NUCLEAR SAFETY AND RELIABILITY

WEEK 4

TABLE OF CONTENTS – WEEK 4

1. Reliability of Simple Systems

This material is covered in Chapter 6 of McCormick. All Sections must be well understood. General principles and simple reliability equations should be known; more complex networks, equations, etc. need not be memorized. All reliability problems can be reduced to combinations of these simple systems. The minimal-cut-set method is the one most commonly used in practice.

2. CANDU Shutdown Systems

Good examples of application of the reliability principles described by McCormick are the safety shutdown systems in CANDU reactors. The four attached Figures show the arrangement of general coincidence trip logic and actuation for SDS1 and SDS2 at Point Lepreau. It is expected that the principles and function of these systems will be understood in terms of their reliability objectives.

The main points are:

a. Each shutdown system must achieve an unavailability of 10^{-3} per year (unavailability = 1-reliability) in order to satisfy the requirements of the AECB Siting Guide. This value must be demonstrated by in-service testing. Testing can be done by setting one channel of the 2-of-3 system to the safe or "tripped" state, so that if either of the other two channels is opened, the reactor will trip. Then, components of the channel under test can be tested singly and in groups. All parts of the shutdown system can be tested this way; following which, the results can be used to calculate the actual past unavailability as well as the predicted future unavailability for the whole system.

b. The system must be designed to minimize the probability of spurious trip; i.e. the chance of any combination of components resulting in a reactor shutdown when real system parameters are within normal range. The target is less than one spurious trip per year. This is an operating reliability requirement, not a safety requirement - if the reactor is tripped spuriously then electricity production time is lost. The 2 - of - 3 system greatly assists this reliability objective, because two channels must trip spuriously at the same time before the reactor trips.

c. The two shutdown systems must be independent and diverse; that is, operation of one system must not impair operation of the other system and they must operate on different principles. They also must be independent of process systems -- those used to operate the station. This requirement must be met so that failure of one shutdown system cannot cause failure of both systems. Total independence is impossible to prove, but every effort is made to keep the systems independent.

d. At least two trip parameters on each shutdown system must be capable of detecting any system fault with high reliability and within the required time, in order to meet the safety requirements for protection of the fuel and for prevention of damage to other reactor components that could increase the severity of the initial accident.

e. To the extent possible, components must be designed to fail in the direction of safety; that is, failure of a component should lead to a "vote" for shutdown.

The first two requirements given above have led to use of a 2 out of 3 logic in all trip systems of CANDU reactors. This permits on-power testing of one trip channel while the system remains fully capable; during testing, one channel of the system is put into the "tripped" state. Therefore, during this period the trip chain is a One-out-of-Two system.

Note that any M-out of-N (M>1) logic is less reliable for trip than is One-out-of-N logic. The compromise is made to ensure operational reliability against spurious trips.

Some earlier CANDU units have Local Coincidence logic on one of the shutdown systems. This logic involves a two-out-of three vote on each trip parameter, rather than the combination of any two parameters as in the General Coincidence logic. Local coincidence systems have a higher reliability against spurious trips, but lower reliability for trip. It has been found that the spurious trip rate is low enough with modern equipment, so that general coincidence logic can be used for both shutdown systems.

The Darlington trip systems utilize digital logic, which approximately mimics the relay logic of earlier designs. A comprehensive logic testing system, which is isolated from the logic itself by optical couplings, carries out the many trip tests which are required. This testing system is much more reliable than manual testing, which has led to several spurious trips in other stations.

3. Reliability and Availability of Systems With Repair

This material is covered in Chapter 7. Only a very general understanding is expected for Sections 7-1 and 7-2. Markov models are beyond the scope of the course.

Figures 4.1 to 4.5 depict the logic of the two CANDU shutdown systems.

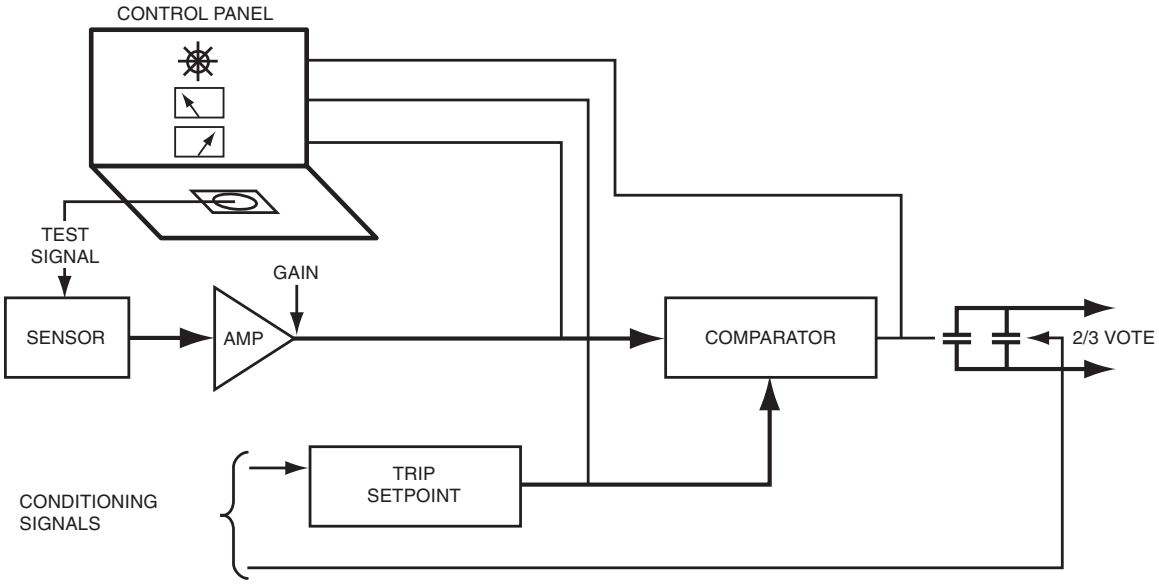
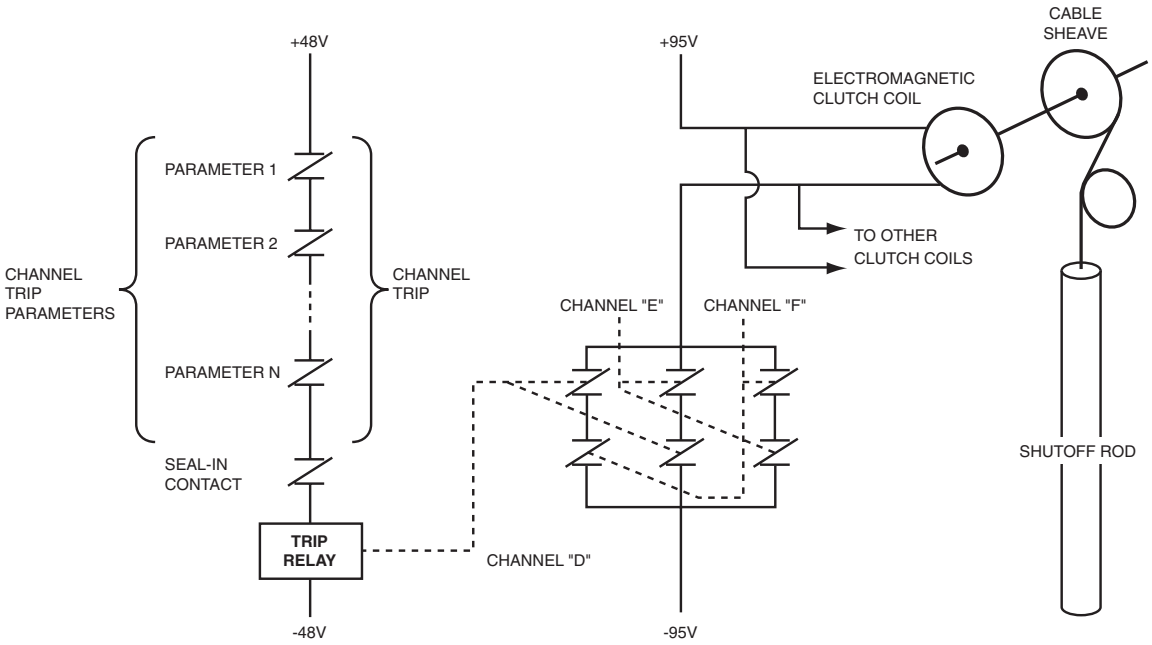


FIGURE 4.1 — COMPARATOR LOGIC



Note: This is a general coincidence circuit - opening of any one contact in each of two channels will trip the reactor

FIGURE 4.2 — SDS1 TRIP LOGIC - SIMPLIFIED

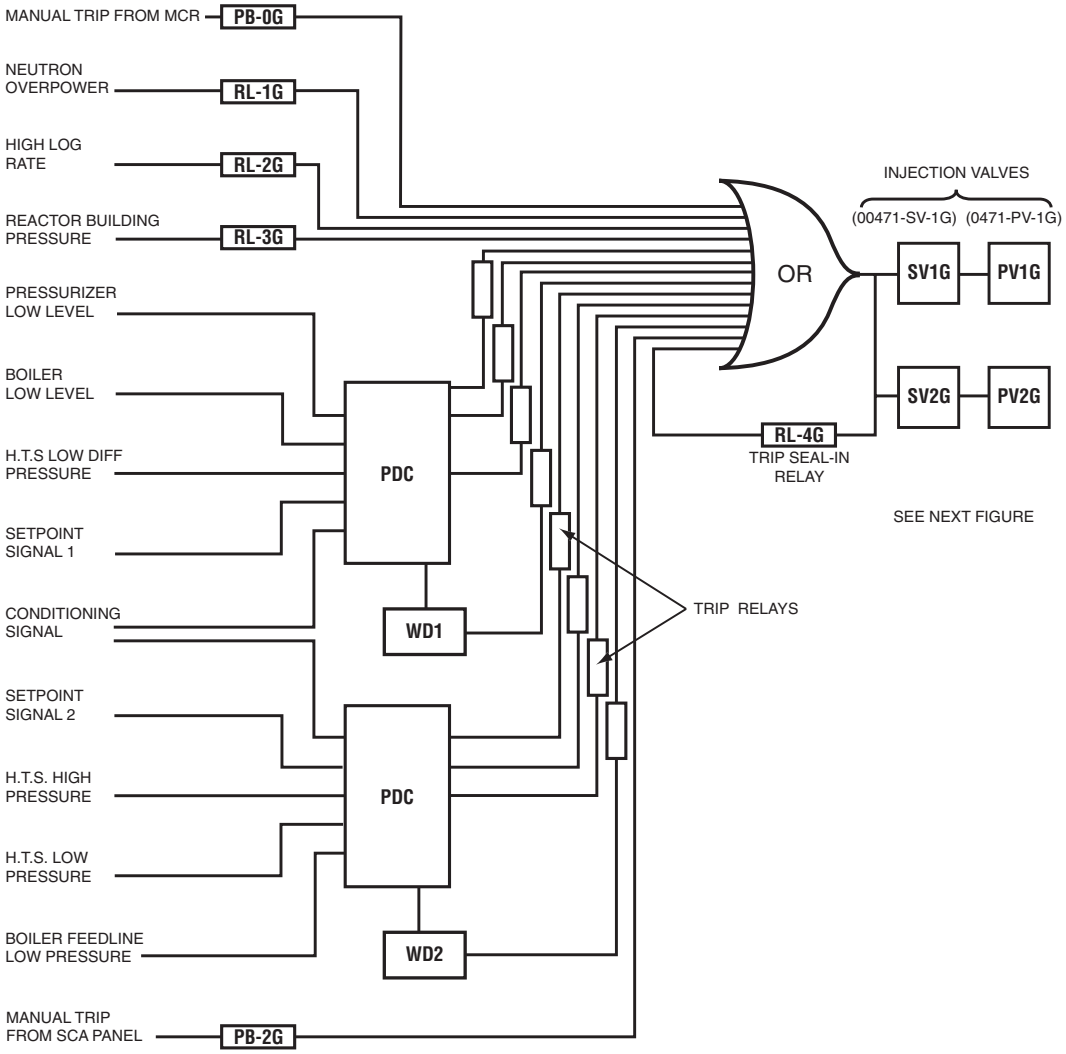


FIGURE 4.3 — CHANNEL "G" TRIP CHAIN

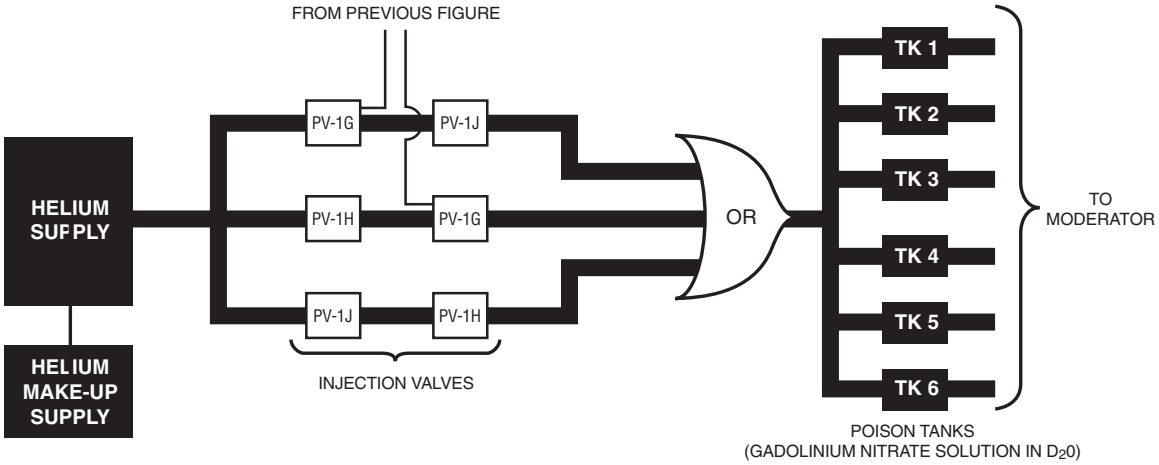


FIGURE 4.4 — SDS2 INJECTION LOGIC

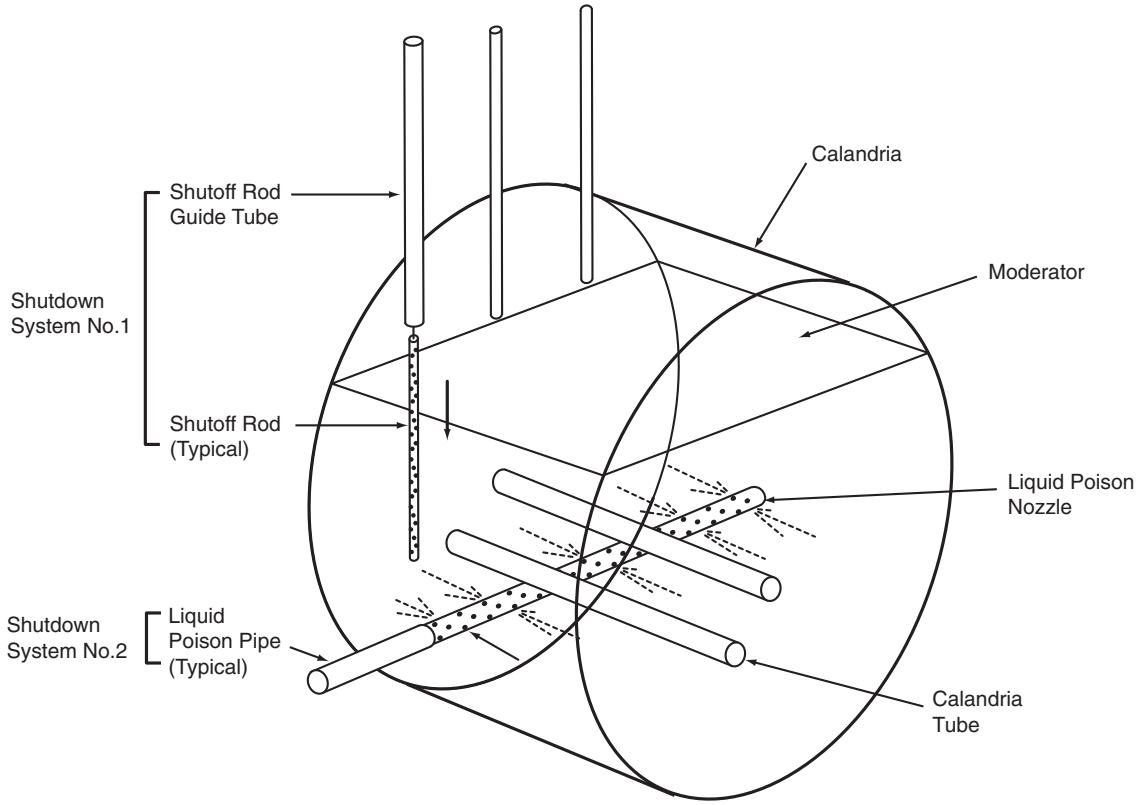


FIGURE 4.5 — GENERAL LAYOUT OF SHUTDOWN SYSTEMS