3.9 OPERATIONAL SAFETY INSTRUMENTATION, CONTROL SYSTEMS, AND ACCIDENT MONTITORING INSTRUMENTATION

Applicability:

Applies to plant instrumentation system.

Objective:

To specify the conditions of the plant instrumentation and control systems necessary to ensure reactor safety.

Specification:

A. Reactor Protective System

The minimum number of operable reactor protective system functional unit channels shall be as shown in Table 3.9-1 when the reactor is at hot standby or power operation.

Exception:
One channel in each functional unit may be made inoperable by bypassing for purposes of surveillance, trouble shooting or maintenance. This exception does not apply to the manual trip functional unit.

Remedial Action:
With one channel in a functional unit inoperable, restore that channel to operable within 48 hours. (A channel in the tripped condition is considered operable.) This remedial action does not apply to the manual trip functional unit.

B. Engineered Safeguards Features Actuation System

The minimum number of operable sensors per engineered safeguards system actuation subsystem shall be as shown in Table 3.9-2 whenever automatic initiation of engineered safeguards systems is required to be operable.

Exception:

1. One subsystem may be removed from service for maintenance or on-line testing for a period not to exceed 24 hours.

2. One sensor in each functional unit may be made inoperable by bypassing for purposes of surveillance, trouble shooting or maintenance. This exception does not apply to the manual actuation device.

Remedial Action:
With one sensor in a functional unit inoperable, restore that sensor to operable within 48 hours. (A sensor which has been placed in a configuration which simulates the tripped condition is considered operable.) This remedial action does not apply to the manual actuation device.

C. Accident Monitoring Instrumentation

The minimum number of accident monitoring instrumentation channels shall be as shown in Table 3.9-3 when the reactor is in the power operation condition.

Remedial Action:
In the event the number of operable accident monitoring instrumentation channels falls below the Minimum Channels Operable requirements in Table 3.9-3, either restore the inoperable channel(s) to operable status within 48 hours or be in at least hot shutdown condition in the next 6 hours.

Basis:

The reactor protection system is designed to rapidly shutdown the reactor automatically in the event that selected nuclear steam supply system conditions deviate from predetermined ranges. The system acts to prevent violation of safety limits, and maintains operation within bounds assumed in safety analyses.

The system is designed for high reliability. The design incorporates sufficient redundancy to assure that surveillance testing, trouble-shooting, and maintenance activities can be accomodated with margin. This specification establishes the limiting conditions for operation necessary to maintain adequate system reliability under anticipated operating conditions.

Each automatic trip function usually operates in a two-out-of-four coincidence mode. One trip channel at a time within a functional unit can be bypassed, in which case a trip signal generated by that channel will not contribute to the coincidence necessary to produce a reactor trip. In this case, a coincidence trip of two of the three remaining channels will produce a reactor trip. Bypass of a channel is limited to 48 hours to restrict the time when the degree of redundancy is reduced to one.

An inoperable channel, i.e., one that cannot automatically develop a trip signal as required, may be restored to operability by placing it in the trip mode. In this case, only one additional trip of the three remaining channels in the functional unit is required to produce a reactor trip. This restores the degree of redundancy to two. An inoperable channel made operable by placing it in the trip mode may be subsequently bypassed for troubleshooting and maintenance or surveillance when such activities must be performed or are best performed under bypass conditions. This flexibility is permitted to allow a malfuncting channel to be repaired and restored to service without necessitating a shutdown and to avoid long periods of operation of a repairable channel in the trip mode.

Although no credit is taken for the high rate-of-change-of-power channel in the Maine Yankee accident analysis, operability of this channel at low power levels provides back up assurance against excessive power rate increases. Temperature feedback effects protect against excessive power rate increases at higher power levels.

Redundant sensors and logic are provided for the initiation of all engineered safeguards systems. In both the containment isolation and containment spray systems, two identical subsystems are used in each system. In the safety injection actuation systems diverse sensors are used for the initiation of two identical subsystems. Each of these three engineered safeguards systems may be operated, as shown in Table 3.9-2 and the associated exceptions, without jeopardizing safeguards initiation. One subsystem may be removed from service for a limited time for purposes of maintenance or testing because it is highly unlikely that a failure of the operable subsystem would occur concurrent with an accident requiring engineered safety features actuation. The second exception allows testing, troubleshooting or maintenance that must be performed or is best performed under bypass conditions. This flexibility is permitted to allow a malfunctioning sensor to be repaired and restored to service without necessitating a shutdown and to avoid long periods of operation of a repairable sensor in the trip mode.

The safety injection actuation system is initiated by two out of four pressure sensor channels. When three sensors are operable the degree of redundancy, as defined in the definitions section, is one. This degree of redundancy is also provided when two sensors are operable with a third sensor placed in a configuration which simulates the tripped condition.

The minimum number of operable channels for the accident monitoring instrumentation is given in Table 3.9-3. The accident monitoring instrumentation is used to evaluate and aid in mitigating the consequences of an accident.

TABLE 3.9-1

Instrumentation Operating Requirements

for Reactor Protective System

No.	Functional Unit	Minimum Operable[a] Channels	Bypass Conditions	
1	Manual (trip buttons)	1 set	None	
2	High Rate-of-Change Power	4	Below 10^{-4}% and Above 10% of Rated Power (b)	]
3	High Power Level	4	None	]
4	Thermal Margin/Low Pressurizer Pressure	4	Below 10% of Rated Power (b)	]
5	High Pressurizer Pressure	4	None	]
6	Low Reactor Coolant Flow	4	Below 2% of Rated Power (b)	]
7	Low Steam Generator Water Level	4	None	]
8	Low Steam Generator Pressure	4	100 psi Above the Trip Setpoint	]
9	High Containment Pressure	4	None	]
10	Axial Flux Offset	4	Below 15% of Rated Power (b)	]

(a) A Channel in the tripped condition is considered operable.]
(b) As indicated on Nuclear Instrumentation Channels.

TABLE 3.9-2

Instrumentation Operating Requirements

for Engineered Safeguards Systems

No.	Functional Unit	Minimum Operable Sensors[a] Per Subsystem	Bypass Conditions	Initiation Set Points
1	Safety Injection:			
	A. Manual	1	*	
	B. High Containment Pressure	4	*	less than 5 psig]
	C. Low Pressurizer Pressure	4	*	greater than 1585 psig]
2.	Containment Spray:			
	A. Manual	1	*	
	B. High Containment Pressure	3	*	less than 20 psig]
3	Containment Isolation:			
	A. Manual	1	*	
	B. Containment High Pressure	3	*	less than 5 psig]

(a) A sensor which is placed in a configuration which simulates the tripped condition is considered operable.]]

* Reactor coolant pressure less than 1685 psig.

TABLE 3.9.3

Accident Monitoring Instrumentation

	Instrument	Minimum Channels Operable
1.	Pressurizer Water Level	1
2.	Auxiliary Feedwater Flow Rate	1 per Steam Generator
3.	Reactor Coolant System Subcooling Margin Monitor	1
4.	PORV Position Indicator (Accoustic Flow Sensor)	1/valve
5.	Safety Valve Position Indicator (Acoustic Low Sensor)	1