CHAPTER 5: REACTOR CONTROL AND PROTECTION

MODULE 3: REACTOR SHUTDOWN SYSTEMS

Introduction

The shutdown systems are designed to shut down the reactor under abnormal or potentially hazardous operating conditions. To ensure high reliability two completely independent systems are provided: ShutDown System 1 (SDS1) and ShutDown System 2 (SDS2). SDS2 is designed to operate at higher 'trip' levels than SDS1 and ensures reactor shutdown should SDS1 fail.

Both shutdown systems are designed to quickly insert sufficient negative reactivity into the reactor core to reduce the reactor power output to a safe, low level. The conditions which would cause the shutdown systems to come into operation are:

(1) Loss of reactor regulation.
(2) Loss of effectiveness of the primary heatsink.

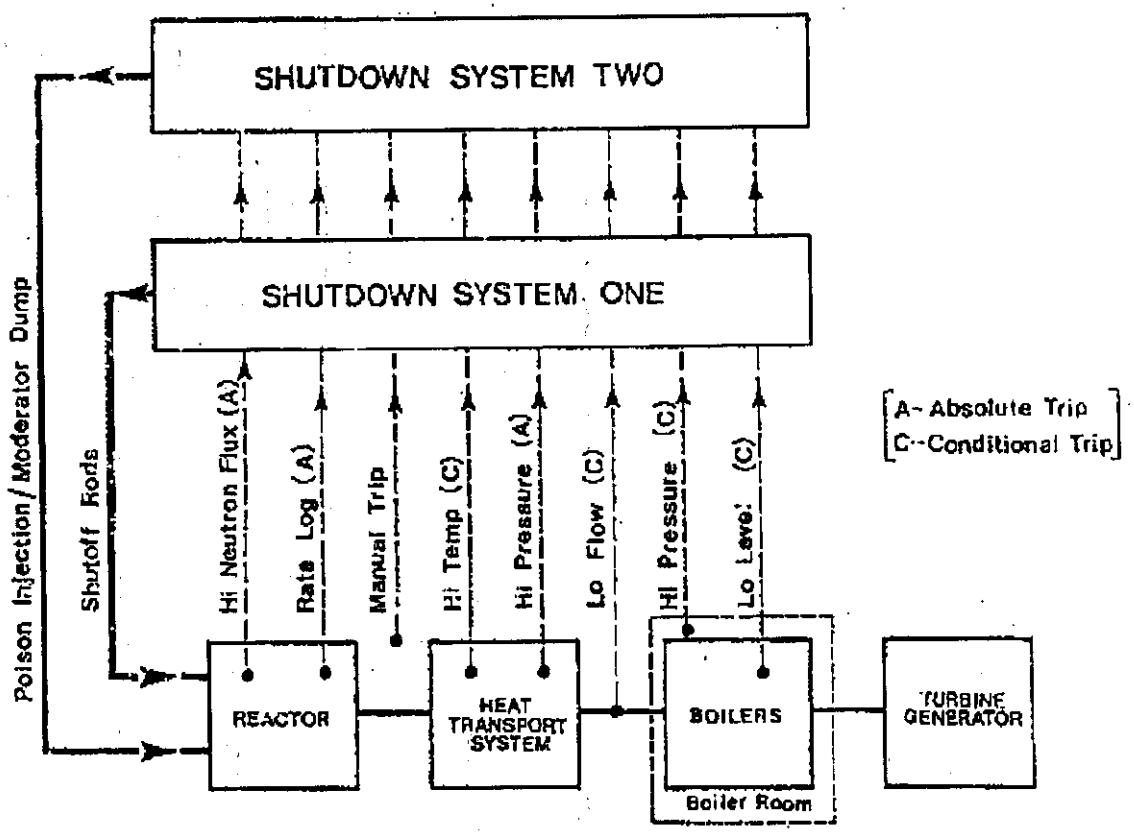

Figure 1: Typical CANDU Shutdown System Block Diagram.

Trip Conditions

SDS1 is designed to meet all the safety conditions listed and yet allow the reactor to be quickly restored to fully operational conditions without exceeding the Xenon poisoning out period of approximately 40 minutes.

SDS2, as a backup method, is somewhat more drastic and its operation will mean that a poisoning out due to Xenon will occur as the recovery period from a SDS2 trip will be in excess of 40 minutes.

To meet shutdown system requirements, it is necessary to monitor several key parameters at all times. These parameters have "trip" values assigned. These 'trips' are either absolute (i.e., valid at all states of reactor power), or conditional (i.e., available only above 2% FP).

Loss of reactor regulation is detected by continuously monitoring both gross neutron flux levels and the rate of increase in neutron flux levels by means of neutron detectors (e.g., ion chambers). It is necessary that these detectors should be fast acting so that safety action is initiated at the instant the trip parameter is exceeded.

Recall that the rate of change of neutron population (and hence, reactor power) essentially follows a logarithmic function. The time taken for reactor flux to increase by a factor 'e' (base of natural logarithms, equal to 2.718) is defined as the reactor period. Typical reactor periods for CANDU systems are reasonably. long (in the order of 100 sec). The trip parameter for rate of change of reactor power is set for a reactor period of 10 sec (approximately 10% of typical period) and is defined as the Rate Log Trip. A ten second reactor period corresponds to a rate of change in power increase of 10% power per second. (Note: this is 10% of the power level existing at any state of reactor operation). Rate Log is the abbreviated form of Rate of Change of the Logarithm of Neutron Flux.

The high neutron power limit is a basic design parameter and is set to a level at which fuel bundle maximum over power ratings are not exceeded.

The above parameters are absolute. A further absolute trip parameter is high heat transport system pressure. This condition is likely to be exceeded if the heat sink capacity on the generator side of the heat transport system is drastically reduced. For example, tripping of the turbine could cause this condition.

Conditional trips are armed automatically at an output level of greater than 2% full power. Below this level of power it is unlikely that these trip parameters will be exceeded, or their consequence is not critical to safe reactor operation. Protection will still be provided at low power levels by the absolute trips.

In order to meet the requirement of continuous availability, it is essential that the shutdown systems should be made as nearly as possible 100% reliable.

- The equipment chosen should therefore be of the highest quality with key items triplicated.
- It is also essential that the system should be available for testing at all times and this, together with any maintenance requirements, implies that each trip system should have more than one channel.
- In fact, each system, SDS1 and SDS2, consists of three separate and independent channels (Channels D, E and F for SDS1 and Channels G, H and J for SDS2) with a requirement that two of the three channels must exceed the setpoints before a reactor trip is initiated. This removes the possibility of spurious trips causing a reactor shutdown.
- It should also be noted that equipment used on shutdown systems is allocated exclusively to shutdown and for no other purposes.
- In addition, interlocks are provided such that if a shutdown system has been operated, it is not possible to insert any positive reactivity into the reactor core by, for example, insertion of booster rods or removal of adjuster rods. This eliminates the possibility of the reactor power increasing while the original fault condition still exists.

Shutdown System One

This system consists of stainless steel encased, hollow cadmium rods which drop, under gravity (and for some reactors assisted by springs), into the reactor core in the event of a trip. The rods are an effective neutron absorber which quickly reduce the reactor power to a safe, low level. These rods are retracted on cables which are connected to a winch via an electromagnetic clutch and are normally suspended out of core in a 'poised' state.

A simplified schematic diagram of SDS1 is shown in Figure 2.

- Each individual trip channel can be triggered if any trip parameter for that channel is exceeded.
- We must also ensure that the system is fail safe so that in the event of an equipment or power failure, the shutdown system will fire and the reactor will be shut down, albeit for an erroneous reason. The general method of achieving this fail safe condition is to ensure that the system operates on the de-energizing of devices.

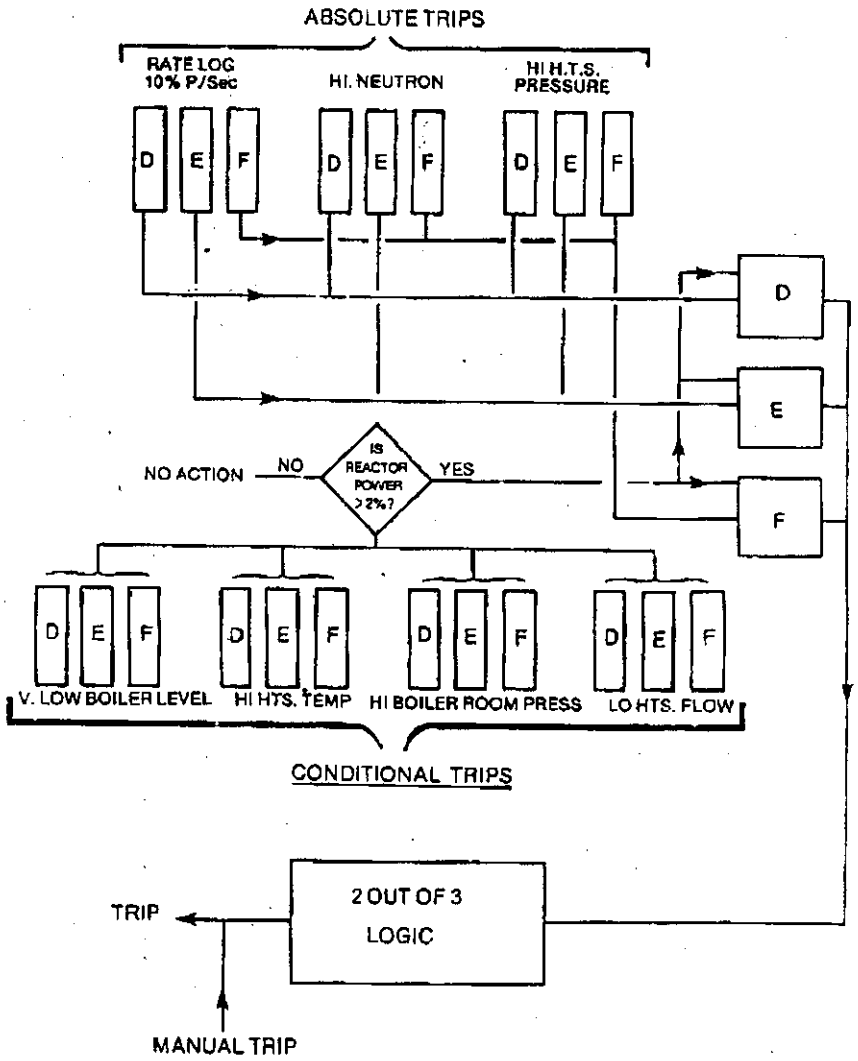

Figure 2: Shutdown System One Schematic.

A more detailed diagram of SDS1 is shown in Figure 3. The relays associated with the individual trip parameter detectors (RL1, 2 & 3; HN1, 2 & 3; HTS1, 2 & 3) are energized when the reactor is operating normally. The individual relay contacts (1RL1 etc.) are therefore closed and thus, relays D, E and F are energized. The contacts D_1, D_2, E_1, E_2, F_1 and F_2 are also closed and a current path exists through the electromagnetic clutch. This clutch when energized, holds the shutdown rod, suspended on its cable, out of the reactor core., This arrangement of relay contacts is known as a triplicated contact set. It ensures that the two out of three requirement for tripping is maintained. In practice, there are multiple sets of Relays D, E and F. Each triplicated contact set controls one pair of shutdown rods.

Consider, for example, a Rate Log Trip occurring on Channel D. Relay RL1 will de-energize opening contact 1RL1. This will cause relay D to de-energize with the consequent opening of contacts D_1 and D_2. A current path through the clutch still exists, however via contacts F_2, E_1 and either E_2 or F_2, and the clutch remains energized. The shutdown rod will not drop into the reactor. As this trip occurred only on channel D, the two out of three criterion has not been met and therefore no reactor trip has occurred and the cause of the incident should quickly be investigated.

Now consider a trip, say High Neutron Flux, on channels D and E. Contacts 1HN1 and 1HN2 would open, de-energizing relays D and E. Contacts D_1, D_2, E_1 and E_2 open, the clutch is de-energized, the shutdown rod will drop and the reactor will be shut down. In actual fact, there is, a bank of shutdown rods to distribute the shutdown action throughout the reactor.

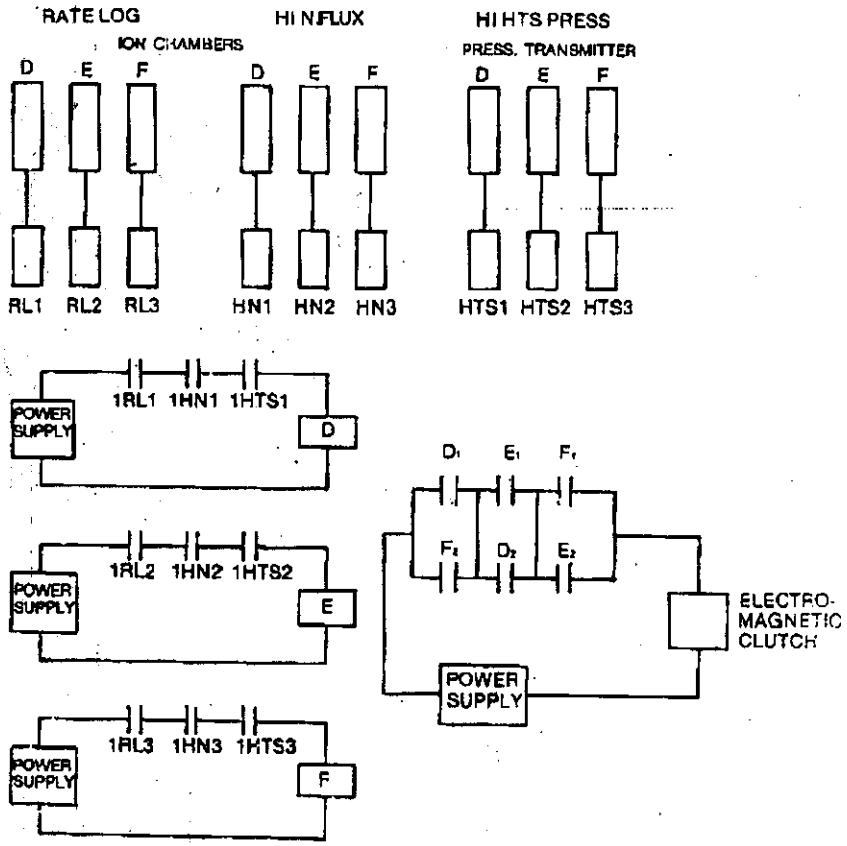

Figure 3: SDS1 Control Schematic.

It can be seen that the arrangement of equipment as shown in the previous diagram, fulfills all the reliability requirements of the shutdown system:

- System is not susceptible to spurious trips.
- Two out of three channels are required to initiate trip action.
- On-line testing and maintenance of individual channels is possible.

To enable testing, and to give further indications to the operator of equipment serviceability, modifications to the triplicated contact set are made by the addition of resistors R_1, R_2 and R_3 in one leg of the contact set.

Under normal operating conditions, with all contacts closed, the preferential (low resistance) current path will be via contacts D_2, E_2 and F_2 with a current indication shown on the ammeter M1.

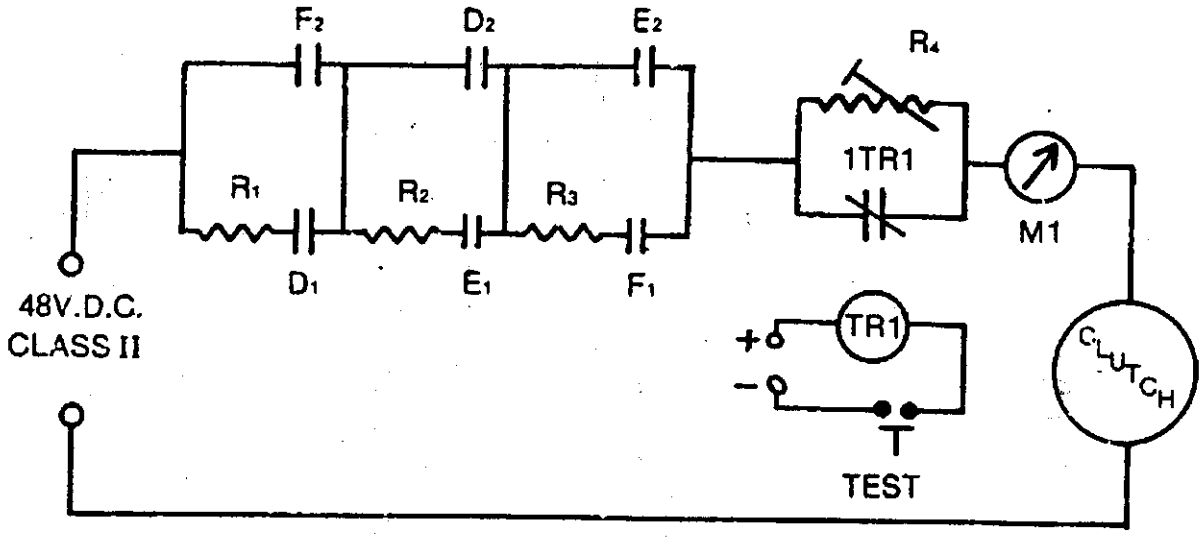

Figure 4: Current Monitoring and Partial Drop Test Circuitry.

Should a trip occur on just one channel, say D_1 contacts D_1 and D_2 will open and the current path to the clutch will now be via E_2, F_2 and E_1. (Note: only one channel tripped, so no shutdown). The presence of R_2 will lower the current flowing in the circuit with a new, lower, indication shown on M_1. This, in addition to a warning annunciation lamp, will indicate to the operator that one channel has tripped.

To ascertain full system reliability, it is also necessary to check that the shutdown rod is free to drop, when the clutch is de-energized.

- It would not be desirable, due to the large local negative flux transient which would occur, to drop any rod over its full distance into the core.
- If we can arrange to drop the rod for a limited distance only, we can be reasonably certain that, in the event of a trip, the rod is able to drop to its limit.
- This procedure is known as a Marginal Drop Test and is performed, on one rod at a time, by the following means:

Relay contact 1TR1 is normally closed (Relay TR1 - de-energized). Resistor R_4 is adjusted such that, when in circuit, (i.e., when 1TR1 is open) the current flowing through the clutch will be reduced such that the clutch can not quite sustain the load, and the rod will drop. Relay TR1 is a timer relay. operation of the Marginal Drop Test switch button will energize the relay for a period of about, 0.2 sec. During this time interval 1TR1 will open, R_4 will be in circuit, clutch current will be reduced and the shut off rod will drop. The distance dropped (typically 1.2 metre) will be indicated on a meter. The contact TR1 will then close, the clutch is re-energized and the rod will be retracted to the 'poised' position by means of the motor driven winch.

Operation of the Manual Trip will de-energize all three channels.

Shutdown System Two

Shutdown system two is similar to shutdown system one with the following differences:

- **Higher trip set points.**
- **The final negative reactivity device.**

With one exception all CANDU units have a SDS2 that operates by injecting, under high pressure, a suitable neutron absorbing liquid (poison) into the reactor. The poison chosen is Gadolinium Nitrate.

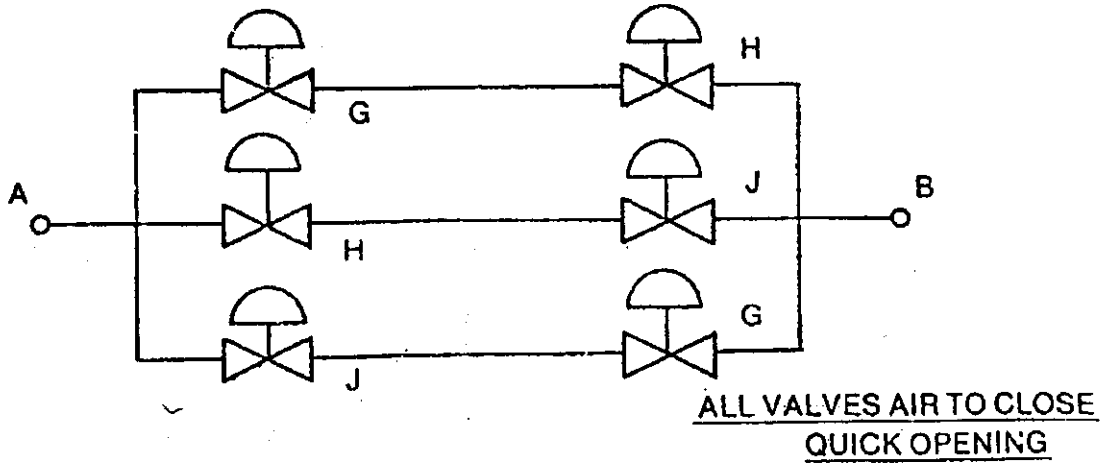

Figure 5: SDS2 Control valve Arrangement.

The system has a two out of three trip circuit using control valves instead of relay contacts.

- **The valves used are air to close style so that following a loss of instrument air, the valves will fail open and a reactor shutdown (fail safe) will occur.**
- **In the event of a trip, the air supply to the valves is dumped via electrically operated solenoid valves.**
- **If any two of the three pairs of valves open, a flow path will be established between A and B, injecting the poison.**

Poison Injection System

Some of the general principles introduced in this lesson can be demonstrated by examining the poison injection system (SDS2) utilized at a CANDU reactor. The triplicated channels are designated as G, H and J and can be activated manually or by such trip parameters as rate log, high neutron power, or high primary heat transport pressure.

The helium storage tank is maintained at approximately 8 MPa.

Should a trip request be initiated by at least two of the three channels, the poison injection valves will open and apply the stored helium pressure to the gadolinium nitrate in the seven storage tanks.

The poison is forced through the seven injection nozzles by the helium pressure so that it is sprayed into the centre of the reactor core.

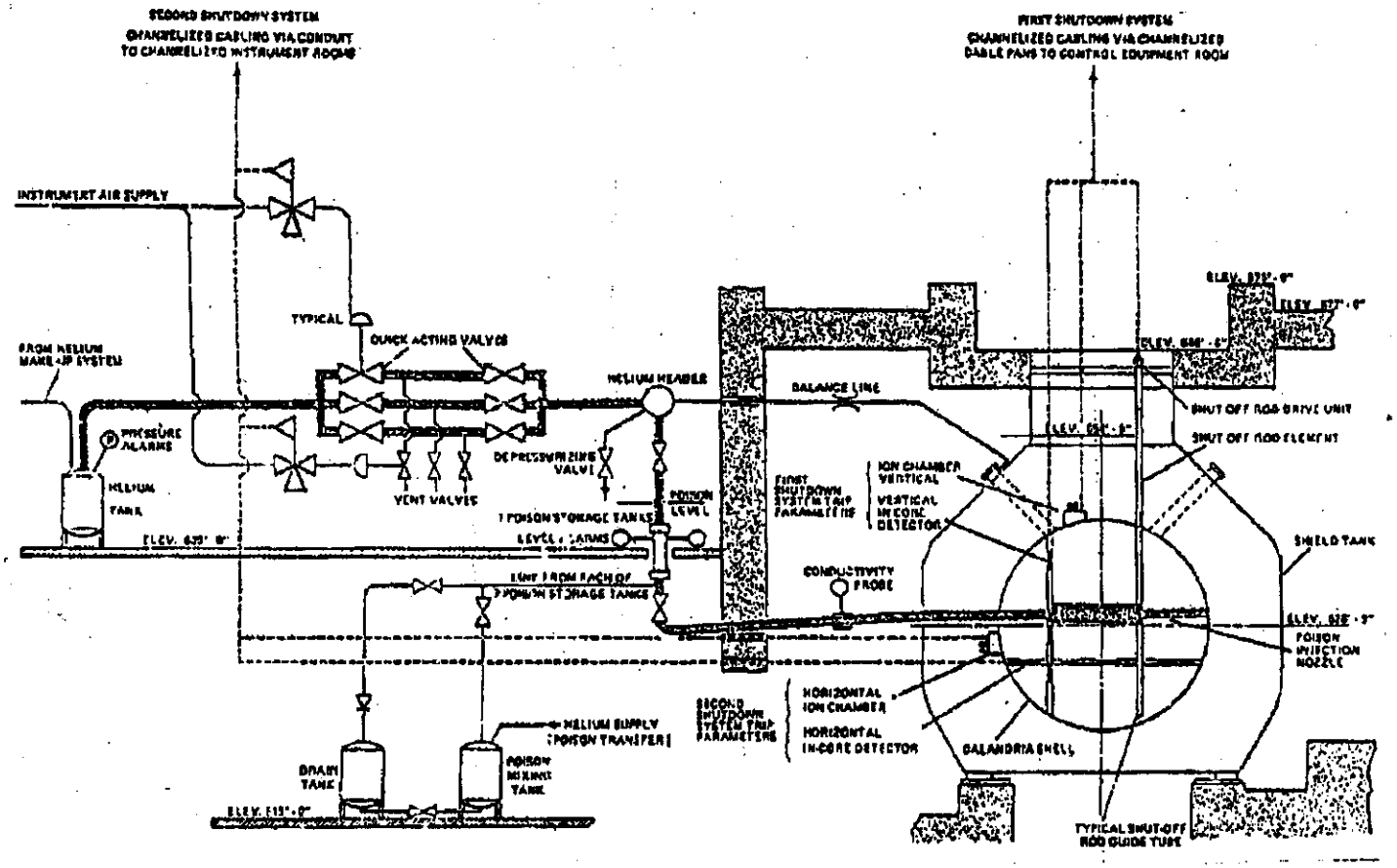

Figure 6: Simplified Schematic for SDS2.

The poison tanks each contain a polyethylene ball which floats on the surface of the poison. When the poison is injected, the ball will be forced onto the lower seat in the poison tank and prevents the helium gas from over-pressurizing the calandria.

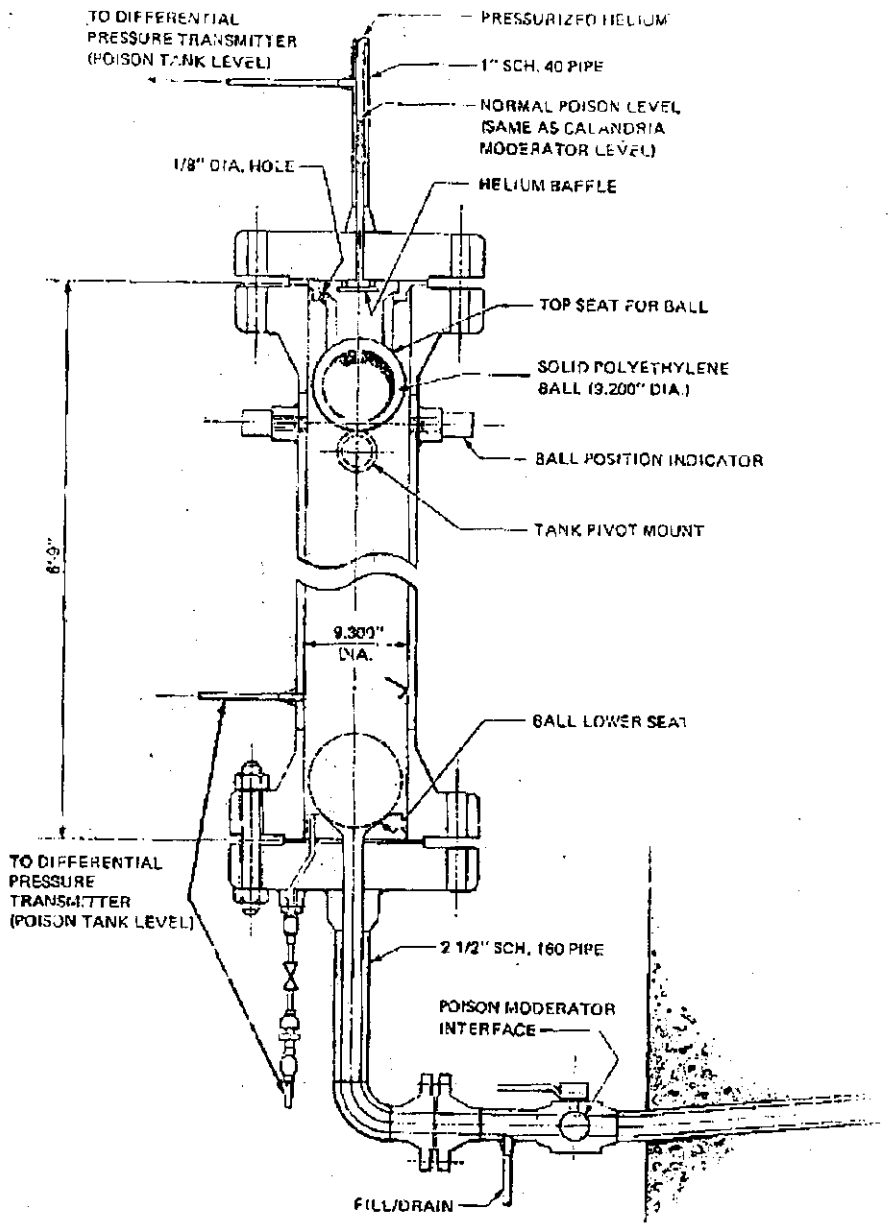

Figure 7: Gadolinium Poison Tank.

The triplicated valve configuration consists of the six injection valves (MV1G, 2G; MV1H, 2H; MV1J, 2J) and the three interspace vent valves (MV3G, MV3H, MV3J). All nine of these valves are of the air to close, quick-open type. The poison injection valves will have some seat leakage when the valves are closed. With the large differential across the closed valve, a substantial pressure could build up between the two injection valves. This would then result in pressure leakage across the second injection valve and the possible accidental injection of the poison into the moderator. To counteract this problem, the interspace vent valves are held open as long as the channel is energized. These valves will vent the interspace so that the seat leakage of the poison injection valves is not a problem.

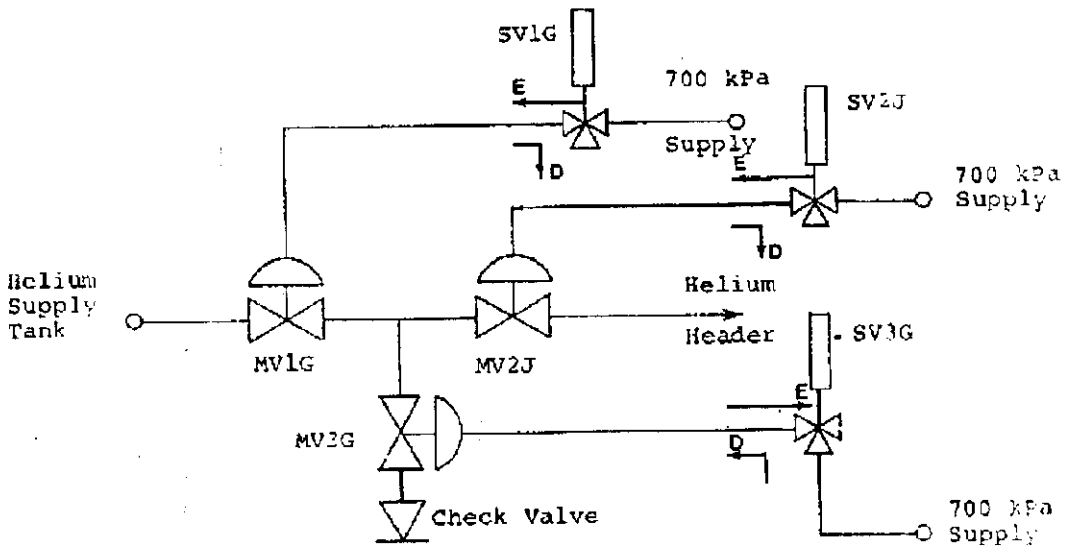

Figure 8: Connections to Injection and Vent Solenoid Valves.

System Operation

Assume channels G and J are energized (refer to Figure 9). Then SV1G, SV2J, and SV3G will all be energized so that the 700 kPa(g) signal is applied to MV1G and MV2J holding these injection valves closed. MV3G is able to vent through SV3G so that the interspace vent valve will be open. Should a trip occur, these solenoid valves would become de-energized, allowing the injection valves to open and the interspace vent valves to close.

A simplified trip channel (for example G in Figure 9) can be considered for this injection system. For simplicity, consider only high neutron power or rate log as the parameters which will activate SDS2.

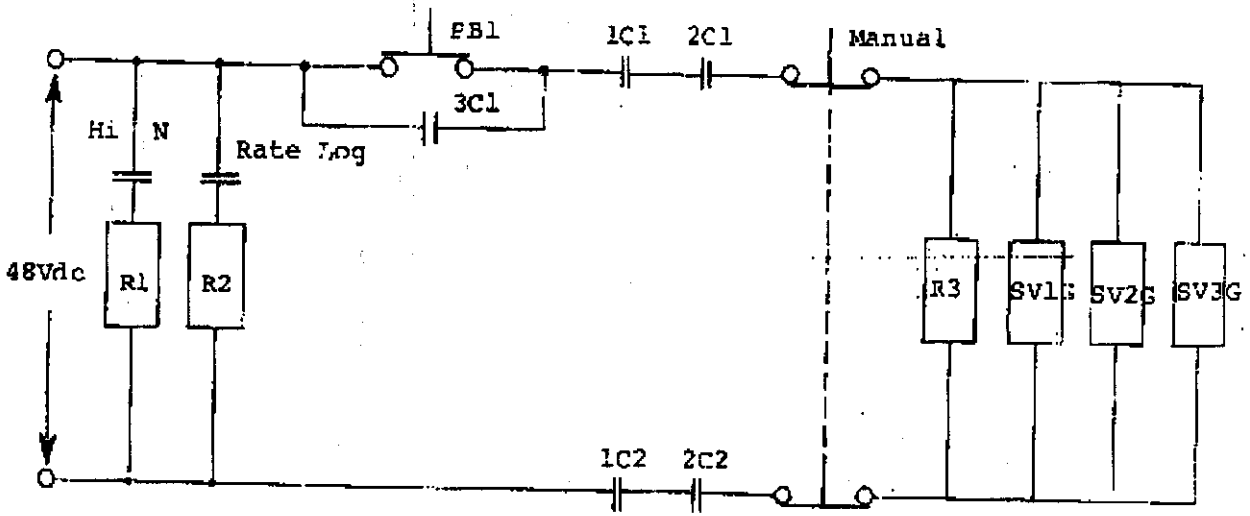

Figure 9: Simplified Trip Channel G for SDS2.

Assume a rate log trip occurs so that relay R_2 is de-energized. Immediately contacts 2C1 and 2C2 will open and remove power from relay R_3 and the three solenoid valves (1G, 2G & 3G) . The poison injection valves will drive open and the vent valve will close due to the change in status in the solenoid valves. Contact 3C1 will open since relay R_3 was de-energized. Notice that if only channel G had tripped, a complete injection would not occur. Two of the channels must request safety action before a trip can occur.

If this was a spurious trip, the rate log contacts would reclose, but the channel would not be energized since the trip was latched in by relay R_3. Operating staff would have to depress pushbutton PB1 to reset the channel. Pushing PB1 will apply power to R_3, SV1G, SV2G, and SV3G. Contact 3C1 will close so that power is maintained to the equipment mentioned when the pushbutton is released (3C1 bypasses PB1). The channel has been restored or reset to its pretrip status.

Testing and maintenance can be carried out on individual channels without tripping the reactor. The control valve state, i.e., closed for normal operation, is verified by control room indication.

Normal System Operation (SDS1 and SDS2)

During normal reactor operation, both shutdown systems must be available and operational at all times. The minimum number of shutdown rods to guarantee reactor shutdown (safety bank) must also be available. Maintenance of more than one channel at the same time is not allowed.

Testing and maintenance should be performed with the reactor at full power in order to verify the full power trip settings. Various control room indications are available to ascertain that the systems are fully operable. The flux detectors can be tested by driving a boron shutter which is a neutron absorber located near the detector. This should result in a rise in indicated neutron flux readings which has the effect of testing the complete channel for both Rate Log and High Neutron Flux. Control room indications are also available to verify that supply voltage to the neutron detectors is present and at the correct value.

During normal (i.e., safe) conditions, certain changes in reactor operation are necessary which, if not compensated for, could produce situations where trip parameters would be exceeded unnecessarily with shutdown of the reactor occurring. Consider for example, requests for increases in power output. Power increases are computer controlled, and applied at a rate such that the High N and the Rate Log Trip Setpoints should not be exceeded. It is necessary at these times that the operator visually checks the neutron instrumentation to ensure that trip settings will not be exceeded.

Refuelling can cause large fluctuations in neutron detector output. This is due simply to the physical movement of neutron absorbers (metal fuelling ram extension or spent fuel), or neutron producers (fresh fuel) between the detectors and the usual neutron source (reactor core). Increased instrumentation surveillance is necessary during refuelling to ensure that compensation is present and that the Neutron Flux (High Neutron and Rate Log) trip parameters are not likely to be exceeded.

Abnormal Operating Conditions

Should a single channel trip, the operator must first establish, by instrumentation inspection, whether the trip was genuine or through an equipment malfunction. In the event of a genuine trip due to a transient condition occurring on just one channel (e.g., during refuelling) the channel may be reset after the transient has subsided. If the trip was the result of equipment failure, the channel must be rejected, the necessary approval for maintenance must be obtained, and the work carried out. If for any reason, a single channel has been worked on during an outage, that channel must be rejected until normal operating (full power) conditions have been attained to permit the proper testing under in-service conditions. Normal testing and maintenance must be carried out at full power.

In the event of a complete reactor trip, it is first necessary for the operator to establish, from his instrumentation and read out devices, the cause of the trip. He must then decide whether it is possible to diagnose and clear the fault within thirty minutes and thus be able to restore criticality before poisoning out.

Should a shutdown rod become trapped in the core (say faulty marginal drop test), this condition will be indicated by the appropriate shutdown rod position meter. Severe local flux distortions will result. These local negative reactivity excursions may be partially corrected by other reactivity devices, (e.g., adjuster rods and liquid zone level adjustment). However, the power output must be reduced to avoid local fuel overrating and possible fuel failure.

Care must also be taken when operating with the heat transport system at reduced pressure. The heat transport system will boil if the pressure is allowed to fall too low. This will result in cavitation of the pumps and a low condition may develop which could cause a conditional trip. If boiling were allowed to persist, voiding in the fuel channels could occur. This condition would case the reactivity to increase which could also trigger a neutron trip.

Grounding Problems

Ground faults appearing in a trip channel circuit must not be able to make that channel fail unsafe. Consider a simplified trip channel consisting of a power supply, a contact set, and a relay. De-energizing the relay by opening the contact set will initiate safety action.

Ground faults can occur in a system as a result of physical abuse or dampness allowing a leakage path. Imagine someone drilling through a tray bracket, and the drill bit nicks the insulation allowing the conductor to contact the bracket screw. On the other hand, the insulation of a flexed portion of the cable may become cracked and split, and allow a current to flow to ground if the cable should become wet.

The ground faults (G1 and G2) shown in Figure 10 can allow a ground current flow (Ig). This ground current may be sufficiently large to keep the relay energized. In this case, the trip contacts can be opened or closed, and the relay will remain energized. This is a potentially hazardous situation where the ground faults have caused the trip channel to fail unsafe - a requested trip would be ignored.

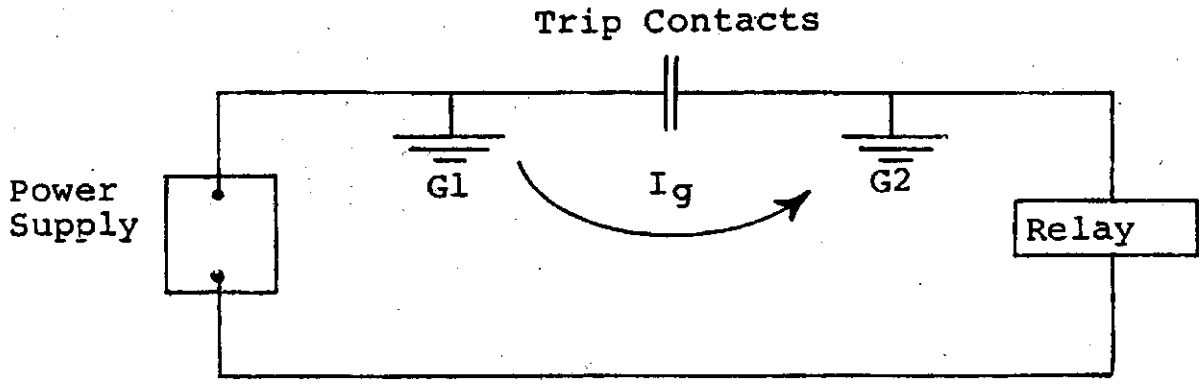

Figure 10: A Simplified Trip Channel with Ground Faults G1 and G2.

One solution to this problem that is employed in conventional instrumentation loops is to apply an intentional ground to the power supply.

The disadvantage of applying an intentional ground is that one ground fault appearing on the trip channel can now cause a channel trip request. For example, if ground fault G_1 appears as shown in Figure 11, the ground current effectively shorts out the relay. The relay is de-energized and safety action is initiated. This results in ground faults causing an unnecessary channel trip - but the trip channel has failed safe.

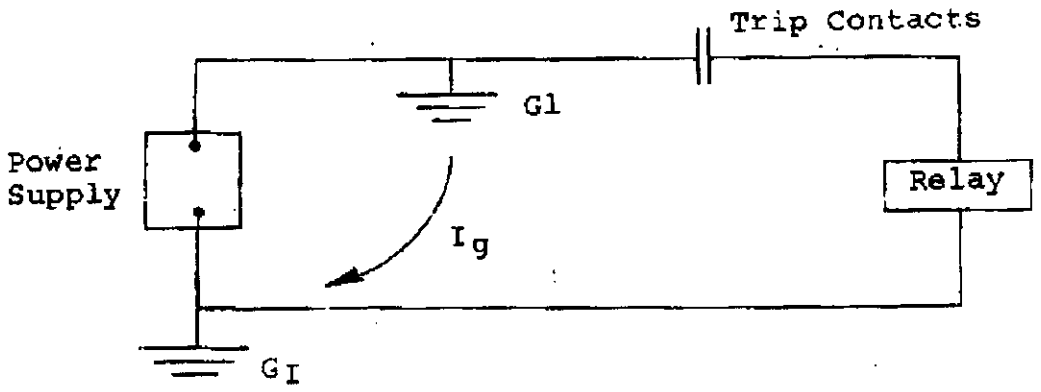

Figure 11: A Trip Channel with an Intentional Ground (G1)

An improvement in the trip channel performance with ground faults can be achieved by duplicating the trip contacts on both sides of the trip channel.

If ground faults G1 and G2 should now occur, the top line of the trip channel would appear as a complete circuit regardless of the trip contact status. However, the second contact on the lower line of the trip channel can still open the circuit if a trip is requested. This channel will now initiate safety action even with two ground faults (G1 and G2) present. Should ground faults appear on both sides (unlikely) of the channel (G1 and G3) then the ground current flow can short out the relay. Ground faults appearing on both sides of the trip channel will cause an unnecessary trip, but the channel will fail safe.

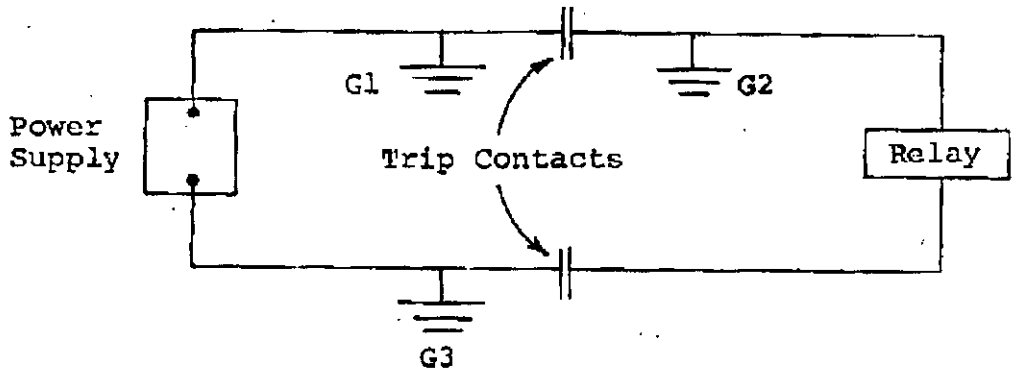

Figure 12: A Trip Channel with Duplicated Trip Contacts.

Ground Faults on the Triplicated Contact Set

Consider the Triplicated Contact Set as shown in Figure 13.

Note that as the normal circuit is not referenced to ground at any point, the circuit will show complete immunity to a single ground fault. More than one ground fault may or may not affect the reliability of the circuit depending upon their location. The worst possible location for multiple ground faults is at position A & B. This could by-pass the contacts and disable one set of shutdown rods. However ground detection equipment is installed for Class II systems. This will inform staff that a ground fault has occurred, enabling maintenance action to be initiated.

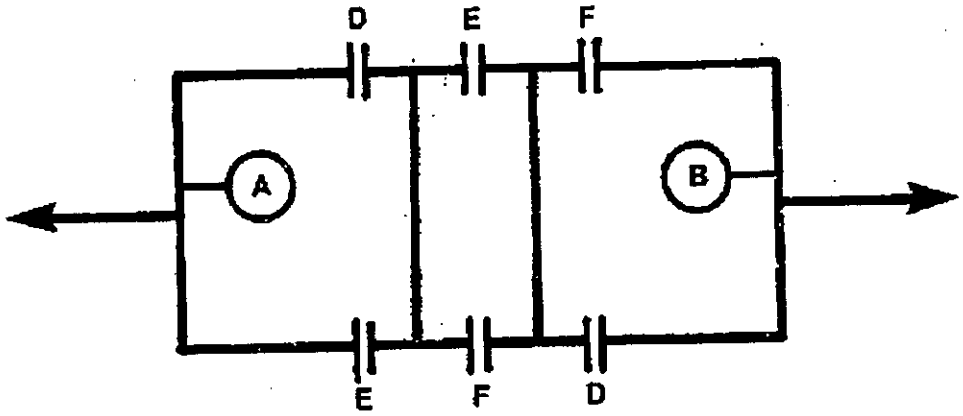

Figure 13: Triplicated Contact Set.

Summary

Recall the conditions for fail safe operation. The complete loss of electrical power to either shutdown system will result in a reactor trip. Loss of air to the control valves for shutdown system two will result in a reactor trip. Remember also that operation of SDS2 will automatically result in a poisoning out of the reactor. An overriding consideration in the design of both shutdown systems is that they must FAIL SAFE. In the event of equipment failure an erroneous trip is preferred to the possibility of no trip should a safety parameter be-exceeded.

Remember, if the plant is to be in an operational state, the reactor protective system must be in a poised state in order to provide safety action at all times.

ASSIGNMENT

1. State the two prime requirements for a reactor shutdown system.

2. State two general conditions which would cause safety action to be initiated by a shutdown system.

3. Distinguish between an absolute and a conditional trip and state two typical parameters for each trip group.

4. Sketch a typical relay contact configuration used to actuate SDS1. Explain the advantages of such redundancy in a protective system, and discuss the general operation following a trip condition.

5. Refer to Figure 5 and describe how the clutch current indication (M1) will change should channel F be de-energized, opening contacts F1 and F2.

6. Describe the general method and purpose of performing

7. What are the general differences between SDS1 and SDS WRT reactivity magnitude, trip settings, and trip recovery time.

8. Sketch a typical valve configuration that could be use for either poison injection or moderator dump.

9. Refer to Figure 10 and describe the circuit response following a rate log trip. State the purpose of push button PB1. Why are Relay 1 and 2 contacts duplicate on both sides of the trip channel?

10. Briefly describe how shutdown system maintenance would be performed WRT authorization, power conditions, shift interaction and testing.

11. What operational status would a trip channel have if a faulty or suspect device was identified in that trip channels

CANDU I&C Course September 1996 - Assignment #5

1) Explain the difference between a reactor leading and a turbine leading power station control strategy. Sketch & label a block diagram to illustrate the key components for a reactor leading configuration?

2) List six reactivity control mechanisms used in CANDU reactors. Which is the principle reactivity control means?

3) Sketch a diagram which shows the preferred reactivity control by liquid zone level versus power error. Label areas on this diagram to show: high level & high positive power error and low zone level & large negative power errror. In each case - give an example of reactivity device control that you would recommend to correct the problem.

4) Sketch a typical liquid zone assembly to show the helium and water feed tube connections. Describe how water flow is allowed, pressure differential is applied and zone level measurement is possible.

5) Sketch the helium circuit for the liquid zone system and describe how the pressure differential from the top of the liquid zones (helium balance header) to the top of the delay tank is maintained relative constant.

6) Sketch the water circuit for the liquid zone system (including neutronic detectors) and describe how reactor control is achieved.

7) Sketch a typical limit control routine diagram that can be used to coordinate various reactivity mechanisms. Choose a positive going power error with rising zone levels as an example to explain the coordination of reactivity mechanisms with the principle means (liquid zone control).

8) Sketch and label a xenon transient that would be expected following a reactor trip from full power, long term operation. Label equilibrium xenon load, reactor trip point, the xenon peak transient, override time, poison outage time and first return to operation time.

9) Distinguish between a reactor trip, a reactor stepback and a reactor setback. Give an example parameter for each case.

10) Explain the difference between a absolute reactor trip and a conditional reactor trip.

11) Sketch a typical triplicated trip circuit contact set and describe how 2 of 3 channels are required to initiate the trip but so that one channel will not cause an unnecessary trip.

12) What general considerations should be made prior to starting up the reactor and at key points during the reactor power up? (for example - confidence in neutronic indicators and trips, settings for trips, availability of heat sinks, confirmation of expected performance, etc - what general considerations would you recommend and why?).

13) Sketch the injection circuit for SDS2 , a liquid poison injection system. Include, and label, the helium tank, injection/vent valve manifold, poison tanks, and injection nozzles. Describe the general principle of operation.

14) Provide a detailed sketch of one valve manifold injection flow path showing two injection valves (two different channels), one vent valve and the respective three-way solenoid valves. Describe the performance of each valve (injection, vent, solenoid) to show how a flow path can be established once both channels have received a trip signal.

15) Sketch an ungrounded circuit with a power supply, single trip contact and relay. Show how the appearance of two ground faults on either side of the trip contact could prevent the relay from being de-energized (unsafe condition). Present one solution to ensure that this circuit would be immune to such a fault or at least would fail safe (the relay would be de-energized).