NUCLEAR SAFETY AND RELIABILITY

WEEK 6

TABLE OF CONTENTS – WEEK 6

1. Event Tree Analysis

This material is covered in Sections 9-1 to 9-3 of McCormick. These sections concentrate mostly on methods used in the US Reactor Safety Study. The only major weakness of McCormick's presentation is that it does not address the question of completeness; that is, it presumes that the collection of initiating events analyzed, along with the associated event trees, gives an estimate of the total risk spectrum from plant operation. On the contrary, the experience of past accidents indicates that event sequences usually contain unexpected events and surprises. Also, the event sequences rarely follow exactly the path expected by the designer before the accident. These sequences represent the Unidentified Failure Modes (UFM) discussed in Week 1. A careful analyst should try to select event sequences that show the essential features of plant systems, even though the details are uncertain.

The US Reactor Safety Study (or Rasmussen Study) attempted to account for the existence of UFM by increasing consequences by 20% and by smoothing the frequency distribution. The result was judged to be unsatisfactory by a senior review committee. To some degree, this objection is addressed in reactor design by requiring safety systems to be independent and redundant, so that "surprises" in one area do not propagate through to public consequences. This procedure is known as the defense in depth approach - more than one barrier exists to prevent dispersion of fission products. Nevertheless, the existence of potential UFM sequences must be recognized.

The second weakness of McCormick's presentation is that it does not address the many possible combinations of system states that can exist in the plant before an accident - many of these will change event sequence development. To analyze the consequences of each sequence independently would require thousands of event trees, thereby making the procedure impractical. It is necessary to group similar sequences into general classifications (reactor overpower, small LOCA, large LOCA, etc.) with appropriate conservative assumptions with regard to the performance of sub-systems that influence the sequence.

2. Event Tree Example

Consider the initiating event of heat transport circuit piping failure in Point Lepreau, identified as a loss of coolant (LOCA). We will here consider only a large LOCA - the small LOCA requires very different considerations because of its much longer duration. The safety objective is to reach a stable, shutdown condition with the fuel (which contains more than 99 percent of the radioactive materials) cooled. If possible, the fuel sheaths should remain intact. If radioactive material is released from fuel it will enter the containment space, where it will be retained if the containment systems function properly.

Only if both fuel failure and containment malfunction occur at the same time is there a potential for consequential damage to public health. Even if containment is breached in some way (the degree of failure can range from a small hole to open airlock doors), the 3000 foot zone between the plant and the nearest permanent habitation offers considerable further protection via dilution of radioactive materials.

The following event tree considers only those events that occur inside containment. It lists those systems or functions required to minimize fission product release from fuel. The simplified event tree chosen for this example is:

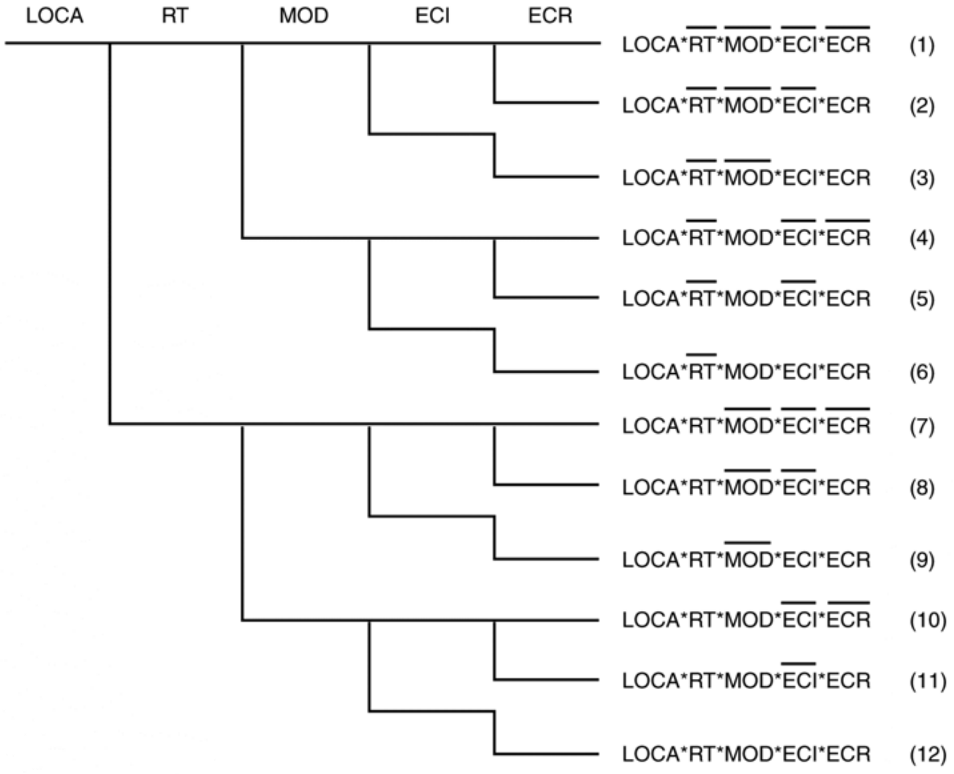
LOCA
RT
MOD
ECI
ECR
$LOCA*\overline{RT}*\overline{MOD}*\overline{ECI}*\overline{ECR}$ (1)
$LOCA*\overline{RT}*\overline{MOD}*\overline{ECI}*ECR$ (2)
$LOCA*\overline{RT}*\overline{MOD}*ECI*ECR$ (3)
$LOCA*\overline{RT}*MOD*\overline{ECI}*\overline{ECR}$ (4)
$LOCA*\overline{RT}*MOD*\overline{ECI}*ECR$ (5)
$LOCA*\overline{RT}*MOD*ECI*ECR$ (6)
$LOCA*RT*\overline{MOD}*\overline{ECI}*\overline{ECR}$ (7)
$LOCA*RT*\overline{MOD}*\overline{ECI}*ECR$ (8)
$LOCA*RT*\overline{MOD}*ECI*ECR$ (9)
$LOCA*RT*MOD*\overline{ECI}*\overline{ECR}$ (10)
$LOCA*RT*MOD*\overline{ECI}*ECR$ (11)
$LOCA*RT*MOD*ECI*ECR$ (12)

FIGURE 6.1
EVENT TREE FOR LOCA IN CANDU REACTORS

(Note that some branches have been left out, because ECR fails automatically if ECI fails.)

Event "A", such as failure of shutdown, will be designated by A. and event .not.A will be designated by $\overline{A}$. Other symbols:

LOCA -- a large loss of coolant occurs
RT -- failure of the reactor trip function
MOD -- failure of moderator to remove decay heat
ECI -- failure of the Emergency Coolant Injection function

ECR -- failure of the emergency coolant recirculation function
(recovering water from the reactor building sump)
DP -- damage occurs to the plant
$\overline{RT}$ -- not (RT) = success of the reactor trip function (&etc.)

Symbols: * - logical AND
__ - (overbar) indicates NOT failed

Consider each numbered branch in turn.

Branch 1 - In this case all the process and safety systems function as designed. One additional piece of information is required; that is, is it a large LOCA, in which some fuel sheath damage probably will occur, a small ex-core LOCA in which no sheath damage will occur, a pressure tube/calandria tube rupture which could affect the moderator system or a fuel channel end fitting failure, in which all fuel from one channel certainly will fail? In a complete event sequence diagram, the possibility of complete or partial failure of electric power systems also would be included.

Fault trees are constructed to determine the branching probability at each node. This probability might depend on the particular LOCA under consideration; for example, small LOCA is more difficult to detect under some conditions. Also, in-core LOCA might have an effect on shutdown system effectiveness if a broken calandria tube damages a neighboring channel.

Branch 2 - In this case the recovery phase of the emergency cooling function is presumed to fail. The analyst must consider the time of failure and the potential for repair. Failure of ECR immediately after the injection phase puts a demand on the moderator system to maintain channel integrity (since the fuel decay heat is still high). ECR failure a day or two after the LOCA would not be as serious because there is considerable time available for restoration of recovery flow, before the fuel begins to overheat.

Branch 3 - With emergency coolant injection and recovery presumed to fail, the heat transport system drains at a rate determined by the size of the opening in the piping. Decay heat produced in the fuel raises its temperature, along with the temperature of the surrounding pressure tubes. Pressure tubes sag or balloon (depending on the system pressure) and contact the calandria tubes. Fuel heat is conducted to the moderator water and the fuel temperature stabilizes below its melting temperature. If the moderator circulation system operates, heat is then transferred to the station heat rejection system (in Lepreau, the closed circulating water system) through the moderator heat exchangers, and eventually to seawater. If this heat flow path fails (for example, by loss of pumping power) moderator water boils and depletes, eventually leading to slow core collapse and local fuel channel failure.

Branch 4 - Moderator system fails and drains the tank. ECI and ECR operate, so there is no fuel channel failure except in a very fuel channels for specific LOCA break sizes (which are very unlikely within the class of large break LOCA). Shutdown is guaranteed due to loss of moderator and injection of light water into the core.

Branch 5 - Moderator system has failed. ECI operates, so cooling is reasonably well maintained for the first few minutes. The severity of this event depends on the time delay before failure of ECR.

Branch 6 - Because MOD, ECI and ECR are failed, there is no immediate heat flow path to remove decay heat. Fuel channels collapse to the inner boundary of the shield tank. Some fuel melting, and large fission product release to containment. Heat removal by conduction to shield tank and water pool boiling remove decay heat and stabilize the fuel rubble.

Branch 7 - Failure of reactor trip following an LOCA in CANDU is a very serious accident because of the positive coolant void reactivity. The frequency is low, however; in the range of 10-8 to 10-12 per year. (Due to this low frequency, these sequences are not required to meet AECB Siting Guide release limits). Fuel melts and produces a series of vapour explosions, destroying the core. Shutdown is achieved by moderator voiding and light water injection. Vapour explosion energy and fission products are retained by intact containment. This accident is similar to the one which occurred in Chernobyl Unit 4 on April 27, 1986. The CANDU probability is lower because, in the RBMK design, the core can void extensively without any piping break; in CANDU a pipe must break to achieve a large amount of voiding. The CANDU consequences are less severe than in RBMK because the solid moderator in the RBMK design restrains the fuel until extremely high pressures are reached in the channels -- even then, the fuel must be accelerated axially for a long distance before the reactor will reach subcritical conditions. The second reason for large consequences in the RBMK design is the absence of a strong containment structure.

Branch 8 - Very similar to Branch 7, except that long-term heat removal from the fuel may be impaired.

Branch 9 - Lack of emergency injection in this case relative to Branch 7 leads to further questions regarding fuel cooling in the period immediately following shutdown.

Branch 10 - This is similar to Branch 7, but possibly less severe if moderator draining shuts off the reactor earlier. (In fact it is difficult to follow branch 6 without consequent loss of moderator tank integrity.)

Branch 11 - Similar to Branch 8.

Branch 12 - Similar to Branch 7, but re-criticality may be possible during core collapse if there is still moderator water present. In all of the last three cases, if the shield tank is overheated the core will collapse through it and reach the reactor vault floor. It is here that the water lost from the heat transport system, shield tank, containment sprays, emergency injection, etc. is collected. This large heat capacity quenches any hot fuel. Boiling and condensation heat transfer to the building coolers, containment walls, etcetera stabilizes the system. Recovery water coolers also remove heat if they are still working.

Summary: These are the worst possible accident sequences in CANDU reactors. Many other sequences (loss of regulation, power loss, etc.) do not release any significant fission products from the fuel until a heat transport system boundary breach occurs. These sequences therefore can be considered as precursors to the LOCA initiating event. Analysis of LOCA sequences is central to an understanding of the safety performance of the CANDU system. An introduction to LOCA analysis will be presented later in this course.

3. Boolean Reduction of Event Tree

Example: event tree for large LOCA (loss of coolant accident) shown in Figure 6.1.
Assumptions:

1. The consequence of event sequence (1) is cool fuel. The consequence DP occurs for failure sequences (2) to (8); all chains ending in DP have the same degree of damage. This is assumed only for the sake of simplicity; different DP states will exist - and this fact will influence the simplification process of the event tree.

2. If ECI (failed emergency coolant injection) then ECR (failed recirculation)

Reduction of Event Tree:
Equations:
Assumption 2: $\mathrm{ECI} * \overline{ECR} = 0$
Identity: $\mathrm{ECR} + \overline{ECR} = 1$ | $\mathrm{ECI}*\mathrm{ECR} = \mathrm{ECI}*(\mathrm{ECI}+\overline{ECR}) = \mathrm{ECI}$

Event tree: $\mathrm{DP} = \mathrm{A}+\mathrm{B}+\mathrm{C}+\mathrm{D}+\mathrm{E}+\mathrm{F}+\mathrm{G}+\mathrm{H}+\mathrm{J}+\mathrm{K}+\mathrm{L}$

Where:

$A = LOCA * \overline{RT} * \overline{MOD} * \overline{ECI} * ECR$

$B = LOCA * \overline{RT} * \overline{MOD} * ECI * ECR ------------ B = LOCA * \overline{RT} * \overline{MOD} * ECI$

$C = LOCA * \overline{RT} * MOD * \overline{ECI} * \overline{ECR}$

$D = LOCA * \overline{RT} * MOD * \overline{ECI} * ECR ------------ C + D = LOCA * \overline{RT} * MOD * \overline{ECI}$

$E = LOCA * \overline{RT} * MOD * ECI * ECR = LOCA * \overline{RT} * MOD * ECI ------$

$.......C + D + E = LOCA * \overline{RT} * MOD$

$F = LOCA * RT * \overline{MOD} * \overline{ECI} * \overline{ECR}$

$G = LOCA * RT * \overline{MOD} * \overline{ECI} * ECR ------- F + G = LOCA * RT * \overline{MOD} * \overline{ECI}$

$H = LOCA * RT * \overline{MOD} * ECI * ECR = LOCA * RT * \overline{MOD} * ECI ------$

$...........F + G + H = LOCA * RT * \overline{MOD}$

$J = LOCA * RT * MOD * \overline{ECI} * \overline{ECR}$

$K = LOCA * RT * MOD * \overline{ECI} * ECR -----------J + K = LOCA * RT * MOD * \overline{ECI}$

$L = LOCA*RT*MOD*ECI*ECR = LOCA*RT*MOD*ECI$ --- $J+K+L =$
$LOCA*RT*MOD$

$$F+G+H+J+K+L = LOCA*RT$$

Final Equation -- $DP = LOCA * \overline{RT} * \overline{MOD} * \overline{ECI} * ECR + LOCA * RT * \overline{MOD} * ECI +$
$LOCA * \overline{RT} * MOD + LOCA * RT$

Which corresponds to the (common-sense) simplified event tree:

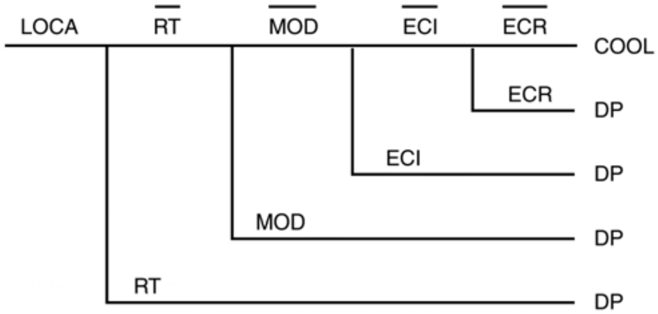

FIGURE 6.2
REDUCED LOCA EVENT TREE

It must be remembered that this simplification process applies only to the case in which the consequence DP is independent of the failure pathway.

Boolean Reduction to Minimal Irredundant Sequences (Canonical Minterms)

(a) For this we need the Boolean identity:

$A + \overline{AB}$ = A+B (not to be confused with A+AB = A)

$$
\begin{aligned}
DP &= LOCA * \overline{RT} * \overline{MOD} * \left(\overline{ECI} * ECR + ECI\right) + LOCA * \overline{RT} * MOD + LOCA * RT \\
&= LOCA * \overline{RT} * \overline{MOD} * \left(ECR + ECI\right) + LOCA * \overline{RT} * MOD + LOCA * RT \\
&= LOCA * \overline{RT} * \left\{\overline{MOD} * (ECR + ECI) + MOD\right\} + LOCA * RT \\
&= LOCA * \left[\overline{RT} * \left(ECR + ECI + MOD\right) + RT\right] \\
&= LOCA * \; [ECR + ECI + MOD + RT]
\end{aligned}
$$

(b) So, due to our Assumption 1 that all damaged states are equivalent, DP is the union of four disjoint "canonical minterms":

*(LOCA*RT, LOCA*MOD, LOCA*ECI, LOCA*ECR)*

We now need only to examine the probabilities of these four event chains.

3. Event Tree Quantification

Some additional information is required; for example, the size and location of the LOCA. For purposes of illustration, a large LOCA is assumed. Consequences should be quantified in terms of the magnitude of fuel failures expected. Fault trees defining the branch failure probabilities of the various top events are shown below. Since the branch success probabilities are near unity, this is assumed for all of them. Schematics of the systems are shown in Figures 6.4 to 6.8.

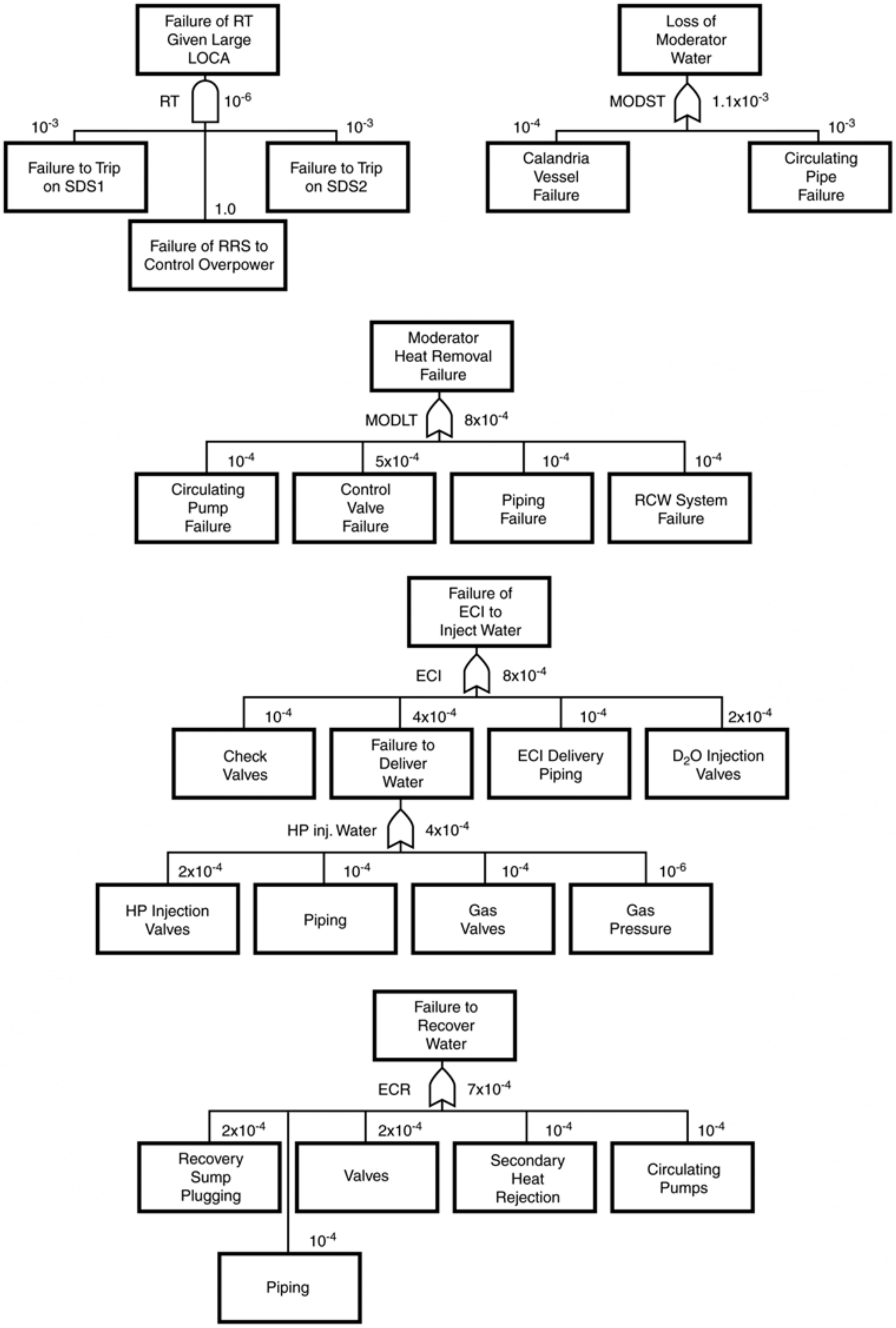

FIGURE 6.3
FAULT TREES FOR QUANTIFICATION OF LOCA EVENT TREE

PPI649 6-3

The above event probability figures are useful for illustration purposes only, but give some idea of the high reliability demanded of safety subsystems. In a real design analysis, these fault trees would be developed in much greater detail, in some cases down to the component level. Common cause analysis is carried out to determine the susceptibility of the various primary and intermediate events to failure from external conditions (e.g. common location and vulnerability to steam, fire, etc.) or to support systems such as power, instrument air, etc. Common cause failures are discussed in Sections 5-5 and 7-9 in McCormick, and in Chapter 2 of the DPSE Summary report.

Reliability calculations and measurements are carried through to the operating phase, by testing the performance of subsystems at regular intervals. The test interval required for a subsystem is determined by its reliability target and the magnitude and time dependence of its hazard rate. (Systems with repair are discussed in Chapter 7 of McCormick).

One unique aspect of the CANDU system is the licensing requirement for regular testing of special safety systems components to demonstrate that the system's unavailability does not exceed 10-^{3} a/a. This safety principle is now being considered for adoption in several other jurisdictions around the world.

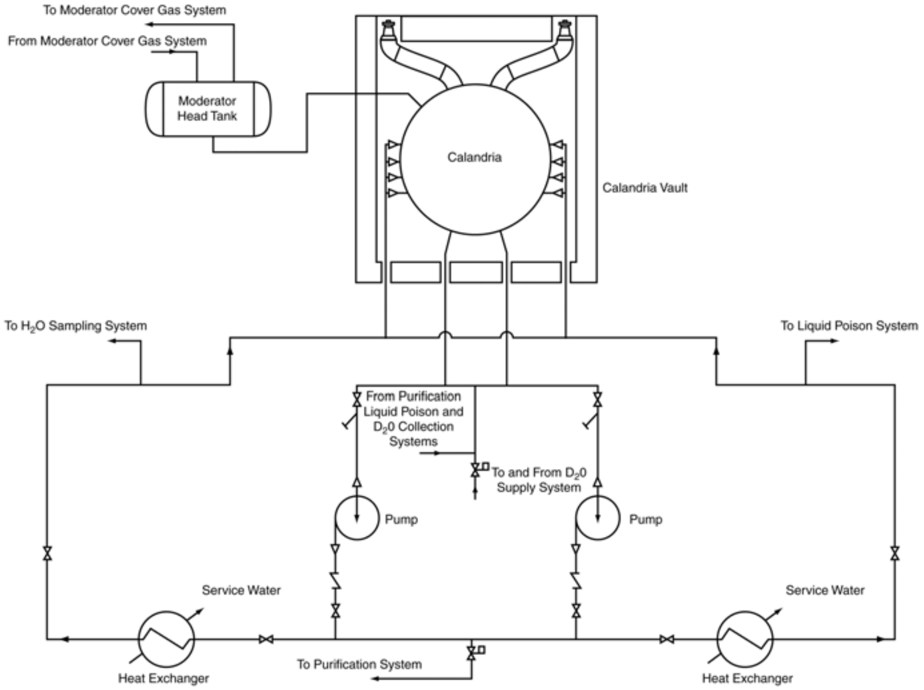
To Moderator Cover Gas System
From Moderator Cover Gas System
Moderator Head Tank
Calandria
Calandria Vault
To H_2O Sampling System
To Liquid Poison System
From Purification Liquid Poison and D_20 Collection Systems
To and From D_20 Supply System
Pump
Pump
Service Water
Service Water
Heat Exchanger
To Purification System
Heat Exchanger

FIGURE 6.4
MAIN MODERATOR SYSTEM

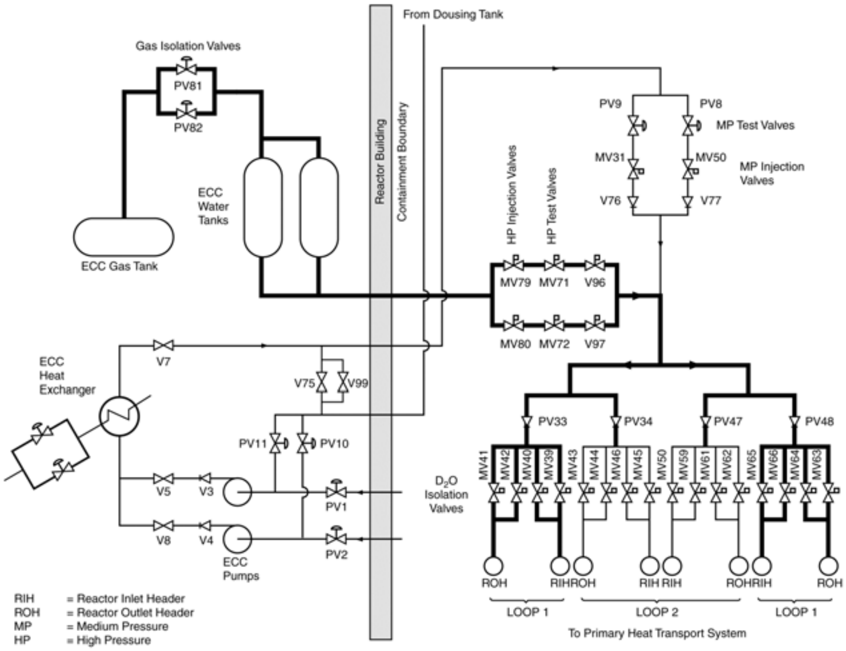

FIGURE 6.5
EMERGENCY CORE COOLING HIGH PRESSURE STAGE OPERATION; 25 TO 30 MINUTES DURATION. ASSUMED LOSS OF COOLANT IN LOOP 1

PPI649 4-3-2

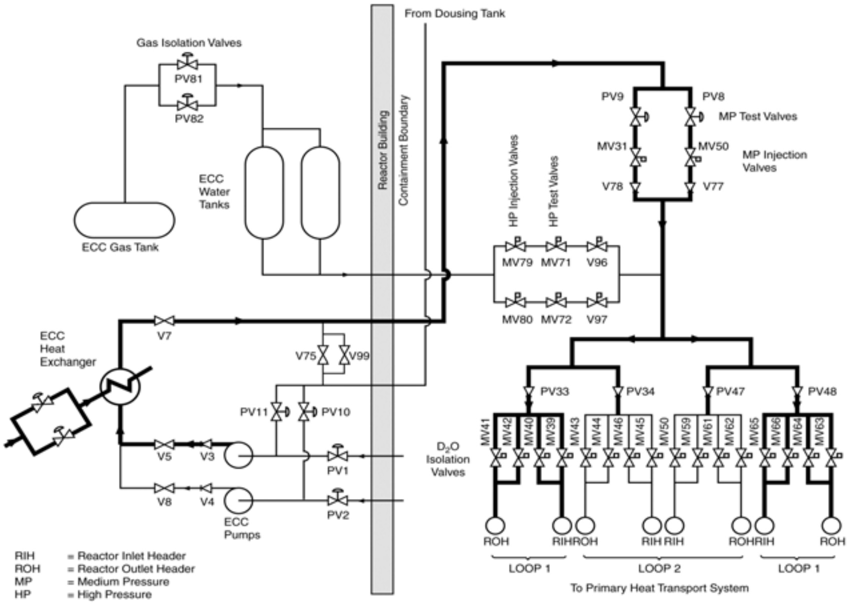

FIGURE 6.7
EMERGENCY CORE COOLING LOW PRESSURE STAGE OPERATION: INDEFINITE DURATION. ASSUMED LOSS OF COOLANT IN LOOP 1

PPI649 4-3-4

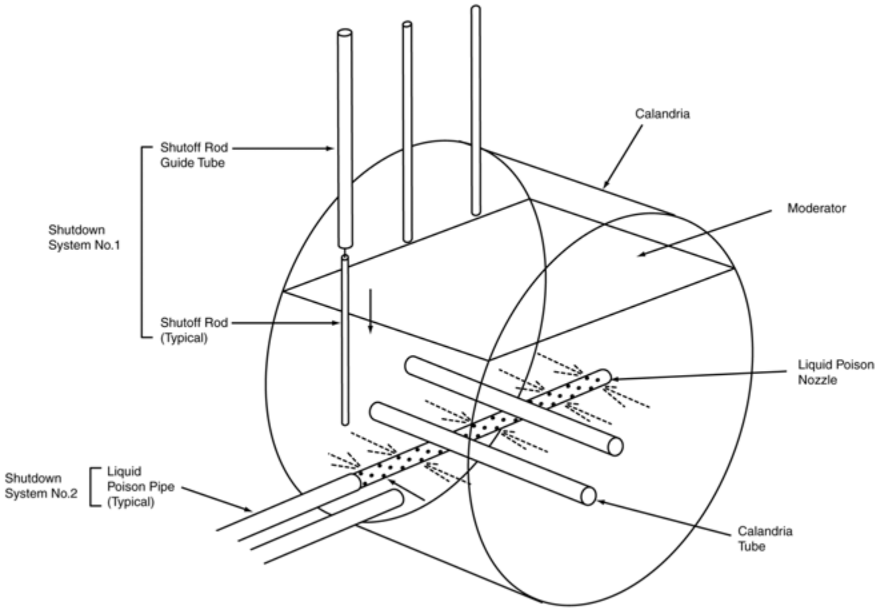

FIGURE 6.8
SHUTDOWN SYSTEM SHUTOFF RODS AND LIQUID "POISON" INJECTION

ᴾPI649 4-3-5