). A typical HPCI system is illustrated in Figure 5.25.5 (from Ref. 6). BWR plants having a HPCI system are listed in Table 5.25.3.

The HPCI system operates independently of AC power, plant service air and external cooling systems. Like the RCIC system, cooling water for the pump, turbine, lube oil cooler, and gland seal barometric condenser is supplied from the pump discharge. System valves and auxiliary pumps (e.g., condensate and vacuum pumps for the gland seal barometric condenser and an auxiliary lube oil

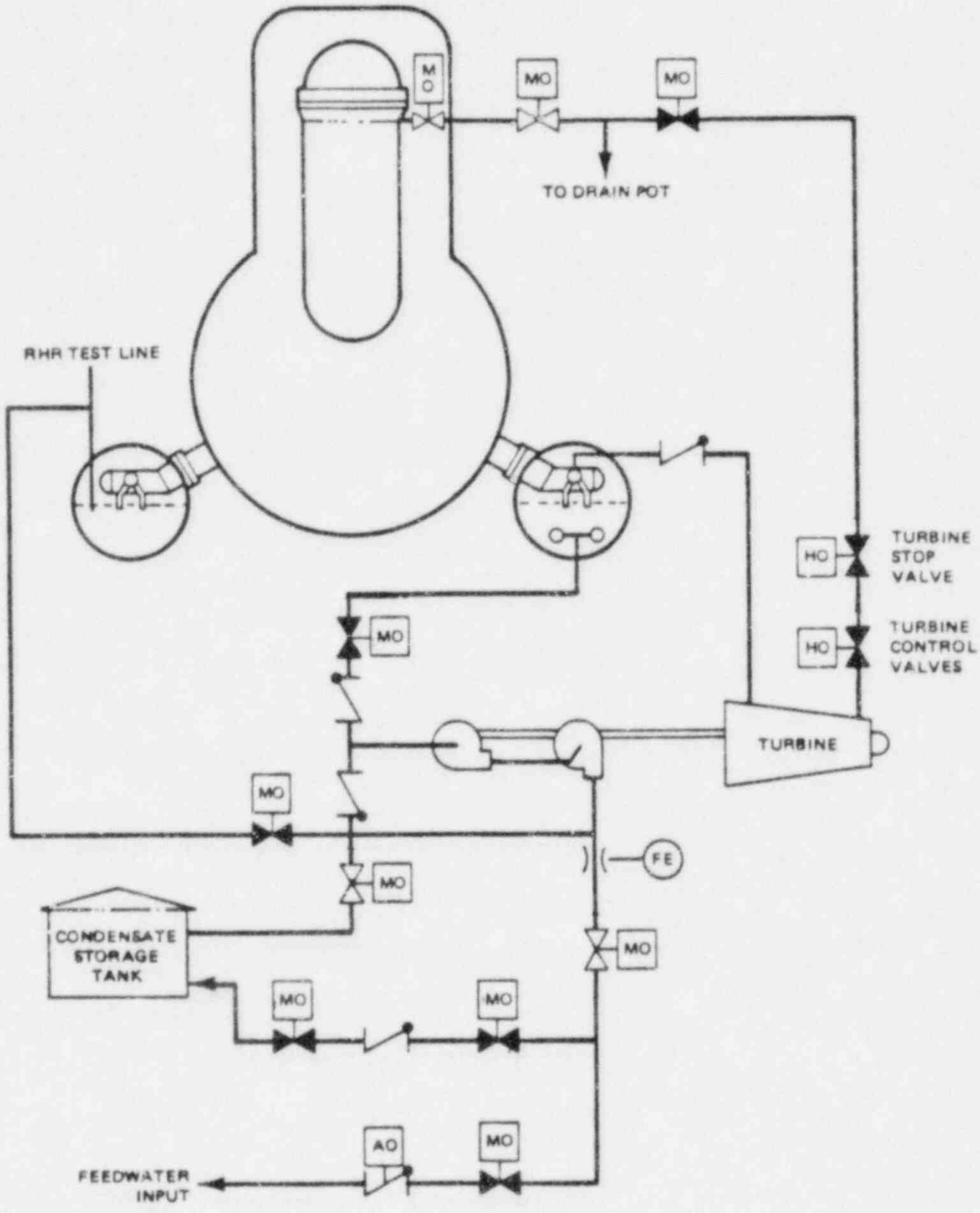


Figure 5.25.5. High Pressure Coolant Injection (HPCI) System (From NUREG-0626).

pump for opening the turbine stop turbine control valves and for bearing pressure lubrication) operate on DC power. The HPCI pump room space cooling system does, however, require AC power for operation. Long-term operation of the HPCI system may require space cooling to maintain pump room temperatures within allowable limits (Ref. 6). The NRC has recommended that the HPCI system should be designed to withstand a complete loss of AC power to its support systems, including lthe space cooler system for at least two hours (recommendation B.3 in Ref. 6).

To place an HPCI system in operation, normally closed DC motor-operated valves in the steam supply, pump discharge and pump recirculation lines must be opened. The DC-powered auxiliary lube oil pump must start and open the turbine stop and control valves. Once open, the turbine will start, and a shaft-driven lube oil pump then maintains lube oil pressure. The DC lube oil pump will then shutdown. The DC-powered condensate and vacuum pumps for the gland seal barometric condenser must also be started. In this lineup, the HPCI system is drawing a suction on the condensate storage tank which can typically support about an hour of HPCI system operation. The suppression pool is the alternate source of water for the HPCI system.

The HPCI system is not designed to be operable following loss of DC power to the system (e.g., loss of Class 1E DC Division 3). System features that preclude operation of the HPCI system without DC power may include one or more of the following:

- Loss of power to the turbine control system, preventing turbine startup.
- Valves in turbine steam supply line fail in the closed position, preventing turbine startup.
  - Normally closed DC motor-operated HPCI steam line supply valve fails as-is when DC power is lost.
  - Auxiliary lube oil pump is inoperable when DC power is lost and no hydraulic pressure is available to open the turbine stop and control valves.
- Normally closed DC motor-operated valve in HPCI pump discharge line fails as-is (closed) when DC power is lost, preventing the proper alignment of the pump discharge.

- Normally closed DC motor-operated valve in the HPCI cooling water recirculation line fails as-is (closed) when DC power is lost, preventing cooling water from reaching the lube oil cooler.

Other features that may preclude effective operation of a HPCI pump without AC and DC power include the following:

- Loss of DC-powered condensate and vacuum pump for the gland seal barometric condenser may result in the HPCI pump room being uninhabitable because of steam (and consequently, airborne radioactivity) leakage into the pump room from the gland seals of the HPCI turbine and its stop and control valves.
- High radiation level in the HPCI pump room during system operation may limit occupancy.
- Loss of room ventilation and cooling following loss of AC power.
- Lack of appropriately positioned local indication of reactor vessel level and HPCI flow rate.
- Lack of adequate illumination, communications and emergency procedures, as described previously.

5.25.4.2 HPCI System Conditions During Sabotage Scenario

The HPCI system is inoperable following loss of DC power to the system. As a minimum, Class 1E DC Division 3 is assumed to be unavailable. If Class 1E DC Division 1 has not also been sabotaged, the RCIC system may be available and would provide adequate core cooling for some events (e.g., non-LOCAs) without restoring the HPCI system to operation. The RCIC is, however, also assumed to be unavailable.

Reactor vessel water level will be dropping rapidly. When the level drops to approximately 1.5 feet above the top of the core (e.g., Level 1), the automatic depressurization system (ADS) would normally be actuated and makeup would be provided by the low pressure injection systems. The ADS or the low pressure injection systems are assumed to fail, thus forcing reliance on the HPCI system. This scenario is comparable to plant conditions resulting from a station blackout (e.g., loss of offsite and onsite power). It has been estimated that, under these circumstances, the reactor coolant level will drop to the core midplane in approximately 1.4 hours (Ref. 5).

5.25.4.3 HPCI System Alignment Necessary for Operation Without AC or DC Power

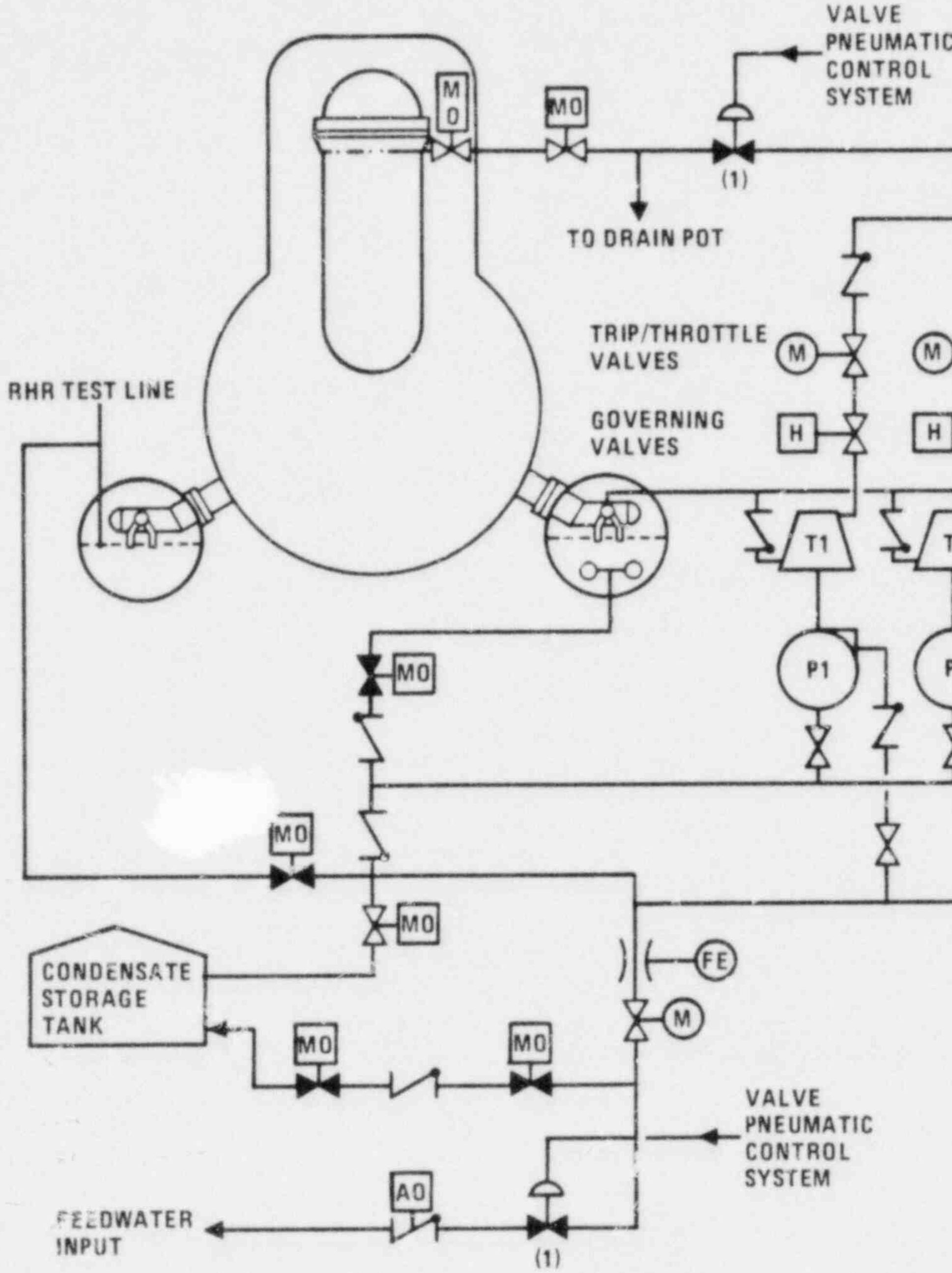
To provide effective HPCI system operation without AC or DC power, system design features must circumvent the failure modes and operational difficulties described previously. A major design difficulty relates to the size and auxiliary system requirements of the HPCI turbine. Because of the high horsepower rating of the HPCI turbine ball-type thrust bearings, as used in RCIC and most AFW turbines, are inadequate. Tilting-pad thrust bearings (e.g., Kingsbury-type) are found on HPCI turbines. These bearings require pressure lubrication to establish an oil film between the bearing surfaces before startup of the turbine. Typically, ball-type thrust bearings are not used in turbines rated above 1500 horsepower. The HPCI turbine is rated at 2675 HP in some plants and at 4000 to 4600 HP in most other plants.

Specific design features to permit HPCI system operation without DC power include the following:

- Replacement of the single large HPCI turbine-driven pump with three or four parallel, smaller turbine-driven pumps (comparable in size to the RCIC pump) that utilize ball-type thrust bearings. This will permit the auxiliary lube oil system to be deleted and the trip/throttle and governing valves to be designed to be normally open. In addition, the gear-driven booster pump required by the large single HPCI pmp could also be deleted.

- All other design features listed in Section 5.25.3.3 for the RCIC system would also be required by the HPCI system.

A HPCI system with these modifications is illustrated in Figure 5.25.6. In that figure, T1, T2 and T3 are three small turbines which respectively drive pumps P1, P2 and P3. With these design features, a spurious loss of Class 1E DC Division 3 during power operations will cause an unintended startup of the HPCI system. With AC power available, containment isolation valves in the steam supply and pump discharge lines can be closed to terminate this event. The use of normally open trip/throttle and governing valves eliminates one of the primary NRC concerns raised about the HPCI system in NUREG-0626 (Ref. 6).



NOTES:

(1) ALL NORMALLY CLOSED PNEUMATIC VALVES FAIL OPEN ON LOSS OF AIR PRESSURE OR LOSS OF DC POWER TO THE SOLENOID PILOT VALVES. MANUAL HANDWHEELS AND REACH RODS ARE PROVIDED, IF NECESSARY, FOR OPERATION OF THESE VALVES FROM OUTSIDE THE PUMP ROOM.

Figure 5.25.6. HPCI System Modifications For Operation Without AC or DC Power.

If inadvertent HPCI makeup to the RCS following loss of DC Division 3 is unacceptable, one or more valves in the steam supply line for each of the small HPCI turbine-driven pumps should be designed to fail closed. Timely operator response will be necessary, however, the remaining HPCI design changes should minimize the number and complexity of operator actions necessary to place the HPCI system in operation.

5.25.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #25

5.25.5.1 Impediments to AFW System Design Changes

The operation of the AFW system without AC and DC power for an extended period of time appears to be technically feasible. Other systems (e.g., high pressure injection) would also need to be restored to operation to maintain the plant in a safe condition. Following station blackout and loss of feedwater, core uncovery to the core midplane has been calculated to occur in approximately 2 hours (Ref. 5).

The spurious actuation of the turbine-driven AFW train following loss of its DC division may cause some regulatory concern if this is determined to be a high probability event. The system in Figure 5.25.2 includes isolation provisions to manually terminate such an event.

The potential impact of this damage control measure on the likelihood of an overcooling transient or other damage due to overfilling the steam generators should be assessed. In addition to the AFW system modifications, emergency operating procedures and operator training may be adequate to minimize these concerns.

5.25.5.2 Impediments to RCIC System Design Changes

The operation of the RCIC system without AC and DC power for an extended period of time appears to be technically feasible. The suppression pool cooling system would also need to be restored to operation to maintain the plant in a safe condition. Following station blackout and loss of suppression pool cooling it has been estimated that the suppression pool will heat up from $100^{O}F$

to $150^{o}F$ in approximately three hours (Ref. 5). Additional time is available before containment design temperature is reach (e.g., $185^{o}F$ for Mark 3 containments, higher for Mark 1 and Mark 2 containments).

The spurious actuation of the RCIC system following loss of Class 1E Division 1 may cause some regulatory concern if this is determined to be a high probability event. With level in the normal range, an inch change in level in a BWR corresponds to approximately a 150 to 175 gallon change in coolant inventory. At the RCIC injection rate of 400 to 800 gallon/minute (at $70^{o}F$), reactor vessel level will be increasing at 3.6 to 7.1 inches/minute (at $540^{o}F$ considering a water specific volume increase of 1.34) if feedwater flow is not reduced by the feedwater control system. During operation, reactor vessel water level is maintained between the low and high level alarm setpoints (e.g., approximately 15 and 50 inches, respectively, on the narrow range level instruments). The RCIC system will automatically shutdown and the reactor will scram on reactor vessel high water level (Level 8, which corresponds to approximately 55 inches on the narrow range level instruments). The system in Figure 5.25.3 includes isolation provisions to manually terminate such an event from the control room. Depending on the initial reactor vessel water level, several minutes may be available for the operator to take manual corrective actions and shutdown the RCIC system before a reactor scram occurs.

5.25.5.3 Impediments to HPCI System Design Changes

The operation of the HPCI system without AC and DC power is only possible following wholesale redesign and retrofit of major components (e.g., the turbine drives and pumps). Space limitations within the plant may preclude replacing the single large HPCI turbine-driven pump with several smaller units. If the proposed modifications can be made, other plant systems would also be required (e.g., the suppression pool cooling system) to maintain the plant in a safe condition for an extended period of time.

The spurious actuation of the HPCI system may be a more significant concern than an RCIC system spurious start. At the HPCI injection rate of 2980 to 4250 gallons/minute, reactor vessel level will be increasing at 26.6 to 38 inches/minute without corrective action by the feedwater control system. The

HPCI system will automatically shutdown and the reactor will scram on reactor vessel high level (e.g., Level 8). Rapid operator response would be required to terminate this event manually from the control room before a reactor scram occurs.

5.25.6 Conclusions and Recommendations Regarding Damage Control Measure #25

The AFW system redesign to operate without AC or DC power is feasible, but will amount to a significant redesign effort in most cases. Further investigation into the potential safety benefits and impacts of this redesigned system should be made. A simpler, alternative approach would be to modify the DC power distribution system to facilitate reenergizing equipment in the turbine-driven AFW train from another DC source (see damage control measures #20, #21, and #22).

The RCIC system redesign to operate without AC or DC power is also feasible. It will require a greater amount of component redesign and retrofit than the AFW system to account for unique support system required by the RCIC (e.g., gland seal barometric condenser and associated condensate and vacuum pumps). Further investigation of the potential safety benefits and impacts of this redesigned system should also be made. Damage control measures #20, #21, and #22 could restore DC power to the RCIC system, thereby permitting normal system operation. These damage control measures should be considered as potential alternatives to RCIC system redesign.

The magnitude of the HPCI system redesign to operate without AC or DC power strongly suggests that these design changes are impractical. The RCIC system would be available as a backup to the HPCI system for providing core cooling when the reactor vessel is isolated from the main condenser and normal feedwater flow is lost.

5.25.7 Section 5.25 References

1. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Westinghouse - Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

2. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

3. NUREG-0565, "Generic Evaluation of Small Break Loss of Coolant Accident Behavior in Babcock and Wilcox Designed 177-FA Operating Plant," U. S. Nuclear Regulatory Commission, January 1980.

4. NUREG-056[illegible], "Staff Report on Generic Assessment of Feedwater Transients in Pressurized Water Reactors Designed by the Babcock and Wilcox Company," U. S. Nuclear Regulatory Commission, May 1979.

5. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

6. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

5.26 DAMAGE CONTROL MEASURE #26 - BWR AND PWR

The purpose of damage control measure #26 is to provide a standby Nonclass 1E combustion turbine generator that could supply power to the station startup bus for distribution to designated equipment and system when offsite power is unavailable.

5.26.1 Sabotage Scenario

Loss of offsite power occurs and the main turbine trips on loss of load coincidentally with one of the following two scenarios: (1) safety-related systems required for maintaining the plant in a safe condition have been sabotaged. Nonsafety-related systems capable of maintaining the plant in a safe condition have not been sabotaged, but are unavailable because of the loss of Nonclass 1E AC power, or (2) all emergency diesel generators have been sabotaged, preventing the operation of the majority of safety-related systems. Nonsafety-related systems capable of maintaining the plant in a safe condition have not been sabotaged, but are unavailable because of the loss of Nonclass 1E AC power.

5.26.2 Onsite AC Electric Power System and Startup Bus Description

A simplified diagram of an onsite electric power system is illustrated in Figure 5.26.1 (from Ref. 1). This system is divided into two major parts: a Nonclass 1E part, which supplies nonsafety-related equipment and a Class 1E part, which supplies safety-related equipment.

During power operation, the main turbine generator, via the unit auxiliary transformer, is the normal source of power to the Nonclass 1E distribution system. The preferred feeder from the offsite grid is the normal source of power to the Class 1E distribution system. At least two feeders from the offsite grid are provided as sources of preferred power for the Class 1E system. When the main turbine is not operating, power to the Nonclass 1E distribution system is supplied from the preferred feeder via the startup bus (see Figure 5.26.1).

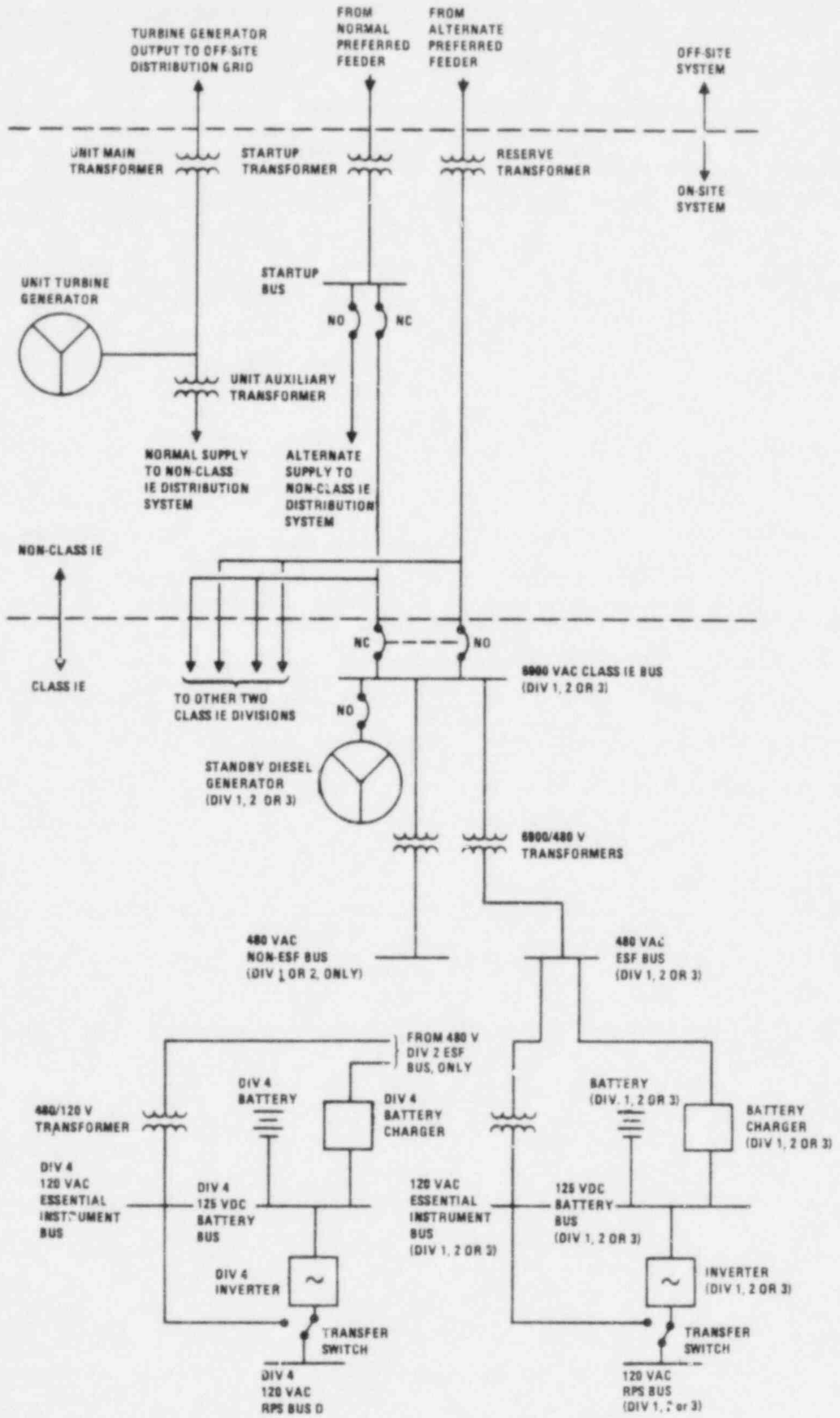


Figure 5.26.1. Simplified Onsite Electrical Distribution System -- Only One Class 1E Division Shown (from SAI01379-627LJ).

5.26.3 Plant Conditions During Sabotage Scenarios

Loss of offsite power is assumed to cause a trip of the main turbine generator. This effectively eliminates the sources of Nonclass 1E power to plant systems. In the first sabotage scenario described in Section 5.26.1, the plant is tending toward an unsafe condition because safety-related systems required for mitigating the accident have been sabotaged and nonsafety-related systems capable of mitigating the accident are unavailable. If electric power could be restored to some selected nonsafety systems, these systems could be substituted for the sabotaged safety systems and the plant could be maintained in a safe condition. Other damage control measures describe the specific system substitutions or realignments that have been considered.

In the second sabotage scenario described in Section 5.26.1, the plant is in a station blackout condition. The only power available is from the station batteries. The only fluid systems likely to be operating under these conditons are the turbine-driven portion of the auxiliary feedwater system (PWRs), the reactor core isolation cooling system (BWR/3 to BWR/6), the high pressure coolant injection system (BWR/3 and BWR/4), the isolation condenser system (BWR/1, BWR/2 and some BWR/3), and the diesel engine-driven portion of the fire water system (PWRs and BWRs). The NRC has recommended that at least one train of the AFW system, and the RCIC and HPCI systems be capable of operating independently of AC power sources for at least two hours (Refs. 2, 3 and 4). The isolation condenser system typically has a coolant inventory sufficient for one hour of core cooling without makeup (Ref. 5). Alternate water sources that do not require AC power to transfer water to the isolation condenser are available (e.g., fire water system or an elevated makeup tank). If electric power could be restored to safety-related, or to nonsafety-related systems, the plant could be maintained in a safe condition without being constrained by battery capacity.

5.26.4 Electric Power System Modifications to Incorporate a Standby Combustion Turbine Generator

Combustion turbine generators are available in a variety of ratings. The basic module described in this section is a commercially-available, self-contained, oil-burning unit rated at 35 to 40 MWe. A unit in this size range could provide the AC power necessary for operation of the secondary plant systems required by many of the other damage control measures. In addition, it could support operation of safety-related systems if the diesel generators were unavailable. Larger combustion turbine generator units in the 70 MWe range, and smaller units comparable in size to diesel generator units (e.g., 5 to 7.5 MWe), are also available commercially.

A modular enclosure housing the combustion turbine generator unit measures approximately 32 feet wide by 114 feet long and includes the following:

- Combustion turbine and generator unit
- Starting system
- Lube oil system
- Fuel oil system
- Air system
- Electrical system
- Control system
- Combustion air intake and exhaust system
- Enclosure ventilation system
- Fire protection system

Also required is a long-term fuel oil supply. Main elements of a combustion turbine generator unit are illustrated in Figure 5.26.2 (from Ref. 5).

5.26.4.1 Combustion Turbine Generator Systems and Auxiliaries

A. Combustion Turbine and Generator Unit

The main elements of the combustion turbine are the 18 stage axial-flow compressor, the combustion system and the 3 stage reaction turbine. Rated turbine speed is 4894 rpm. A reduction gear connects the combustion turbine to a 3600 rpm, 2-pole AC generator with a brushless exciter. This entire assembly is supported on an I-beam bedplate.

B. Starting system

Initial rotation of the combustion turbine is accomplished by a DC turning motor after lubrication system pressure has been established. The unit is then cranked by a 700 HP diesel engine to approximately 20 percent speed where ignition occurs. The diesel then helps the turbine

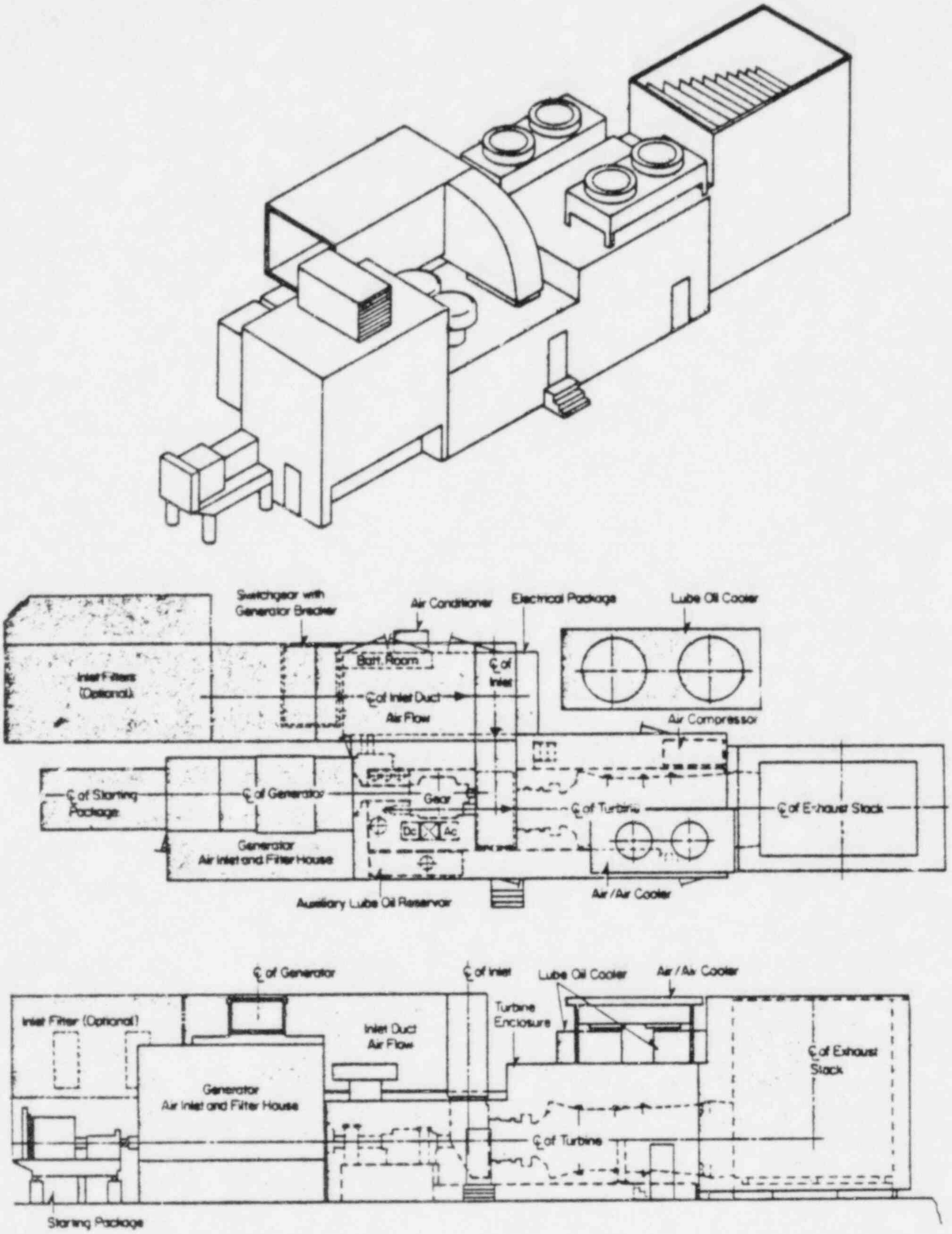


Figure 5.26.2. Combustion Turbine Generator Plant Arrangement (from Westinghouse Descriptive Bulletin 1550).

accelerate above self-sustaining speed, and is secured when the turbine reaches approximately 60 percent speed.

During unit shutdown, the turning gear is again reengaged when the turbine coasts down to 3 rpm. The turbine is rotated for a cooling period to assure no warping of the rotor.

C. Lube Oil System

The lube oil system includes a main AC-powered lube oil pump and a DC auxiliary lube oil pump. The AC lube oil pump is required for turbine startup. The control system is interlocked to prevent rotating the turbine without proper lube oil pressure. The DC lube oil pump supplies lube oil for safe unit shutdown following loss of the AC pump, and for lubrication during rotation of the turbine on the turning gear.

D. Fuel Oil System

The fuel oil system utilizes a shaft-driven main pump to supply fuel oil from a day tank to the turbine fuel nozzles. High pressure air is also introduced in the fuel nozzles to atomize the fuel oil. As the turbine is brought up to speed by its diesel starting engine, the shaft-driven fuel oil pump pressurizes the fuel oil system. When firing speed is reached (less than 20 percent speed), the turbine overspeed trip and isolation valves open, admitting fuel to the nozzles. The throttle valve is modulated by the control system to maintain a pre-set acceleration of the turbine during the startup sequence. When the plant is in operation, air for atomizing the fuel is no longer required. The fuel oil atomizes automatically because of the design of the fuel nozzle and the velocity of the fuel.

A fuel oil day tank is provided in the combustion turbine module. Long-term operation of the unit requires a capability to transfer fuel oil from storage tanks.

E. Air System

An air compressor and accumulator system provides required air pressure for indicating instruments, pneumatic valves, regulators and controllers and for fuel oil atomizing air during startup. A control system interlock prevents starting the combustion turbine with low air system accumulator pressure. Near synchronous speed, the combustion turbines axial flow compressor develops sufficient capacity to meet the service air needs of auxiliary systems. During operation of the combustion turbine, the motor-driven air compressor is not required.

F. Electrical System

The electrical loads associated with a combustion turbine generator are summarized in Table 5.26.1. A local 60-cell battery is provided to supply the 125 VDC loads. The 480 VAC and 120 VAC loads are normally supplied by a feeder from some other source of power (e.g., a station 480 VAC bus or a higher voltage bus via an auxiliary transformer). For a black startup capability, a small diesel generator is commonly supplied with the combustion turbine generator unit. Maximum auxiliary

Table 5.26.1. Electrical Loads Associated With a 35 to 40 MWe Combustion Turbine Generator Unit.

480 VAC Loads	Rating
* Main lube oil pump	50 HP
Battery charger	50 Amp
* Exciter field power supply	10 KVA
Instrument air compressor	10 HP
Air/Lube oil cooler, 2 fans	20 HP (each)
Lube oil heater	18 KW
Air/Air cooler, 2 fans	15 HP (each)
Turbine enclosure fans (4)	30 HP (total)
Electrical package HVAC unit	10 KW
Generator and exciter space heaters	10 KW (total)
Vapor extractor	3 HP
Fuel forwarding pump	7.5 HP
120 VAC Loads	
* Starting motor control package Fire protection system Enclosure lighting Motor heaters (air/air and lube oil cooler fan motors) Space heaters (15 KV switchgear)	20 KVA
125 VDC Loads	
Auxiliary lube oil pump	5 HP
* Turning gear	5 HP
* 15 KV switchgear control * Voltage regulator * Relay panel * Control system	15 AMP
* Pressure switch and relay cabinet	20 AMP

* = Required for startup. Other loads can be energized once the combustion turbine generator is in operation, if necessary.

power requirements are approximately 300 KVA. The combustion turbine generator output circuit breaker is located within the unit enclosure.

G. Control System

The control system provides for automatic, sequenced startup and loading of the combustion turbine generator. It also includes an automatic equipment monitoring subsystem to prevent exceeding safe operating limits and necessary controls and displays to permit the operator to remotely or locally change output or operating modes as required.

H. Combustion Air Intake and Exhaust System

The intake system directs air through trash screens, a silencing baffle, and then to the turbine inlet. Additional filters and evaporative coolers to reduce inlet air humidity can also be provided. The exhaust system directs exhaust air through silencing baffles to a vertical exhaust stack.

I. Enclosure Ventilation System

Ventilation fans are provided to circulate air within the unit enclosure to maintain suitable environmental conditions for equipment operation.

J. Fire Protection System

An integral fire protection system is provided for the combustion turbine generator unit. A Halon 1301 system is provided for all areas of the unit, except for the turbine exhaust bearing area, where an automatically actuated dry chemical system is used.

5.26.4.2 Combustion Turbine Generator Operation

The startup of a large combustion turbine is divided into the following five phases.

A. Ready-to-Start Phase: If 480 VAC power is not available from normal onsite sources (e.g., following a station blackout), a small diesel generator unit must be available to provide power to auxiliary systems until the combustion turbine generator is in operation. With the small diesel generator operating, the main (AC) lube oil pump is placed in operation to lubricate the bearings. After establishing lube oil flow, the turning gear is placed in operation to break away the shaft and start it rotating slowly. The unit is ready to start.

B. Cranking Phase: This is a pre-ignition phase that covers startup to approximately 20 percent speed. The combustion turbine is accelerated by a 700 HP diesel engine. The turning gear disengages. As firing speed is reached, fuel is admitted to the fuel nozzles and is ignited in the turbine combustion chambers.

C. Acceleration Phase: Fuel flow is increased at a pre-set rate to control the acceleration of the turbine. After ignition, the starting diesel engine continues to assist acceleration to approximately 60 percent speed, after which time it is shut down. Near synchronous speed, the generator field is flashed. The generator is in a no-load condition at rated voltage and frequency.

D. Synchronization Phase: If the combustion turbine generator is to be connected to an energized bus, it will be necessary to synchronize the generator and bus phases before closing the generator output circuit breaker. When connected to an energized bus, the unit picks up a small increment of load (minimum load), and enters the loading phase. When the unit is connected to a dead bus, it will reenergize and pick up any loads still connected to the bus. All large loads should be disconnected before reenergizing the dead bus. Time from startup to minimum load is approximately 8 to 10 minutes.

E. Loading Phase: When running in parallel with another AC source after being connected to an energized bus, turbine controls allow loads to be gradually picked up by the generator. Total startup time to full load is 16 to 22 minutes. After picking up loads still connected to a dead bus, additional loads can be reenergized in sequence by remote-manually or locally closing the appropriate circuit breakers. If a small 480 VAC diesel generator has been operating for the startup of the combustion turbine unit, the diesel generator would be synchronized and paralleled with the combustion turbine generator. When all auxiliary power loads have been shifted to the combustion turbine generator the small diesel generator output circuit breaker may be opened and the diesel generator may be secured.

5.26.4.3 Connection of a Combustion Turbine Generator to an Existing Nuclear Power Plant Electrical System

A standby gas turbine generator unit could be connected to a startup bus at a nuclear power plant as illustrated in Figure 5.26.3. The unit is normally in standby with its output breaker open. If offsite power is lost, the supply breakers from the startup bus to the Class 1E distribution system will be opened, and the diesel generators will supply safety-related loads. When the combustion turbine generator is placed in operation, the circuit breaker from the preferred power source should be opened (if not already open following loss of offsite power). The generator output breaker can then be closed, and power can be supplied to the Nonclass 1E system via the existing distribution system from the startup bus.

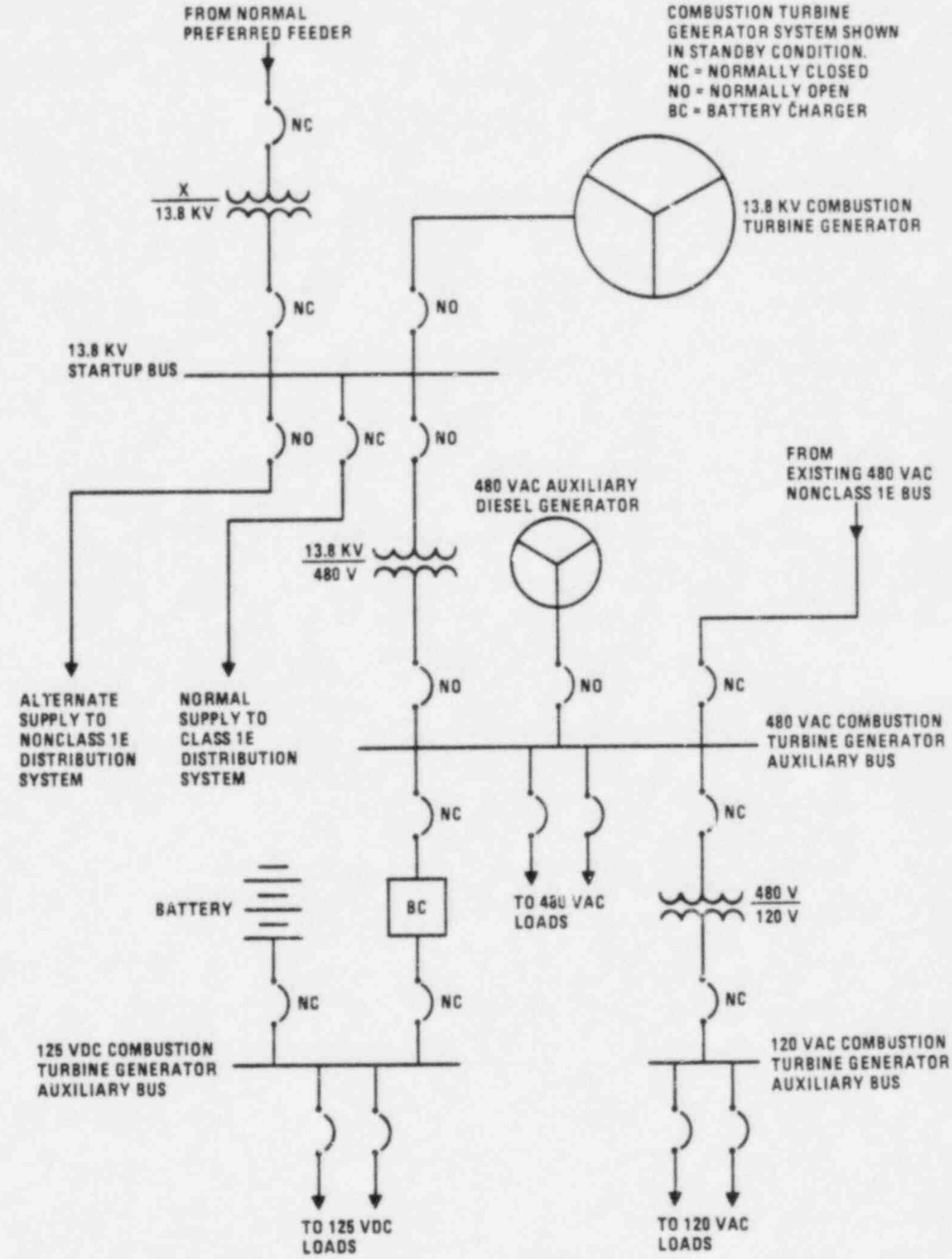


Figure 5.26.3. Electrical System Modifications to Connect a Combustion Turbine Generator to a Startup Bus.

If diesel generators were unavailable, the Class 1E system could also be supplied from the startup bus using the existing distribution system. This arrangement allows maximum flexibility in supplying power from the combustion turbine generator to any plant system that is available and of use in maintaining the plant in a safe condition

5.26.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #26

None. At least one nuclear power plant site (Salem 1 and 2) currently has a Nonclass 1E combustion turbine generator in the size range described in this section (e.g., 40 MWe). The Millstone 1 nuclear plant also has a combustion turbine generator unit, however, it is a smaller Class 1E unit (12 MWe).

5.26.6 Conclusions and Recommendations Regarding Damage Control Measure #26

Adoption of this damage control measure complicates the sabotage actions necessary to prevent effective accident mitigation. Availability of a standby combustion turbine generator would permit the use of some nonsafety-related systems for accident mitigation in approximately 30 minutes following a loss of offsite power. Although credit for the operation of these systems is not usually assumed in conservative safety analyses, their availability would provide an improved capability and flexibilty for accident mitigation. This damage control measure provides a diverse onsite power source that could restore power to safety-related and nonsafety-related systems following a sabotage scenario involving loss of offsite power and all diesel generators. It would be similarly effective for maintaining the plant in a safe condition following a nonsabotaged-related station blackout.

The standby combustion turbine generator, if properly sized, could give a nuclear power plant a viable black startup capability. The loads required for startup are certain to be greater than to maintain the plant in a safe shutdown condition. The modular nature of available combustion turbine generator units and their ability to operate in parallel provides a straight-forward method for extrapolating the basic approach proposed by this damage control measure to meet the power requirements for plant start. The black start capability would enable nuclear power plants to be restored to operation more rapidly following major grid outages.

Cost of a 35 MWe combustion turbine generator is approximately \$5.25 million (about \$150/KW) at the factory, and \$6.3 million (about \$180/KW) installed as a turnkey project.

5.26.7 Section 5.26 References

1. Lobner, P., et al., "The Boiling Water Reactor - A Review of a Typical General Electric BWR/6 Plant," SAI01379-627LJ, Science Applications, Inc., March 23, 1979.

2. NUREG-0611, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Westinghouse Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

3. NUREG-0626, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in GE-Designed Operating Plants and Near-Term Operating License Applications," U. S. Nuclear Regulatory Commission, January 1980.

4. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant-Accidents in Combustion Engineering Designed Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5. "W-251 ECONO-PAC Combustion Turbine Power Plants," Descriptive Bulletin 1550, Westinghouse Electric Corporation, Combustion Turbine Systems Division, December 1978.

5.27 DAMAGE CONTROL MEASURE #27 - BWR AND PWR

The purpose of damage control measure #27 is to provide the capability to place an emergency diesel generator in operation, supplying its normal Class 1E load group, when DC power is not available to the diesel generator control system or to diesel generator auxiliary systems.

5.27.1 Sabotage Scenario

Loss of offsite power is assumed to occur coincidentally with the successful sabotage of the DC power supply for one or more emergency diesel generators. The affected diesel generators do not start. Any unaffected diesel generators operate and supply AC power to their respective Class 1E buses.

5.27.2 Description of Standby Diesel Generator Systems

Class 1E electric power systems at nuclear power plants are normally supplied from an offsite power source. An independent, alternate preferred offsite power source is automatically aligned to supply the Class 1E electric system if the normal preferred supply is lost. When both the normal and alternate preferred power sources are unavailable, the onsite emergency diesel generators provide power to essential loads.

Diesel generators for standby power application fall into two broad categories, medium-speed four-cycle and high-speed two-cycle machines. A diesel generator unit consists of three modules (diesel engine, generator and an auxiliary module) mounted on a common bedplate. A standby diesel generator has the following auxiliary systems:

- Diesel Generator Cooling Water System
- Diesel Generator Lubrication System
- Diesel Generator Starting System
- Diesel Generator Fuel Transfer and Storage System

- Combustion Air Intake and Exhaust System
- Diesel Room Ventilation System
- Diesel Generator Control System

Each diesel generator is provided with its own set of auxiliaries. Interconnections between diesel generator auxiliaries is minimized in order to maintain the independence of the standby power units. Schematic diagrams of typical auxiliary systems are found in Figures 5.27.1 and 5.27.2 (both from Ref. 1). The diesel engine and the aspects of auxiliary systems associated with emergency startup and local control are discussed below.

5.27.2.1 The Diesel Engine

Diesel engines in standby power service are rated at 2300-12500 BHP, with corresponding generator continuous load ratings from 1700-9000 KW. A medium-speed diesel engine operates at 450 or 514 rpm. A high-speed two-cycle diesel operates at 900 rpm.

5.27.2.2 Diesel Generator Cooling Water System

A closed cooling water system is provided for dissipating heat from the engine air intercooler, lube oil cooler, turbocharger and the engine water jacket. This closed cooling water system may transfer heat to the ultimate heat sink through a service water system, as illustrated in Figure 5.27.2, or through water-to-air radiators. A 7665 HP/5500 KW diesel generator will reject about 3200 KW to the cooling water system (Ref. 2).

The system in Figure 5.27.2 includes two redundant water pumps, one driven by a 125 VDC electric motor and the other is gear-driven by the diesel engine. A thermostatically-controlled three-way valve at the pump discharge controls the proportion of pump discharge flow that is bypassed around the cooling water heat exchanger. The cooling water system contains 150 to 250 gallons of water.

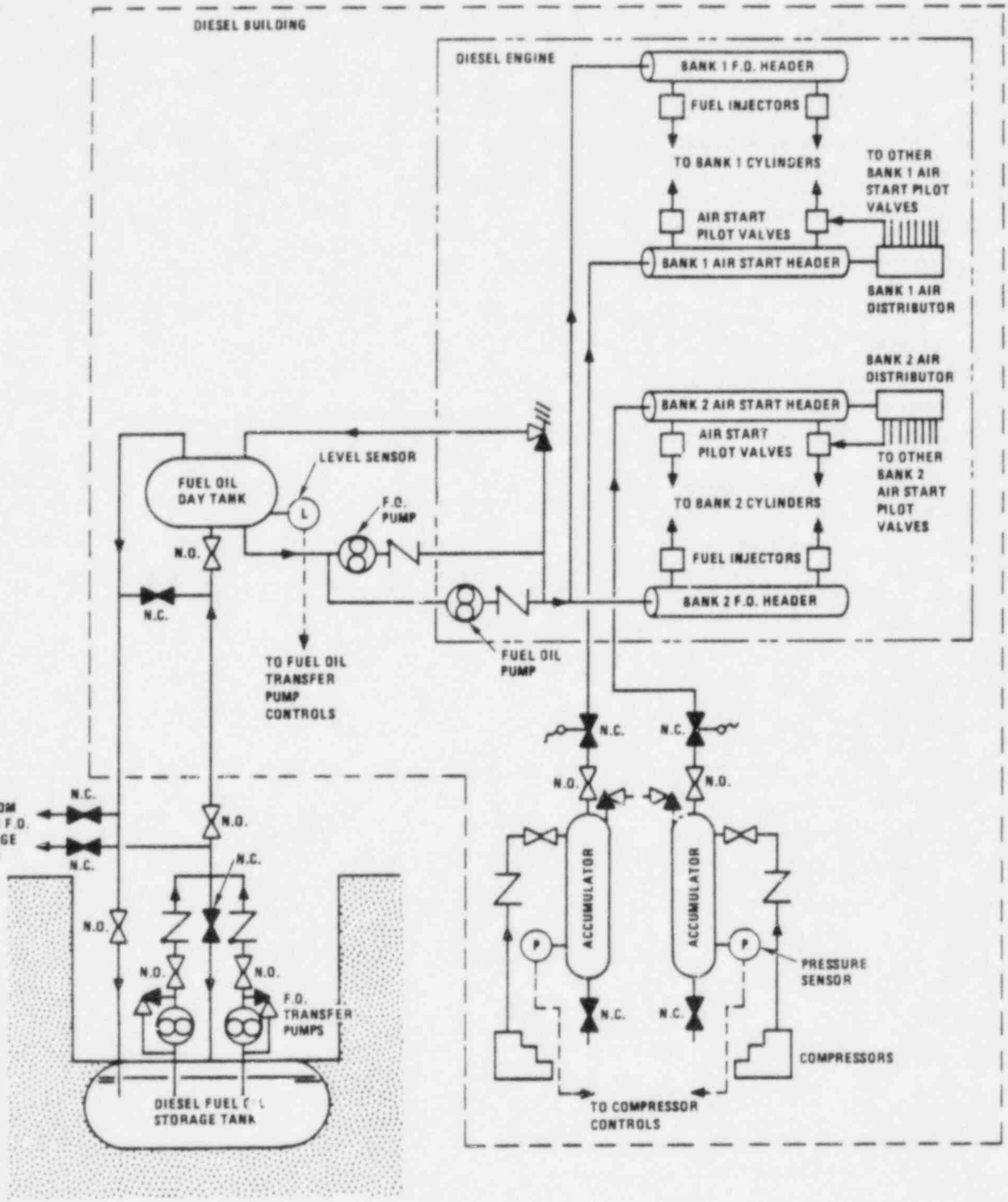


Figure 5.27.1. Typical Diesel Generator Fuel Oil and Air Starting Systems (from SAI01379-585LJ).

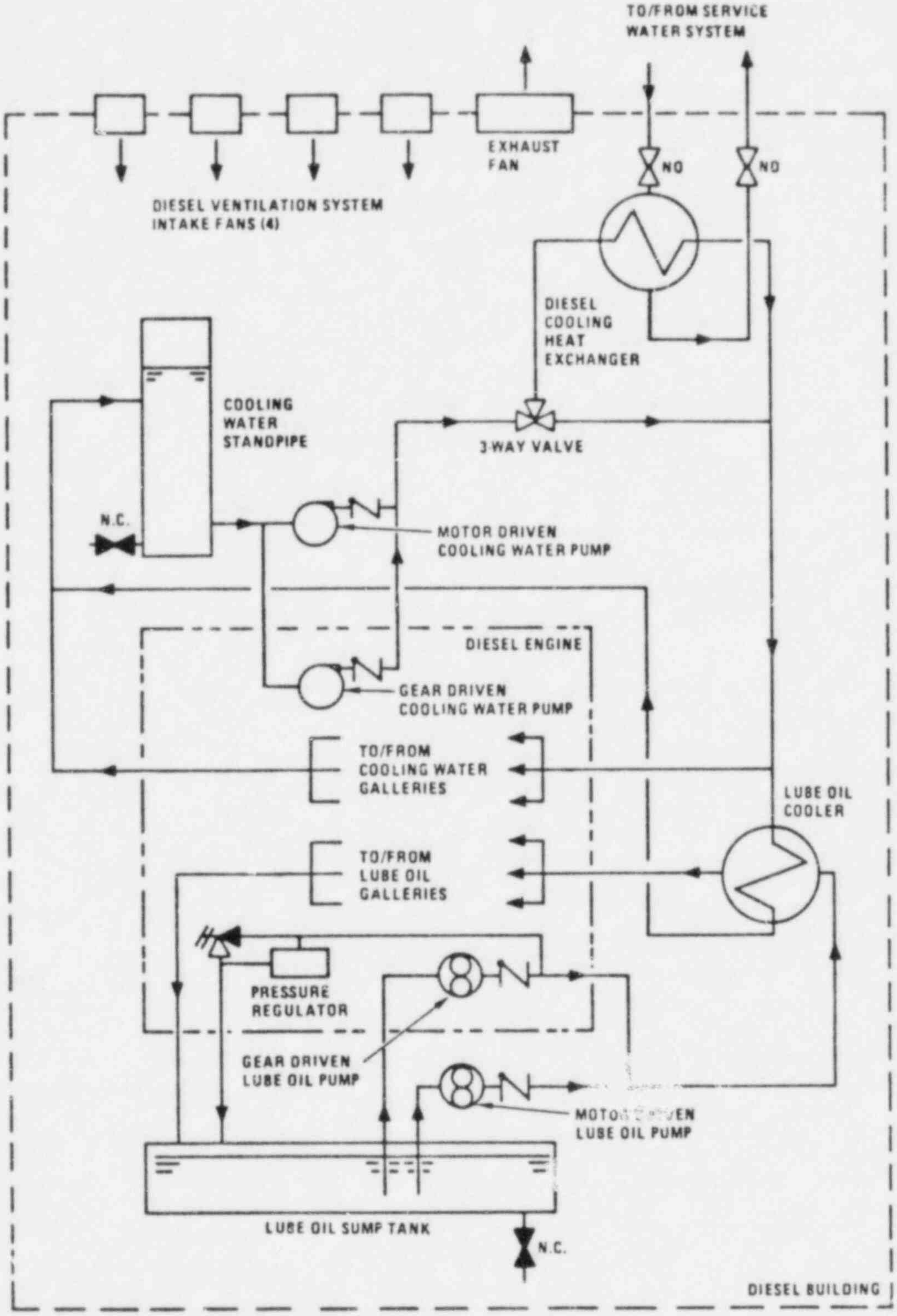


Figure 5.27.2. Typical Diesel Generator Lube Oil, Cooling Water and Ventilation Systems (from SAI01379-585LJ).

During periods when the diesel engine is not operating, "keep warm" heaters maintain cooling water system temperature in the range from 125 to 155^{O}F. During operation, maximum design cooling water temperatures are about 190^{O}F at the engine exit, and 175^{O}F at the engine inlet. The standpipe provides a surge volume for the diesel cooling water system. Maximum cooling water system pressure is about 50 psig.

Local indications associated with the diesel cooling water system include the cooling water temperature and pressure, DC electric motor-driven water pump and keep-warm pump status and keep-warm heater status. There may not be safety-related analog readouts in the control room for diesel cooling water system parameters. Alarms are provided locally and in the control room for high cooling water temperature, low cooling water pressure and low standpipe level.

5.27.2.3 Diesel Lubrication System

The diesel lubrication system provides for lubrication and cooling of diesel engine internal components (e.g., rocker assemblies, cam shafts, gear case, pistons, etc.) and the turbocharger. A typical diesel lube oil system is illustrated in Figure 5.27.2.

There are two positive displacement main lube oil pumps. One is driven by a 125 VDC electric motor and the other is gear-driven by the diesel engine. Constant oil pressure (e.g., 85 to 100 psig) is maintained by a pressure regulating valve at the lube oil pump discharge which bypasses excess flow back to the lube oil sump. A lube oil cooler limits maximum oil temperature to about 215^{O}F with about a 30^{O}F temperature rise between engine oil inlet and outlet. The lube oil sump, or reservoir, is generally mounted on the diesel skid, along side the engine.

Local indication associated with the diesel lube oil system may include engine and turbocharger lube oil pressure, lube oil temperature, DC electric motor-driven main lube oil pump and keep-warm (pre-lube) pump status and keep-warm heater status. Lube oil sump level can be monitored with a dip stick. Lube oil temperature and electric motor-driven main lube oil pump status are likely to be monitored in the control room. Alarms are generally provided locally and in the control room for low lube oil pressure (engine and turbocharger), high oil temperature, high differential pressure across the lube oil strainer and low lube oil level.

5.27.2.4 Diesel Air Starting System

Diesel air starting systems provide a supply of compressed air for starting emergency diesel engines without external power. The air starting system is designed to accelerate the diesel engine so that it can achieve rated voltage and frequency within ten seconds. The air starting system for a four-cycle diesel engine starts the engine by direct application of high pressure air to the cylinder heads (see Figure 5.27.1). The system includes two separate and independent air subsystems, each consisting of a compressor, an accumulator, a solenoid control valve and an air start header serving one bank of cylinders on the diesel engine. Each independent subsystem has sufficient air storage volume to be capable of several (typically five) diesel engine starts without recharging the accumulator. The compressors typically have sufficient capacity to recharge an accumulator from minimum to maximum starting air pressure in 30 minutes.

The air start system may be actuated automatically by an Engineered Safety Feature Actuation System (ESFAS), via the diesel generator control system. The diesel generator can also be started manually from the control room or from the local control panel in the diesel building. A start signal energizes and opens the normally closed DC-powered starting air solenoid valves and admits air to the starting air headers and the pilot air distributors on the diesel engine. The air starting valve in each cylinder head (see Figure 5.27.3) is pilot actuated. The pilot air distributor is cam-actuated to apply pilot air to open the air start valve to each cylinder during the expansion stroke, admitting high pressure air from the starting air header to drive the piston to the bottom of its stroke. At that time, pilot air is removed from the starting air valve causing it to close. The cylinder is then vented through its exhaust valve.

Air is applied to all cylinders in sequence, bringing the engine up to speed rapidly, at which point normal diesel combustion begins and the diesel generator control sytem deenergizes the starting air solenoid valve, terminating the starting air sequence.

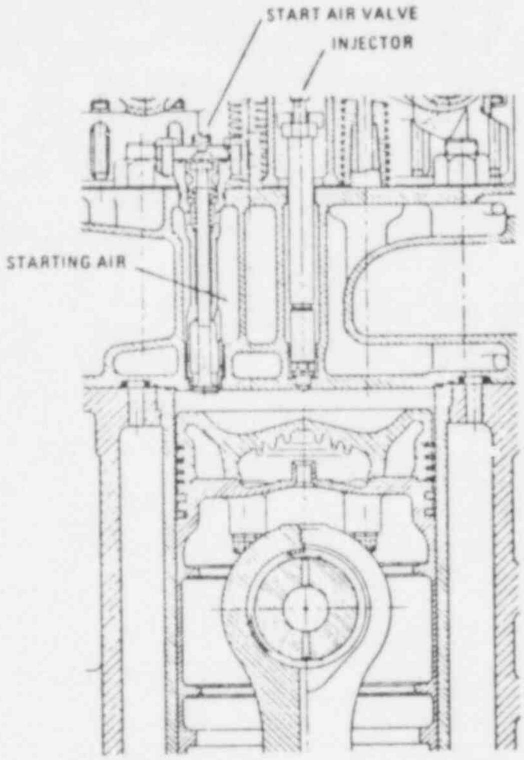


Figure 5.27.3. Typical Configuration of Direct Air Start Valve in Diesel Cylinder Head.

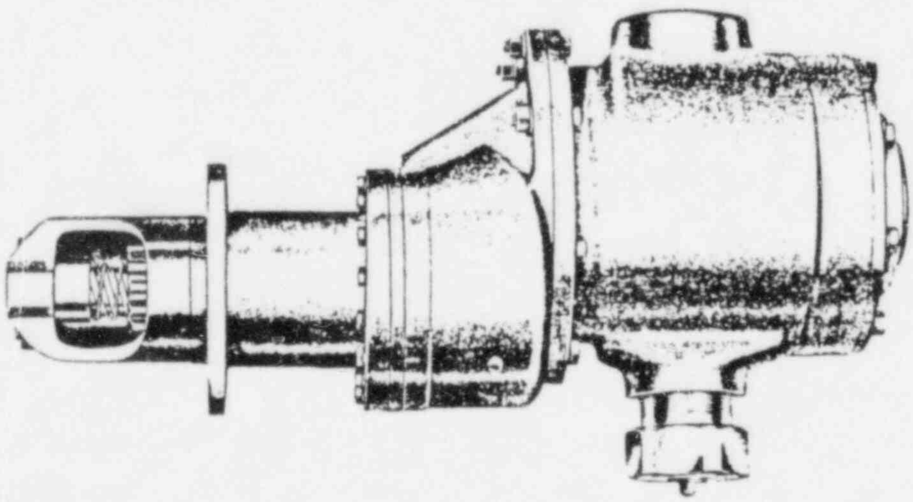


Figure 5.27.4. Typical Air Start Motor for Two-Cycle Diesels.

The compressors in the starting air system are automatically started by low accumulator pressure and are automatically stopped by high accumulator pressure. Starting air system pressure is 200 to 425 psig.

The starting air system for a high-speed 2-cycle diesel engine is very similar to the system illustrated in Figure 5.27.1 with the exception of the starting mechanism on the diesel engine. The two-cycle diesel engines use multiple, redundant air starting motors, similar to the type illustrated in Figure 5.27.4, to engage gears on the flywheel to crank the diesel engine up to speed. On a tandem high-speed diesel, there are typically four air starting motors per diesel.

Local and control room indicators associated with the diesel air start system may include starting air pressure and compressor status. An alarm is provided locally and in the control room for low starting air pressure.

5.27.2.5 Diesel Fuel Oil Transfer and Storage System

Each diesel engine is provided with a short-term fuel oil reservoir (the day tank) within the diesel building. The day tank is able to support several hours of diesel operation without being replenished. A long-term reservoir (storage tanks) is located underground, outside the diesel building. This storage facility provides makeup for the day tank and has at least a seven-day capacity. A diesel fuel oil system is illustrated in Figure 5.27.1.

During diesel engine operation, day tank level drops as fuel is consumed. A 7665 HP/5500 KW diesel will consume about 384 gallons of fuel per hour operating at 100 percent rated load and about 205 gallons per hour at 50 percent rated load. On a low-level signal from the day tank, the first fuel oil transfer pump starts. If this pump fails to maintain the level in the day tank, the second fuel oil transfer pump starts on a low-low level signal. The transfer pumps are powered from a 480 VAC Class 1E motor control center. The day tank is vented to the atmosphere and is equipped with a flame arrester.

From the day tank, fuel oil is supplied to the diesel via duplex fuel strainers and parallel fuel pumps; one is driven by a 125 VDC electric motor and the other is gear-driven by the diesel engine. The fuel pumps discharge through one-inch lines to two fuel supply headers, one serving each bank of the V-engine. Fuel pump discharge pressure is 35 to 50 psig. The fuel pumps are protected against overpressure by a discharge relief valve that recirculates flow back to the pump suction. Each engine cylinder is served by its own cam-driven fuel injection pump and injection valve. The fuel injection pump draws oil from the supply header and raises oil pressure to over 1000 psi for timed injection into the cylinders.

Fuel flow from the injection pump is controlled by the governor which simultaneously actuates two fuel racks, one per bank of cylinders. The racks run parallel to the axis of the diesel and rotate to drive one rack assembly for each fuel injection pump. The setting of the fuel rack establishes the amount of fuel injected into each cylinder. In essence, the fuel rack is the throttle for a diesel engine.

The diesel engine is typically provided with an electric speed regulating governor and an engine-driven actuator to drive the fuel racks. The actuator receives signals from the externally-mounted governor which processes signals from the electrical system to control the speed and load of the engine. The electric governor requires DC power to operate. The engine-driven actuator can be designed to move to the "zero-fuel" or "maximum fuel" position on loss of signal from the electric governor. A wiring diagram for an electric speed regulating governor and actuator is illustrated in Figure 5.27.5. The motor-operated potentiometer ("M.O.Pot." in Figure 5.27.5) provides a means for remotely changing the engine speed setpoint of the electric governor. The power supply for the motor-operated potentiometer may come either from the generator after it is excited, or if speed setting must be altered when the unit is unexcited, this power can come from another supply (e.g., station batteries).

The actuator unit includes a backup mechanical fly-ball governor and hydraulic pilot valve assembly which regulates the engine speed in the event of a loss of signal from the electric governor. The mechanical backup governor is normally adjusted to a higher speed setting than the electric governor so the

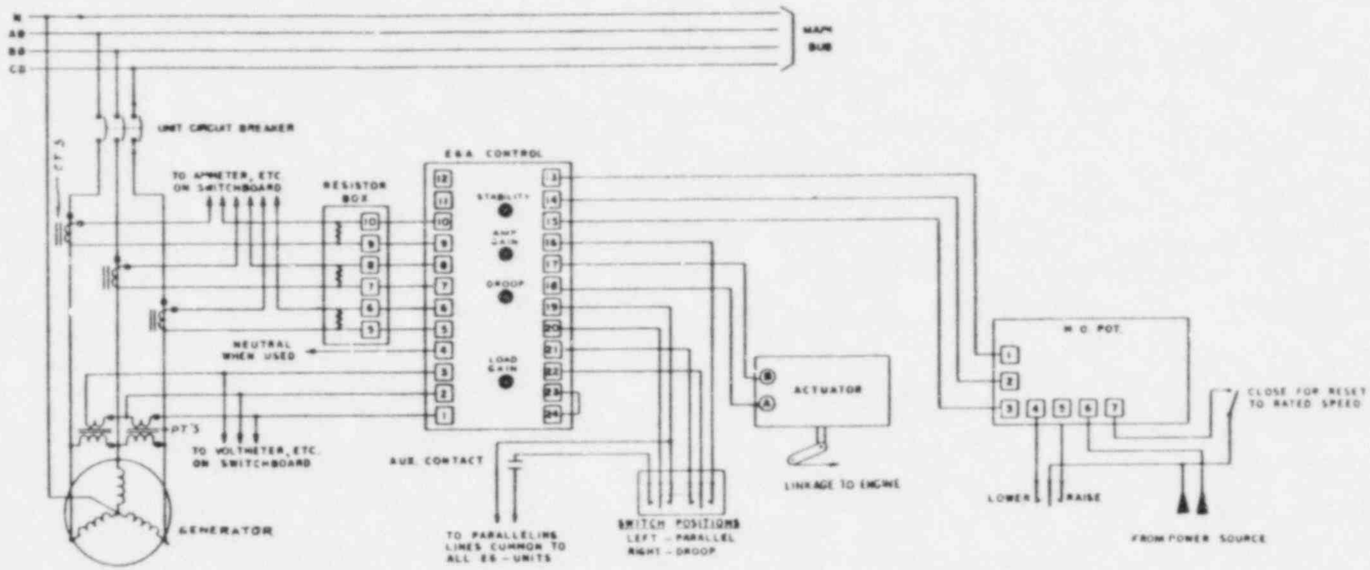


Figure 5.27.5. Wiring Diagram for a Diesel Generator Electric Speed Regulating Governor

latter can control at the desired speed without interference. The mechanical backup governor normally has controls for setting speed, speed droop, and load limit. It may also have a speed-changing motor that allows the speed setting to be changed remotely.

An independent centrifugal-type overspeed trip mechanism is mounted on the drive end of the engine. In the event of an overspeed of the engine, this device uses main lubricating oil pessure to operate a hydraulic servo cylinder to move the fuel racks to the zero delivery position.

Local indications asociated with the diesel fuel oil system may include day tank level, fuel oil transfer pump and DC fuel oil pump status, fuel oil temperature and fuel oil pressure. Day tank level and transfer pump status may be indicated in the control room. Transfer pumps can be operated from the control room. Alarms are provided by level switches for high and low day tank level.

5.27.2.6 Combustion Air Intake and Exhaust System

This is a passive system that supplies air to the diesel engine air intake through intake air filters and silencers and directs the diesel exhaust to atmosphere through an exhaust silencer. A single intake filter and air silencer, generally located in a missile protected enclosure on the diesel building roof, supply air to each turbocharger (one per cylinder bank) through intake ductwork. The turbochargers boost intake air pressure and discharge to an intake manifold, one serving each cylinder bank. The diesel engine exhausts into four exhaust manifolds that join to form two exhaust ducts that discharge through an exhaust silencer, generally mounted in a missile protected enclosure on the diesel building roof.

A 7665 HP/5500 KW diesel engine will dissipate about 5380 KW in the exhaust gases (Ref. 2).

Local indications associated with the combustion air intake and exhaust system include turbocharger inlet temperature and inlet manifold pressure. No readouts are provided in control room and no alarms are generally associated with this system.

5.27.2.7 Diesel Room Ventilation System

This system is required to maintain the diesel room temperature within suitable limits to ensure the operability of the diesel control system and other auxiliary systems. There are many possible configurations of this system. The arrangement illustrated in Figure 5.27.2 has four 25 percent capacity intake fans and one 100 percent capacity exhaust fan. The system is designed to maintain the maximum ambient temperature in the diesel room less than 120°F during continuous diesel operation.

A 7665 HP/5500 KW diesel generator will reject about 1780 KW to the diesel room from all sources during operation (Ref. 2).

Local indications associated with the diesel room ventilation system include inlet and exhaust fan status and room temperature. There may be no indications in the control room.

5.27.2.8 Diesel Generator Control System

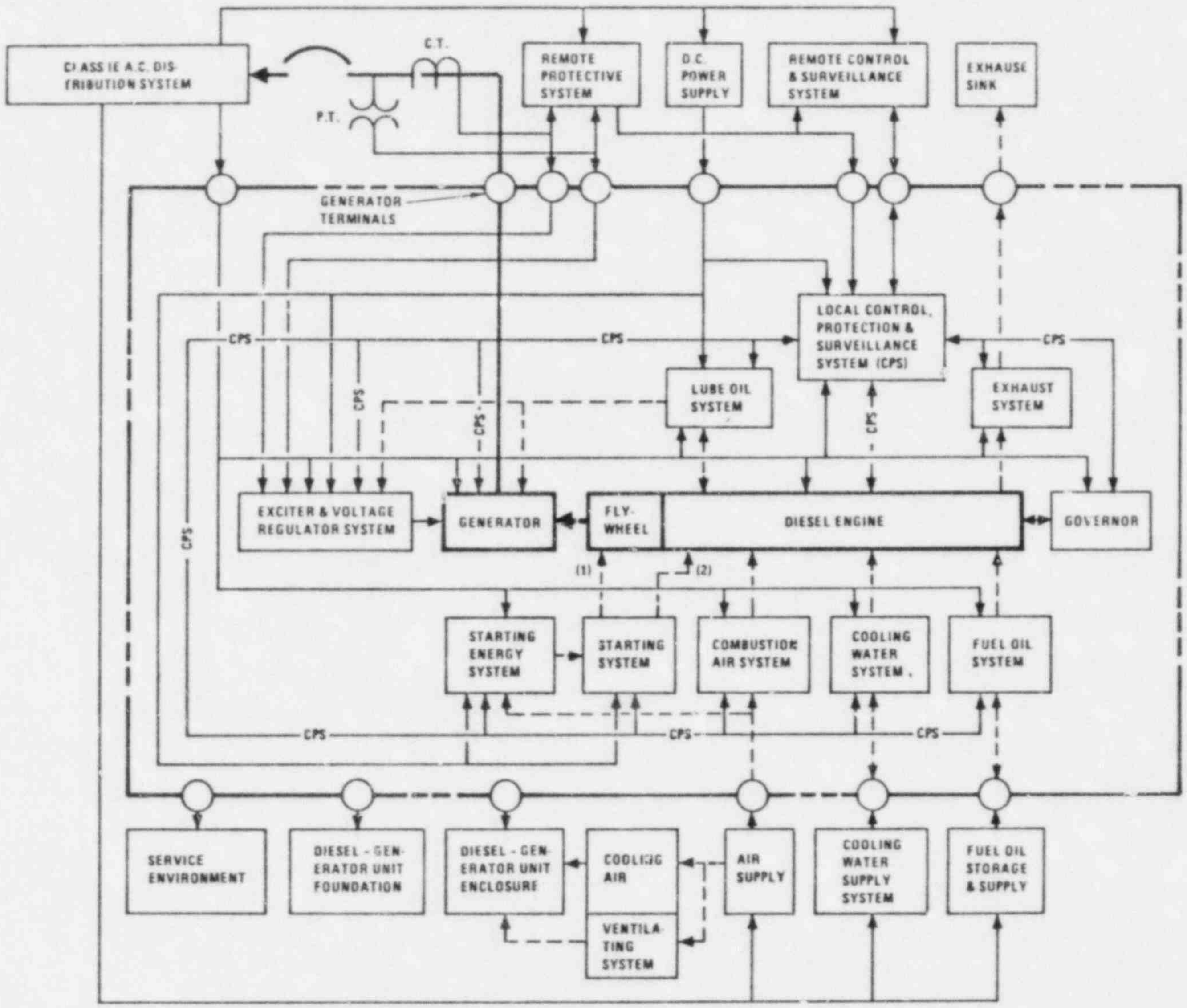
The block diagram in Figure 5.27.6 (from Ref. 1) illustrates the major elements of a diesel generator control system, which include the following:

- Engine control and protection system
- Generator control and protection system
- Automatic control and sequencing system

The operation of these systems is described below.

A. Engine Control and Protection System

Referring to Figure 5.27.6, this system consists of the Local Control Protection, and Surveillance System (or CPS), and the Remote Control and Surveillance System (located in the main control room). The Engine Control and Protection System will start, stop, protect, operate, and monitor the integrity of the diesel engine in its various modes of operation and testing. The system accepts a manual or automatic start signal from a remote or local location and, if the diesel protection



NOTES (1) THIS PATH IF AIR START MOTORS ARE USED FOR DIESEL STARTING.
(2) THIS PATH IF DIESEL IS STARTED BY DIRECT AIR APPLICATION TO ENGINE CYLINDERS.

Figure 5.27.6. Diesel Generator System Block Diagram (from SAI01379-585LJ).

system is permissive, the unit will start, come up to speed and voltage, and send a "ready to load" signal to the Automatic Control and Sequencing System. The protection system is electro-pneumatic. All faults, both alarm and shutdown, are displayed on a local solid state annunciator. In an "emergency start" situation, even though most of the diesel protection system is bypassed, the actions of the individual protective devices are monitored and displayed on the annunciator. The only diesel system protection typically in effect and operable during an "emergency start" will be engine overspeed, generator differential overcurrent, and Class 1E switchgear bus fault.

Figure 5.27.7 (from Ref. 1) shows the schematic diagram of a typical diesel engine control system (only that portion which is required during emergency operation). The control system contains all the circuitry necessary to start the engine, deactivate most of the diesel protection and shutdown system, flash the generator field to begin generating voltage, and produce a "ready to load" signal when the engine is up to speed. Solenoids 1A and 2A are the air start solenoid valves. They are located on or near the engine and admit starting air to the engine when energized. PS40A is deenergized (indicating diesel is in the operational mode) and PS3A is closed (indicating sufficient air in the accumulators for about five starts). PS3A will open on low accumulator pressure, and deenergize the air start solenoids. This pressure switch is present so that, if the unit does not start automatically, there will be sufficient air left for several manual starts.

Receipt of an automatic or manual "emergency start" contact closure simultaneously energizes the start air solenoids (solenoids 1A and 2A) and deactivates the shutdown system (via solenoid 6A), and starts the field flash timer (TD1A). At the same time, signals are sent through solenoid 2A which close PS10A to the governor and voltage regulator, shifting them to automatic operation. Field flashing occurs when the field flash time delay times out after about one second, or when tachometer relay contacts SS1A close, and solenoid 9A is energized, closing PS30A which completes the circuit to flash the generator field. Upon reaching synchronous speed, SS2A of the tachometer relay closes, energizing solenoid 7A which opens PS33A, cutting off the start air. Once voltage is close to normal, VR1 closes, generating the "ready to load" output signals.

For a normal manual start, the control system must be in the operational mode. Then, either remotely or locally, relay 4A is energized, time delay relay 2A is started, and the starting air solenoids 1A and 2A are energized for about five seconds (until TD2A times out). Again, the field flash solenoid 9A is energized by TD1A timing out, or by the tachometer relay contacts SS1A closing. Contacts SS2A close, BR1 closes, and the "ready to load" signal is generated. The shutdown sytem is not deactivated in this case.

Whichever way the system receives a start signal, PS32E will be closed and the run relays R1 and R1A will be latched (if PS9D shows the unit is not tripped). If the unit does not come up to speed within five seconds after R1 is latched, TD4 will time out and reset R1, indicating a failure of the engine to start. R1 and R1A contacts are used

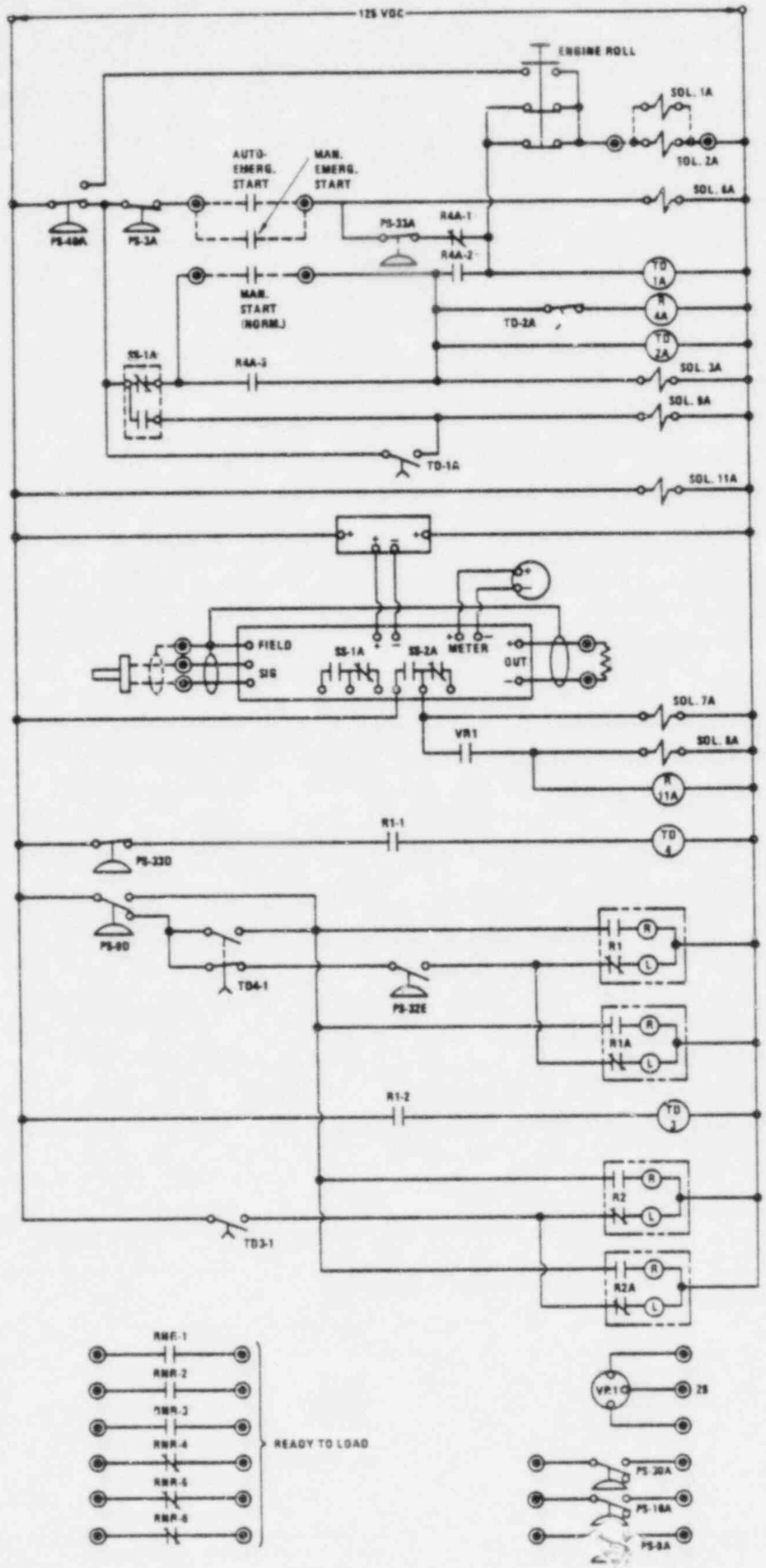


Figure 5.27.7. Typical Diesel Engine Control System (Essential Portion Only, from SAI01379-585LJ).

throughout the control system where a signal is needed to indicate that the engine is running or not running. The R2 relays are responsive to the latching of R1 and R1A, but there is a one-minute time delay (from TD3) before R2 latches. Contacts of R2 and R2A are then used to disarm various alarm functions which are normally in a tripped stated when the unit is stopped, starting, or stopping.

The local diesel engine control and protection system control board typically contains an annunciator (alarm and indication of low fuel level, low fuel pressure, etc.), analog pressure gauges (lube oil pressure, starting air pressure, etc.), temperature limit lights, system status lights (power on, ready to load, unit tripped, etc.), engine hour-meter and RPM tachometer, and all operator controls required for local operation of the unit. This control board is located in close proximity to the diesel generator unit, normally inside the diesel generator room.

The main control room also contains some diesel engine status displays and operator controls. These typically include summary-type annunicators (unit tripped, unit running, failure to start, etc.) and manual diesel start controls.

B. Generator Control and Protection System

Referring to Figure 5.27.6, this system consists of the Remote Protective System (the generator protective metering and relaying system) and the Exciter and Voltage Regulator System. The Generator Control and Protection System will monitor, protect, control and coordinate the operation of the diesel engine-driven AC generator. The one-line diagram in Figure 5.27.8 (from Ref. 1) shows a typical generator remote protective system and an exciter and voltage regulator system.

The generator remote protective system monitors generator performance, protects the generator from electrical faults, controls the operation of the generator output circuit breaker, and coordinates the operation of this circuit breaker with the operation of the normal and alternate preferred power source circuit breakers. In addition to the displays and control on the medium-voltage switchgear, generator displays and control typically included in the main control room are voltage, current, power, reactive power, circuit breaker manual controls, and circuit breaker open-closed-tripped status indication.

The exciter and voltage regulator system is typically of the vector-summing type, deriving its power from the vector sum of the generator output voltage and line current. Figure 5.27.9 (from Ref. 1) shows the schematic diagram of a typical generator field exciter and voltage regulator system. Transformer T1 supplies the no-load requirements of the generator. The current produced by the secondary of T1 is shifted in phase by the linear reactors LR1, LR2, and LR3 so that it lags the voltage from T1. When a load is applied to the generator, current flows through the primaries of the current transformers CT1, CT2, and CT3. This produces a current in the secondaries of the current transformers which is in phase with the load current from the generator. It is thus the vector sum of the currents

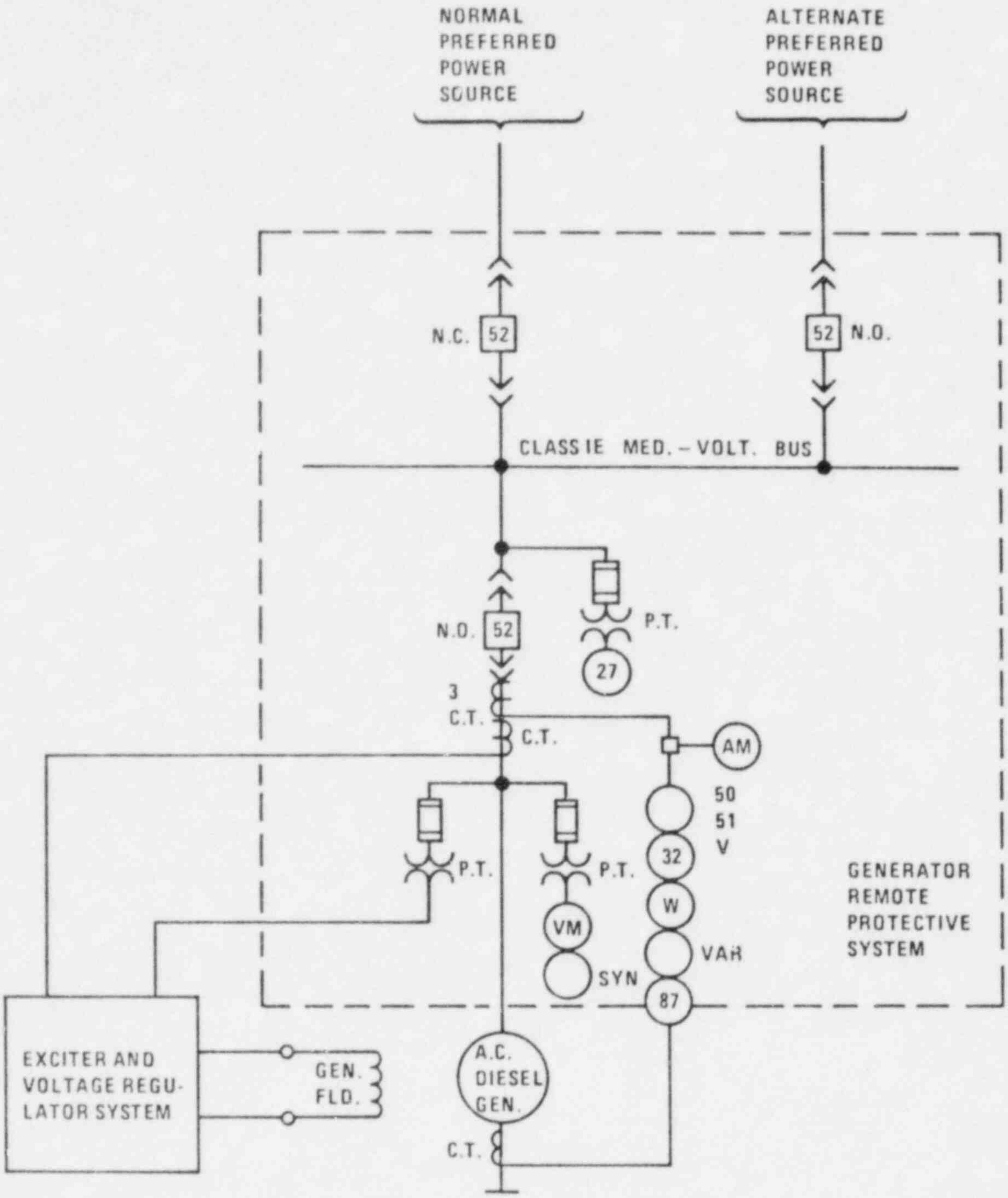


Figure 5.27.8. Typical Generator Control and Protection System (from SAI01379-585LJ).

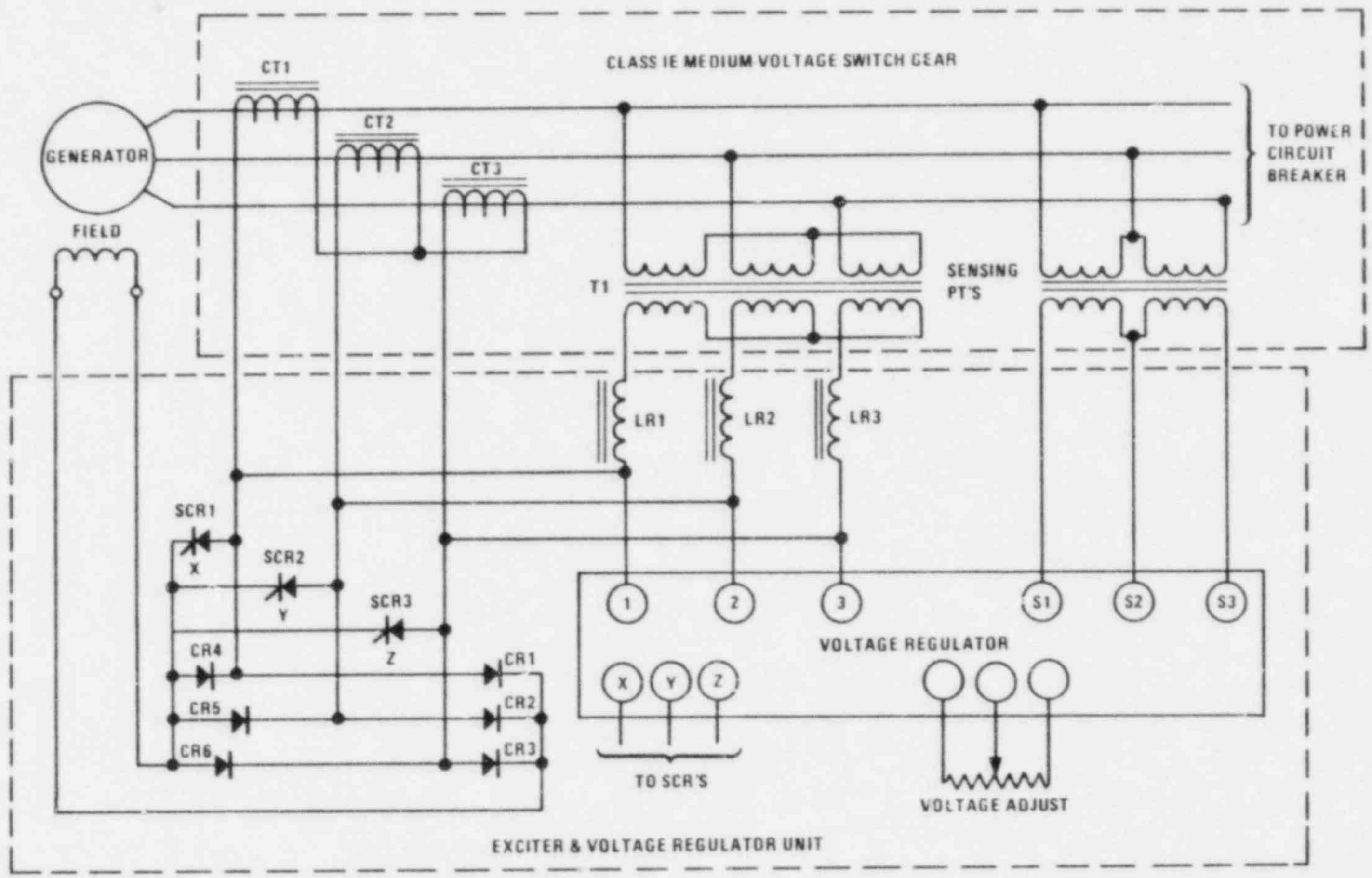


Figure 5.27.9. Typical Generator Field Exciter and Voltage Regulator System Schematic (from SAI01379-585LJ).

from T1 (as shifted by the linear reactors) and these currents from the secondaries of the current transformers that produces the required field current for the generator at that load (via the rectifier bridge CR1 through CR6). The design characteristics of T1, CT1, CT2, and CT3 make it necessary to shunt some excess power away from the rectifier bridge and the generator field in order to maintain the proper generator output voltage. This is done through the use of shunting thyristors SCR1, SCR2, and SCR3. These solid state devices, under the control of the voltage regulator, bypass precise amounts of power away from the generator field.

The voltage regulator derives its power from the input to the field exciter circuit (the rectifier bridge and shunting thyristors). The regulator samples the generator output voltage via the sensing potential transformers, rectifies the sample voltage, and compares it to a reference voltage. The error signal developed by this comparison is fed to an error amplifier, which controls the firing angle of the exciter circuit shunting thyristors. A manually-controlled potentiometer on the generator control board in the diesel room can be used to set the voltage regulator.

C. Automatic Control and Sequencing System

The Automatic Control and Sequencing System will monitor, control, and coordinate the automatic operation of the diesel engine control and protection system, the diesel generator control and protection system, the normal and alternate preferred power supplies to the Class 1E medium-voltage switchgear, and all loads connected to the Class 1E medium-voltage switchgear. Figure 5.27.10 is a block diagram of a system which utilizes a central sequencer.

Initially, the diesel generator is shutdown, the diesel generator power circuit breaker is open, the normal preferred power source circuit breaker is closed, the alternate preferred power source circuit breaker is open, and the Class 1E medium-voltage switchgear bus voltage is normal (see Figure 5.27.8). If the Class 1E bus voltage from the preferred power source should be lost for any reason, the following automatic sequence is initiated:

1. After a short time delay (normally about one second) to allow for short or momentary drops in offsite power system voltage, the normal preferred power source circuit breaker is tripped open.

2. At the same time, an "emergency start" command is sent to the diesel engine control and protection system, and a "breaker close" command is sent to the alternate preferred power source circuit breaker.

3. If the Class 1E bus voltage immediately returns to normal by closing the alternate preferred power source circuit breaker (step 2 above), the diesel generator will be allowed to come up to rated speed and voltage, but no further automatic action will take place.

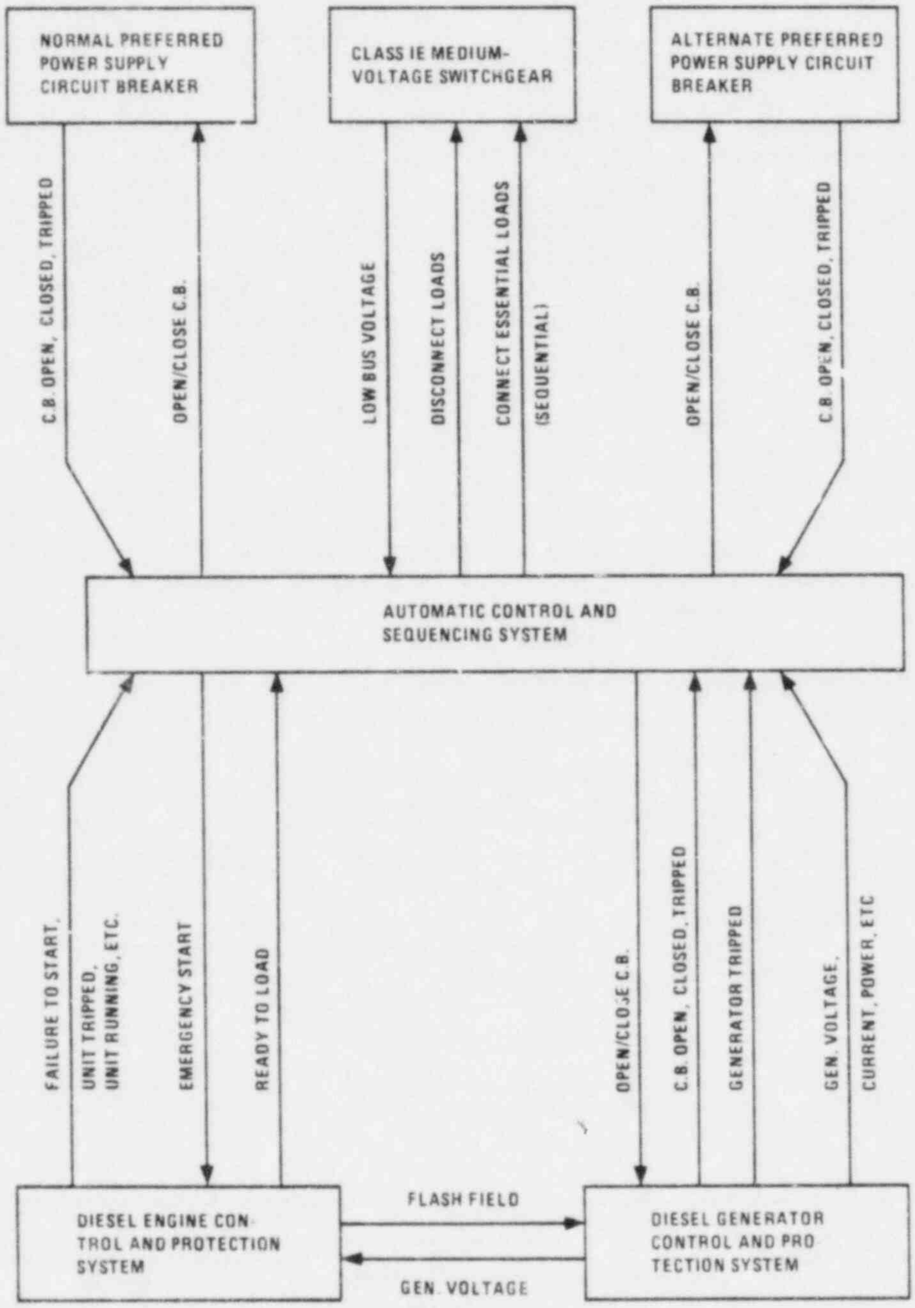


Figure 5.27.10. Automatic Control and Sequencing System Block Diagram (from SAI01379-858LJ).

4. If the Class 1E bus voltage does not immediately return to normal after Step 2, a "disconnect loads" command is sent to the Class 1E medium-voltage switchgear, resulting in the immediate shedding of all loads connected to the bus, and a "breaker open" command is sent to the alternate preferred power source circuit breaker.

5. Approximately ten seconds after receiveing the "emergency start" command (from step 2 above), the diesel generator will be at rated speed and voltage, and a "ready to load" signal will be sent back to the automatic control and sequencing system.

6. A "breaker close" command is now sent to the diesel generator control and protection system, and the diesel generator is connected to the unloaded Class 1E medium-voltage switchgear bus.

7. The Automatic Sequencer, which is part of the automatic control and sequencing system, now begins sending "connect load" commands to the Class 1E medium-voltage switchgear, resulting in the sequential restarting of all essential loads.

8. The fast-responding generator field exciter and electronic voltage regulator and governor ensure rapid diesel generator voltage and frequency recovery after each load is started, and within approximately 30 seconds after closing the generator circuit breaker, all essential loads have been sequenced automatically back onto the switchgear bus.

An automatic central sequencer may be an electromechanical or solid state device. An electromechanical sequencer is a cam-type stepswitch with a rotary solenoid advance mechanism which uses a standard reset timer to operate the solenoid and advance the stepswitch. The solid-state sequencer accomplishes the same timing, control, and programmed output functions using solid-state electronic circuitry with no moving parts. The electronic logic outputs of the sequencer typically operate solid-state relays or relay-drivers to provide output control signals to switchgear circuit breakers and motor starters.

5.27.3 Plant Conditions During Sabotage Scenario

Following loss of one Class 1E diesel generator, one train of some multi-train safety systems and some single-train systems will be inoperable. The nuclear power plant can be maintained in a safe shutdown condition with the remaining AC load groups(s) and operable safety systems.

Some plants only have two Class 1E AC load groups. Loss of the second AC load group in such a plant would create a station blackout condition. Analysis has indicated that, following a total station blackout and loss of feedwater, a PWR core would be uncovered to its midplane in approximately two hours (Ref. 3). Additional time would be available if the turbine-driven auxiliary feedwater (AFW) train operated successfully and enabled core heat to be removed via the steam generators. This train of the AFW system is generally designed to be operable on DC power alone. AC power will eventually be required for the operation of a charging pump for high pressure makeup to the reactor coolant system.

Following station blackout and loss of all makeup to a BWR, it has been estimated that the core will be uncovered to the midplane in approximately 1.4 hours (Ref. 3). Adequate core coolant inventory can be maintained by the reactor core isolation cooling (RCIC) system or the high pressure coolant injection (HPCI) system, both of which are designed to be operable on DC power alone. AC power will eventually be required for the operation of a residual heat removal system for direct core cooling, or for suppression pool cooling.

The specific sabotage actions that resulted in the loss of DC power to the diesel generator(s) have not been specified. If the sabotage actions were directed at the Class 1E station batteries, it may be possible to isolate the batteries from the remainder of their respective DC load groups by opening the battery circuit breakers or disconnect links. If this can be done, it should be possible to use damage control measure #20 or #21 to establish a DC bus tie to reeenergize the affected DC load groups. If the sabotage actions prevent clearing the faults on the affected DC load groups, it may be possible to reestablish DC power to diesel auxiliaries by switching them to an alternate DC power source. Damage control measure #22 describes the use of multiple selectable DC feeders for this purpose. If all these measures fail, it may be possible to place the affected diesel generators in operation by means of a local manual startup without AC or DC power.

5.27.4 Diesel Generator Design and Operational Features to Permit a Local Manual Startup Without DC Power

Design changes and operational considerations related to the local manual startup and operation of a diesel generator without DC power are described below for each auxiliary system. As will become evident, two or three persons will be required to coordinate a variety of actions necessary to manually place a diesel generator in operation.

5.27.4.1 Diesel Generator Cooling Water System

One of the cooling water pumps is gear-driven by the diesel engine. Once the diesel is operating, this pump will provide adequate cooling water flow. If the heat from the diesel cooling water system is in turn transferred to a service water or component cooling water system, it will be necessary to rapidly restore AC power to the 6900 or 4160 VAC Class 1E buses, place the necessary cooling water system in operation and complete the heat transfer path to the ultimate heat sink. Until this complete heat transfer path is established, the diesel cooling water will be rapidly heating and this closed system will pressurize to its relief valve setpoint.

For the diesel engine described in this section, the cooling water system transfers 3200 KW (1.82×10^5 BTU/min.) to the ultimate heat sink during operation. With the diesel engine in thermal equilibrium during operation, this heat load would equate to an initial 109°F/minute heatup rate for a 200 gallon cooling water system, if no heat is transferred to the service water system. This, of course, is not representative of the actual heatup rate that would be experienced by the diesel cooling water system if the service water system was lost during operation, or was unavailable immediately following diesel engine startup. The passive heat sink represented by the 25 to 50 ton diesel engine will significantly reduce the actual diesel cooling water system heatup rate. Although detailed calculations have not been made, it is estimated that the diesel cooling water system will be at its design temperature (about 190°F) within two minutes, and at the safety valve setpoint (297°F at 50 psig) within five minutes after startup, if the service water system is not available. Operation at elevated temperatures will reduce lubricating oil viscosity, and may result in inadequate engine lubrication. In addition, water will be lost from the cooling water system when the system pressurizes to the relief valve setpoint. If service water system operation is restored, an equivalent amount of makeup water must be added back into the diesel cooling water system from some available water source. Rapid establishment of a complete heat transfer path to the ultimate heat sink is essential to operation of a diesel generator.

Some diesel engines are cooled by means of water/air radiators in the diesel building, with forced-draft provided by 480 VAC fans. For the reasons described previously, it will be necessary to rapidly restore AC power to the 480 VAC Class 1E buses and place the necessary fans in operation. This will complete the heat transfer path to the ultimate heat sink.

A diesel cooling water system using water/air radiations could be modified to eliminate the time constraints on establishing the full system heat transfer capability. The basic modifications involve providing a minimum number of fans with mechanical drives that are driven from the diesel engine. Although the diesel engine drives a variety of mechanical components (e.g., gear-driven lube oil, cooling water and fuel oil pumps), all are closed-coupled to the diesel engine unit. A different type of mechanical drive would be required to provide motive power for diesel cooling water system radiator fans. A possible approach for mechanically driving the cooling water system fans is illustrated in Figure 5.27.11. This mechanical drive uses a V-belt and pulley assembly to transfer power from the diesel engine output shaft to one or more overhead rotating shafts. Individual fans are driven by additional V-belt and pulley assemblies connected to one of the main overhead rotating shafts. This system could provide adequate diesel engine cooling without dependence on any equipment outside the diesel building. This same mechanical drive could also provide motive power for the diesel room ventilation fans.

5.27.4.2 Diesel Lubrication System

One of the lube oil pumps is gear-driven by the diesel engine. Although not a recommended procedure for routine operation, the diesel engine can be started with lubrication supplied by the gear-driven pump alone. Once the diesel is operating, this pump will provide adequate lube oil flow.

5.27.4.3 Diesel Air Starting System

An operator in the diesel room could initiate startup of the diesel generator by manually opening the air start solenoid valves. Each of these valves should be povided with a manual handwheel or lever to permit local manual valve operation. Alternatively, a bypass line with a manual valve could be added

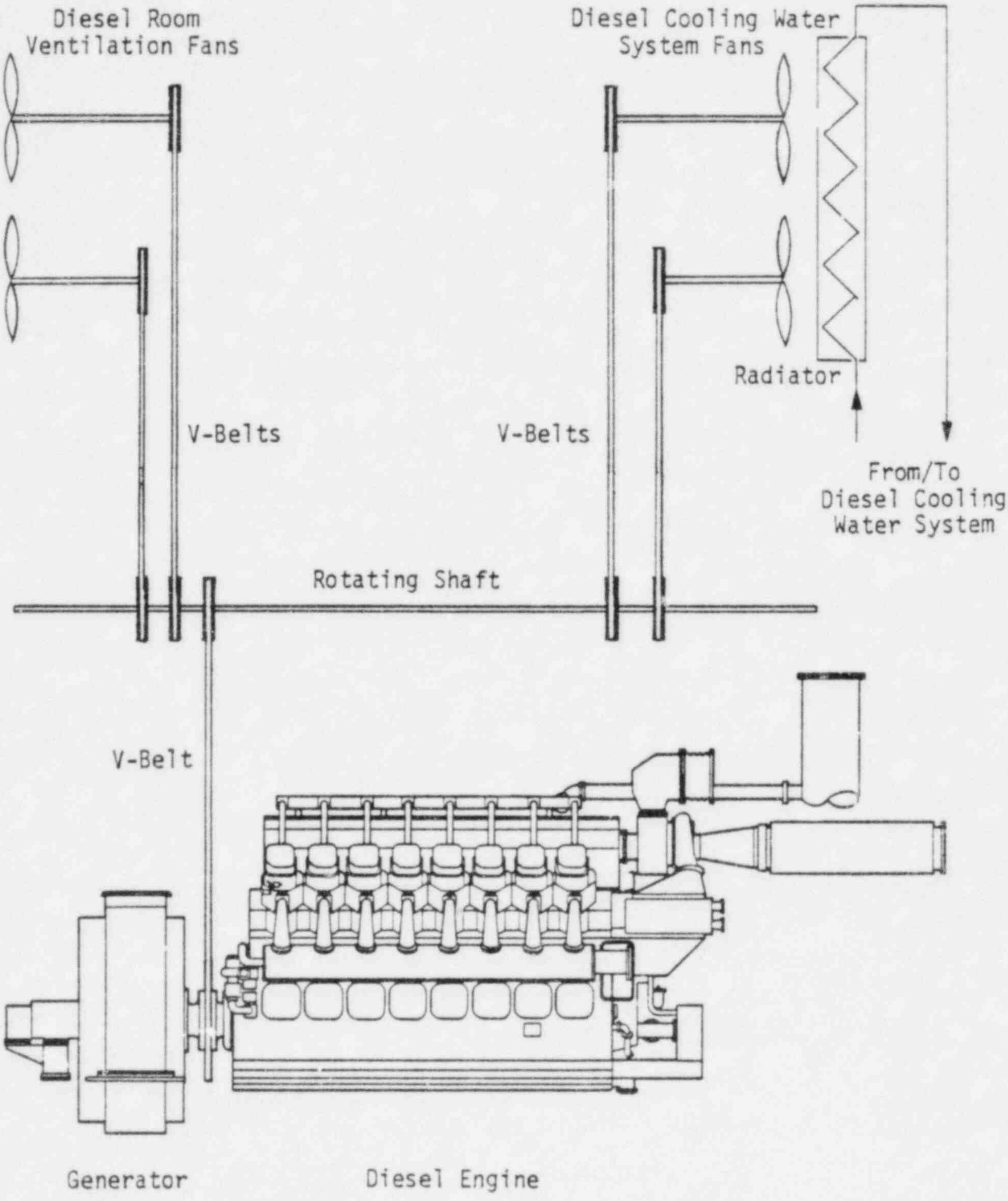


Figure 5.27.11. Mechanical Drive for Diesel Cooling Water and Room Ventilation Fans.

around the existing air start solenoid valves. Other aspects of this system remain unchanged.

5.27.4.4 Diesel Fuel Oil Transfer and Storage System

One of the main fuel oil pumps is gear-driven by the diesel engine. This pump can adequately supply the engine during startup and normal operation.

An electric governor will not be operational without DC power. If this governor and its actuator are designed to be "reverse acting," the failure mode on loss of power will be the equivalent of a "maximum fuel" signal. The fuel racks will move to a position to admit maximum fuel to the engine during acceleration. The backup ball-head mechanical governor will adequately control the diesel engine speed during starting and operation. Available speed controls on the backup governor will require readjusting downward to establish a no-load engine speed that equates to a generator output frequency of 60 Hz. Speed droop on the mechanical governor can be set at "0" for near-isochronous operation. The backup governor will maintain engine speed, and generator output frequency as loads are reenergized on the Class 1E system.

When DC power is restored, the electric and mechanical governors will be competing to control diesel engine speed. The speed control on the mechanical governor could then be manually reset to its normal, higher speed setting. Typically the backup governor is set at a speed more that 3 percent (1.8 Hz) above the electric governor. Speed droop on the mechanical governor would also be reset to approximately 5 percent.

5.27.4.5 Combustion Air Intake and Exhaust System

No changes to this system are required.

5.27.4.6 Diesel Room Ventilation System

Once the diesel engine is operating, it will be rejecting heat directly to the diesel room. It will be necessary to restore power to the 480 VAC Class 1E buses and place the necessary room ventilation fans in operation.

An alternative approach would be to provide a minimum number of fans with a mechanical drive that is driven from the diesel engine, as described previously. A possible approach for mechanically driving the room ventilation system fans is illustrated in Figure 5.27.11. This type of ventilation system would operate independently of equipment outside the diesel building.

5.27.4.7 Diesel Generator Control System

A. Engine Control and Protection System

The operator would be performing many of the functions of this system by manually opening the air start solenoid valves. The engine would accelerate to rated speed under the control of its backup ball-head governor. A centrifugal overspeed trip is also available for engine protection. Other system monitoring and protective functions are not being performed automatically. A local operator would be required to observe engine conditions from the local gauge panel and take manual protective actions (e.g., manual emergency trip) if required.

The effect of reenergizing this system once the diesel generator has been manually placed in operation has not been evaluated.

B. Generator Control and Protection System

One utility has performed an analysis that indicates that a diesel generator can be brought up to rated speed and voltage without the need for DC power from the Class 1E batteries (Ref. 4). This capability is based on there being sufficient residual magnetism in the generator to accomplish the field flashing function without DC power. During normal plant operation, the periodic testing intervals for diesel generators may be as long as 31 days (Ref. 5). If this testing interval does not result in adequate residual magnetism in the generator, a shorter testing interval could be adopted.

The voltage regulator circuitry is powered off the output of the generator, and does not require DC power, except for a reference voltage signal. Voltage can be controlled manually be means of a potentiometer control on the generator control panel.

C. Automatic Control and Sequencing System

The automatic sequencing functions must be performed manually. Specific operations that must be coordinated include (1) closing the diesel generator output circuit breaker, (2) ensuring that circuit breakers to the preferred power sources are open, and (3) sequentially reenergizing safety-related loads in the affected Class 1E electrical load group. During loading of the generator, an operator in the diesel room would be required to manually maintain rated voltage and frequency. More than one person would be required to accomplish these actions in a timely manner.

5.27.5 Technical and Regulatory Impediments to Implementing Damage Control Measure #27

If sufficient residual magnetism exists to "self flash" the generator field, it appears to be technically feasible to start and operate a diesel generator manually, without DC power. If there is not sufficient residual magnetism, it will be necessary to operate the diesel generator more frequently. The potential impact of this increased duty cycle should be evaluated on an individual plant basis to determine the acceptability of implementing this damage control measure. There are no other apparent technical or regulatory impediments to implementing this damage control measure under emergency conditions.

5.27.6 Conclusions and Recommendations Regarding Damage Control Measure #27

Auxiliary system design changes coupled with coordinated operating procedures could provide the capability to manually start and operate a diesel generator without DC power. This damage control measure eliminates or circumvents a few key vulnerabilities of the standby diesel generators. Because of the inherent redundancy of nuclear plant systems, use of this damage control measure is not essential when only a single AC load group is affected. The plant can be maintained in a safe condition with remaining AC load groups and safety systems.

5.27.7 Section 5.27 References

1. Lobner, P., et al., "Nuclear System Components - A Review of Typical Design and Operating Characteristics of Components Used in Nuclear Power Plant Systems," SAI01379-585LJ, Science Applications, Inc., March 21, 1979.

2. "238 Nuclear Steam Supply System - GESSAR," Docket STN-50550, General Electric Company.

3. Ericson, D. M. and Varnado, G. B., "Nuclear Power Plant Design Concepts for Sabotage Protection," NUREG/CR-1345, Sandia National Laboratories, January 1981.

4. NUREG-0635, "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Operating Plants," U. S. Nuclear Regulatory Commission, January 1980.

5. USNRC Regulatory Guide 1.108, "Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants."

DISTRIBUTION:

U. S. Nuclear Regulatory Commission
(385 Copies for AN, RS, 1S)

Division of Document Control
Distribution Services Branch
7920 Norfolk Avenue
Bethesda, MD 20014

U. S. Nuclear Regulatory Commission
K. Markulis (50)
Office of Nuclear Regulatory Research
MS: 1130SS
Washington, DC 20555

Science Applications, Inc. (10)
Attn: Peter Lobner
P.O. Box 2351
La Jolla, CA 92038

1700 W. C. Myer
1750 T. A. Sellers
1760 J. Jacobs
4400 A. W. Snyder
4410 D. J. McCloskey
4412 J. W. Hickman
4412 A. M. Kolaczkowski
4414 G. B. Varnado (5)
4414 D. M. Ericson, Jr. (10)
4416 L. D. Chapman
4440 G. R. Otey
4443 D. A. Dahlgren
3141 L. J. Ericson (5)
3151 W. L. Garner (3)
3154-3 C. H. Dalin (25)
for NRC Distribution to NTIS

☆U.S. GOVERNMENT PRINTING OFFICE: 1982-0-576-021/592

120555078877 1 ANRS1S
US NRC
ADM DIV OF TIDC
POLICY & PUBLICATIONS MGT BR
PDR NUREG COPY
LA 212
WASHINGTON DC 20555