Chapter 7 Safety Systems

7.1 Introduction

7.1.1 Chapter Content

The chapter details functional requirements to be performed by safety systems based on a general safety function, instead of descriptive approach.

7.1.2 Learning Outcomes

The overall objectives for this chapter are as follows:

Objective 7.1	The student should be able to describe and explain the functional requirements of the safety systems and to relate the actual safety systems to these functional requirements.					
Condition	Closed book or oral written examination.					
Standard	75% on key concepts.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a				

7.1.3 The Chapter Layout

First, the safety system requirements are given from a general safety function perspective. Then for a reactor similar in design to a CANDU the safety systems which implement these safety functions are described. The event tree and fault tree methodology developed in previous chapters is then applied.

7.2 Special Safety Systems Functions

For any initiating event, the plant is designed in a way to prevent an accident from occurring or mitigating the consequences of this event. Special Safety systems are specifically designed to mitigate the consequences of a serious process failure. Process systems are designed to a different standard and are not credited. If portions of a process systems are required for some events, only that portion would be qualified. Consequently the effect of process systems will not be considered here for simplicity.

The special safety systems acting together must provide the following function:

- shutdown,
- heat removal,
- containment.

The reactor must the shutdown, and cooled. Any released radioactivity must be contained. These requirements are discussed in more detail below.

The event which determines most of the requirements for special safety systems is Large Break Loss of Cooling Accident, discussed in appendix 6. The initiating event is a break in a large pipe in the heat transport system resulting in loss of cooling to the core as the heat transport fluid ends up on the floor of the reactor building.

Figure 7.1 illustrates the safety system functions (shutdown, heat removal and containment) and the relationship of these functions to the systems that provide these functions. These systems are discussed next.

7.2.1 Shutdown

A safety system must be capable of rendering the reactor sub-critical in all operational states and accident. It must also maintain the reactor subcritical.

With the reactor at any significant fraction of full power the only system capable of cooling the core is the primary heat transport system. Alternative heat sinks are designed to remove the residual heat (decay heat and stored energy) from the fuel.

After a severe event, reactor shutdown must be ensured otherwise heat removal and containment of radioactivity are difficult to demonstrate. Events which include failure to shutdown are considered as part of severe accident analysis.

7.2.2 Heat Removal

Post accident heat removal is usually provided in 2 phases. During the Reactor Coolant Injection (RCI) phase water in injected or pumped into the core. When the water source is exhausted, the heat removal continues by pumping water from the reactor basement in the core using the Reactor Coolant Recirculation (RCR) .

Certain abnormal conditions could impair the capability to remove heat of all normal active in-plant

systems. In some reactors, natural circulation would be adequate for decay heat removal in these circumstances provided that the primary coolant boundary remains intact and some capability for heat removal is maintained on the secondary side. In other cases, for which severe core damage could possibly occur if no alternative heat removal is provided, a capability for emergency heat removal is required. This includes all residual heat removal systems, emergency core cooling systems and emergency feedwater flow to ensure heat removal on the secondary side.

Heat removal can be shown if the reactor core remains in a geometry that allows adequate fuel cooling with adequate flow and sufficiently cold water. In other words, to ensure heat removal the following three conditions must be met: 1) coolable geometry, 2) heat sink, 3) transport mechanism. It is possible to demonstrate heat removal which meet these criteria, but a substantial amount of analyses is usually required.

- **Coolable Geometry:** The core must remain in a configuration that is coolable.
-**Heat Sinks:** There are a number of systems that can transport heat from the core to the ultimate heat sink. For example ECC, Moderator, EWS ,SDC, FW. The final heat sink is usually a lake, cooling tower or a emergency reservoir.
- **Heat Transport**: Heat is transported from the core by water. Water circulation is either forced or natural convection (thermosyphoning) .

7.2.3 Containment

Containment is designed to keep releases within acceptable limits. To accomplish this the containment system must accomplish the following functions:

PAHR- Post Accident Heat Removal - heat removal to limit temperature
PARR- Post Accident Reactivity Removal (Not Applicable to CANDU)
PAPS - Post Accident Pressure Suppression - heat removal to limit pressure inside containment
ISO - Containment Isolation to isolate containment and prevent leakage above the design leakage rate typically around 0.5% volume/day.

7.3 Shutdown Systems

This and following sections give a description of safety systems for a reactor that resembles a CANDU. It also summarizes the design basis, design basis events and availability requirements for safety systems. Design basis events impose one or more requirements on system performance.

The shutdown system design addresses the following issues (for rods): speed (shutoff rod insertion speed), depth (number of shutoff rods) and reliability. Typically LOCA analysis is required to determine speed. Depth is typically determined by a secondary event that displaces reactivity poisons, such as an incore LOCA for CANDU. These issues are all determined as part of safety analysis and design procedure.

7.3.1 Shutdown System No. 1

SDS1 is the primary method of quickly shutting down the reactor when certain operating parameters indicate potentially unsafe operation. SDS1 employs 20 - 30 cadmium-loaded shutoff units (figure 7.2).

The cadmium elements drop under gravity with spring assistance. A triplicated logic system, independent from the regulating system, is used to sense the requirement for shutdown.

7.3.2 Shutdown System No. 2

SDS2 provides a second method quickly shutting down the reactor under accident conditions. This is a rapid injection of a concentrated gadolinium nitrate solution into the moderator through 6 horizontally located nozzles (figure 7.2). This makes SDS2 not only independent form SDS1 but also diverse in function and separate in physical location. SDS2 also has a triplicated logic system, independent from the regulating system and SDS1, which senses the requirements for shutdown and opens fast-acting valves under helium pressure, to inject gadolinium into the moderator.

7.3.3 Design Basis

Shutdown systems acting alone are designed to provide prompt reactor shutdown during a single process failure event, so that the radioactive dose limits to the public during this event are not exceeded.

7.3.4 Design Basis Event

To meet this requirement, SDS must deliver enough shutoff rods/poison with sufficient speed and negative reactivity depth to effect a prompt reactor shutdown. The combination of shutoff rod speed and reactivity depth is known as "shutdown system effectiveness".

7.3.5 Availability Targets

The maintenance and testing requirements of SDS1 must be carried out and be consistent with the overall SDS unavailability target of 10^{-3}.

7.4 Heat Removal Systems

Heat removal from the core after an event is provided by a number of systems. The primary system is ECC. However other heat sinks, such as Moderator, Shutdown Cooling and Emergency Feedwater, are credited in some events.

Limiting core damage by providing a heat sink limits the escape of fission products.

When using the steam generators as a heat sink, evaporation is also used.

7.4.1 Emergency Core Cooling System

The ECC system can be divided into six major subsystems as follows:

- Loop isolation
- LOCA detection and system initiation
- Steam generator crash cooldown
- High pressure injection stage

Medium pressure injection stage
Low pressure recirculation stage.

A mountain of safety analysis is required to show that an ECC system can meet the requirements.

ECC consists of three subsystems; the high pressure system, which uses gas pressure to inject water into the core from a water tank located outside the reactor building; the medium pressure system which supplies dousing tank water (located within containment) to the ECCS recovery pumps (two 100% capacity pumps); and the low pressure system, which pumps water that has collected in the reactor building sump. An emergency core cooling heat exchanger is provided to cool the recirculated ECC water. These three stages follow in series; the high pressure stage is initiated first and is followed by automatic initiation of the medium pressure stage when the accumulator water is depleted. The low pressure stage is initiated from dousing tank low level alarms. Figure 7.3 shows a schematics of the ECCS.

The main steam safety valves also form a part of the ECCS as they are required to quickly reduce the primary circuit pressure, to enhance ECCS performance. The ECCS (including crash cooldown by means of the MSSV's) is assumed when the heat transport system pressure drops to 5.5 Mpa (actual injection occurs at 4.1 Mpa). Loop isolation occurs when the same conditions are reached but different instrumentation is used.

7.4.1.1 Design Basis

The basic function of the Emergency Core Cooling (ECC) system is to provide an alternate means of cooling the reactor fuel in the event of an accident which depletes the normal coolant inventory in the heat transport (HT) system to an extent that fuel cooling is not assured. The ECC system is required to detect a loss of coolant accident (LOCA) and inject water into the HT system to refill the fuel channels and remove residual (stored) and decay heat from the fuel after a LOCA. ECC system effectiveness is measured upon its ability to limit the extent of fuel and fuel channel overheating following a loss-of-coolant accident (LOCA). ECC system effectiveness relies on the successful operation of HT loop isolation as well as the steam generator crash cooldown and certain safety support systems.

7.4.1.2 Design Basis Events

By definition, they are all LOCA events - where ECC is required to refill and maintain the primary circuit inventory. Simply, there are three main design requirements imposed by the LOCA events:

- Speed of ECC Response/Flow Requirements,
- Pressure of ECCS/Cooldown Requirements, and
- Detection of a very small LOCA.

The largest pipe breaks require the fastest ECC response and highest ECC system flows. Safety analysis is required to show that ECC response is quick enough for large breaks to meet all acceptance criteria.

Small breaks, feeder size and smaller, do not require such high flows and quick response. However, the broken loop depressurizes so slowly due to the smaller breaks, that these breaks are critical to designing the secondary circuit cooldown (crash cooldown).

7.4.1.3 Availability Targets

- The system shall be designed as far as practical to the demand unavailability target of 10^{-3}.
- The design of the ECC system and the relevant safety support systems must consider long term reliability of the components which must continue to function after a LOCA. The reliability target for long term unavailability for a three-month mission period is 10^{-2}.

7.4.2 EWS

Many systems, includung process systems, are used to provide cooling after a initiating event. EWS is a safety capable of providing cooling water supply to the steam generator and ECC systems. The system is dispersed and complicated. Herein it is discussed for its ability to provide cooling water to the steam generator.

7.4.2.1 Design Basis

The Emergency Water Supply (EWS) system ensures that there is an adequate heat sink available for decay heat removal following a loss of the normal heat removal systems. Facilities are provided for a separate water supply to the steam generators, heat transport system, and emergency core cooling (ECC) heat exchangers.

The EWS design flow from EWS pumps satisfies the flow requirements for performing the following roles:

- provide water to the secondary sides of the steam generators on total loss of feedwater,
- provide water to the secondary side of the ECC heat exchanger on loss of recirculated cooling water (RCW) following a site design earthquake (SDE) 24 hours after a LOCA.

7.4.2.2 Design Basis Events

The accident modes that could lead to the loss of normal heat removal systems are loss of feedwater, loss of service water and loss of Class III and Class IV power as well as common mode failures such as earthquakes or fires.

7.4.2.3 Availability Targets

The reliability target is 10^{-2}.

7.5 Containment

Containment contains a number of sub-systems: dousing systems, containment isolation, local air cooling system (LACS)??. The dousing system provides pressure suppression (PAPS) after a LOCA. Local air coolers provide long term containment heat removal (PAHR). Containment isolation closes those lines penetrating the containment structure that are open to the containment atmosphere or connected to the HTS (ISO).

The containment system is an envelope around the nuclear components of the heat transport system designed to prevent significant amounts of radioactivity from being released to the environment. The containment system consists of the basic containment structure with an epoxy liner on the inner surface, a dousing system, air coolers and an isolation system (figure 7.4). Containment isolation is triggered when the containment pressure rises to 3.5 kPa (g) or on a radiation signal.

Even for small breaks in the HTS, the building air coolers condense the steam released to containment. Because there is no fuel damage for such breaks, containment isolation is not required.

7.5.1 Post Accident Pressure Suppression

For larger HTS breaks, the air coolers do not prevent building pressure from rising and the dousing system is automatically initiated on a pressure signal (14 kPa(g)). Dousing reduces the overpressure and shuts off automatically as the pressure falls to 7 kPa(g). Cyclic operation of the dousing system continues until there is no further rise of containment pressure above the "dousing-on" setpoint (figure 7.5) or the dousing water is exhausted.

7.5.2 Containment Isolation

The design leakage rate for the CANDU containment system is 0.1% of building volume per day (at design pressure). For analysis purposes a value of 0.5%/day is used.

7.5.3 Containment Design Bases, Design Bases Events

Containment is a complex system consisting of many subsystems. Consequently, this system is not described in detail.

7.5.4 Availability

The reliability target is 10^{-3}.

7.6 Event Tree

7.6.1 Entries and States of an Event Tree

An event tree begins with a defined initiating event. Different initiating events will produce different event trees and the different initiating events must be catalogued and enumerated to obtain a defined set of accidents.

Once initiating events are defined, the safety systems must be incorporated into the event tree structure. For a particular defined initiating event, all safety systems that can be used are identified. Since a reactor has only a small number of safety systems, their identification are straight forward. The safety systems identified are entered into the column headings for the event trees.

Once the systems for a given initiating event have been identified, the set of possible failure and success

states for each systems is defined and enumerated. Careful effort is required in defining the success and failure states for the systems involved in the event tree to ensure that potential failure states are not included in the success definitions. If dichotomous (two-state) modeling is employed, then one failed state and one success state us defined for each system; otherwise a finite number of discrete states and others are defined (such as would be used when including partial failures).

7.6.2 Event Tree Branching Logic

Tree branching simply involves connecting the states of one system to a particular state of another system. The branching is shown in figure 7.6 for the LOCA initiating event and involves three safety systems. In this example the initiating event is depicted by the initial horizontal line and the system states are connected in a stepwise, branching fashion; system success and failure have been denoted by S and F, respectively. The format illustrated follows the standard tree structure characteristic of decision tree methodology. The accident sequence that results from the tree structure is shown in the last column of Figure 7.6. Each branch of the tree yields on particular accident sequence.

7.6.3 Conditional Interpretation of an Event Tree

Using conditional interpretation, the event tree has great power to reduce the number of accident conditions considered. For example, if the failure to shutdown the reactor (system 1) caused ECCS (system 2) and Contain. (system 3) to fail, or caused ECCS (system 2) and Contain. (system 3) to be ineffective, then there are no choices or alternatives for ECCS (system 2) and Contain. (system 3) on the lower branch of the tree, and this lower branch would simply be a straight, horizontal line containing only the failure of shutdown (system 1). Instead of considering the accident sequences IF1F2F3, IF1F2S3, IF1S2F3, IF1S2S3 we thus consider only the sequence IF1.

The identification of the conditional dependencies by the event tree methodology is important because not only is the number of accident sequences logically reduced, but also system interdependencies are thereby incorporated and therefore need not be treated in later analyses. Whenever success or failure choices are not permitted for a system, the failure probability of that system being set equal to unity because of previous events. (In the previous example of removing the S2 alternatives, the probabilities of the event sequences IF1F2F3, IF1F2S3, IF1S2F3, IF1S2S3 are not computed, but instead only the event sequence, IF1, is computed.)

When the system states are detailed for their final definitions, then sufficient information exists to define the set of physical processes that will occur with each accident sequence. For example, for each accident sequence the study computed the magnitude of radioactivity release, which then serves as a source term for the dose and risk calculations. In order to compute radioactivity releases, it as necessary to incorporate the possible modes of containment failure in the event trees. This involves defining tree headings that covered the possible failures that could occur. The failure mode event tree is then combined with the system event trees to form accident sequences leading from initiating event to the release of radioactivity from containment.

7.7 Fault Trees

When the result associated with each accident sequence have been defined, the final task is to compute the probability of system failure. This is the place at which the fault trees enter. Generally, data on failures at the system level do not exist and therefore the system failure probabilities are computed from component failures, which are available. Thus the system state definitions from the event tree can be used as defined "top events" of fault tree that are developed down to the component level.

A fault tree is constructed for each defined system failure in the event trees. Because of the conditional definition of system failures, the fault trees incorporated the conditionalities into the fault definitions and logic constructions. The quantitative system probabilities associated with the fault tree top event are system unavailabilities and system failure probability.

7.8 Exercises

1. Using figure 1 as a guide, give the functional requirements of the safety systems and explain the relationships to the actual safety systems to these functional requirements.

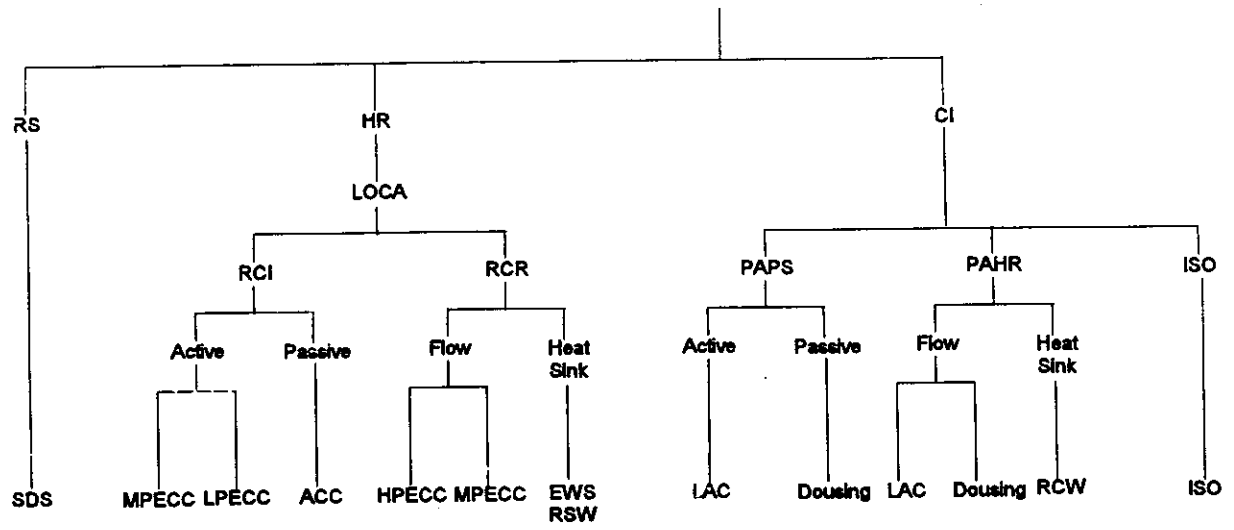

Figure 7.1 Reactor Safety Function and Protective System

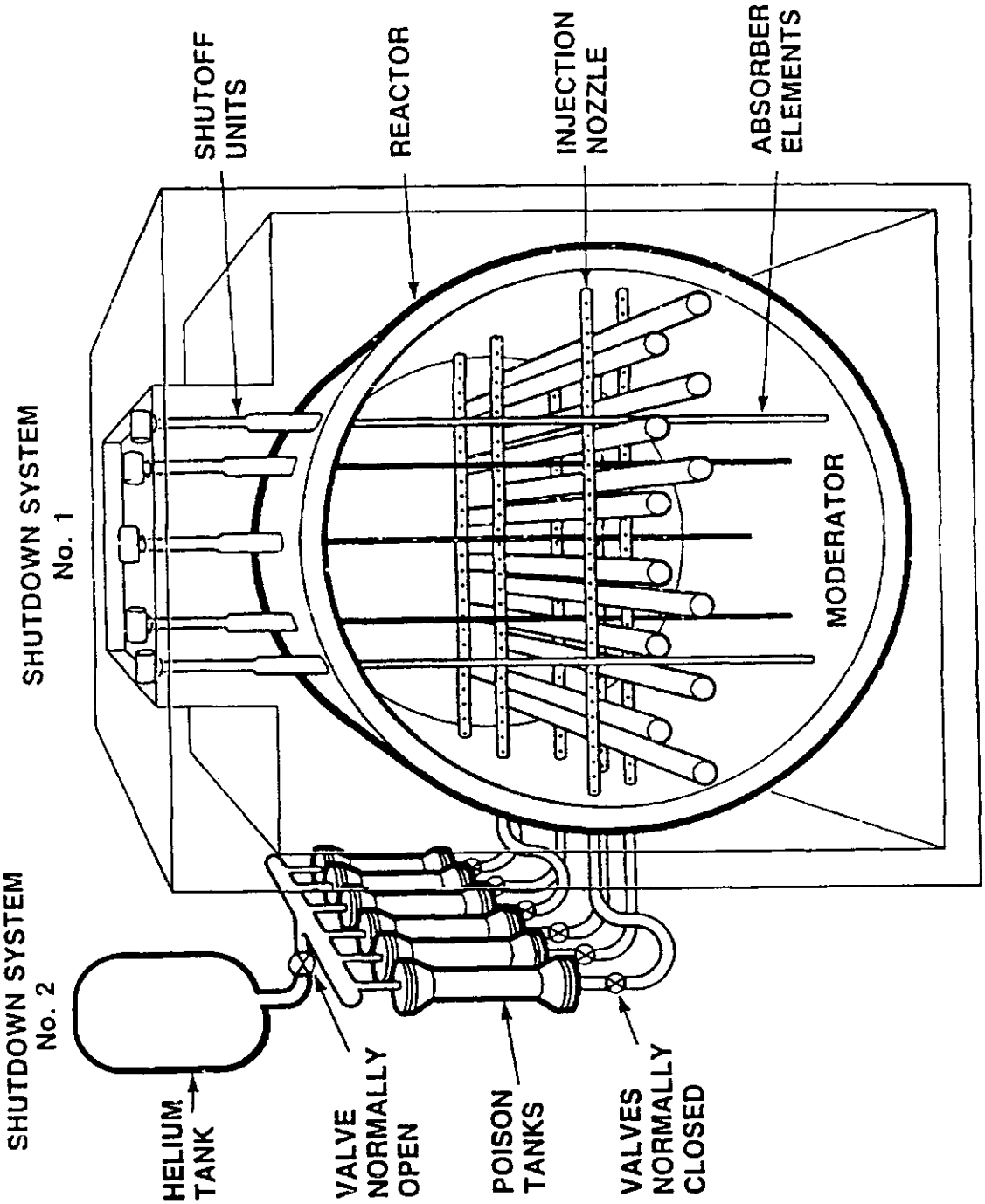

Figure 7.2 Special shutdown systems [NAT85b, figure 19]

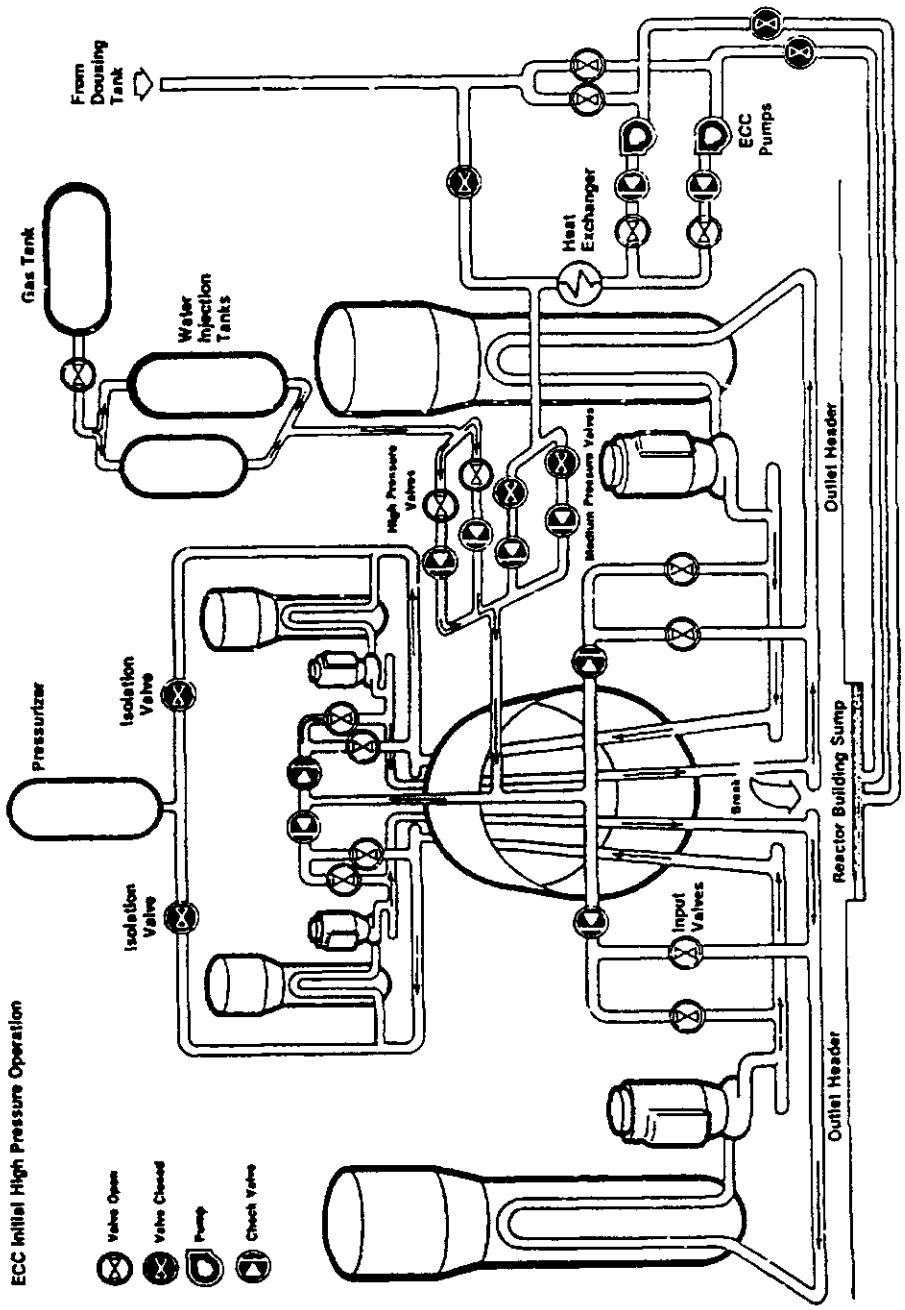

Figure 7.3 Emergency Core Cooling System [NAT85b, figure 20]

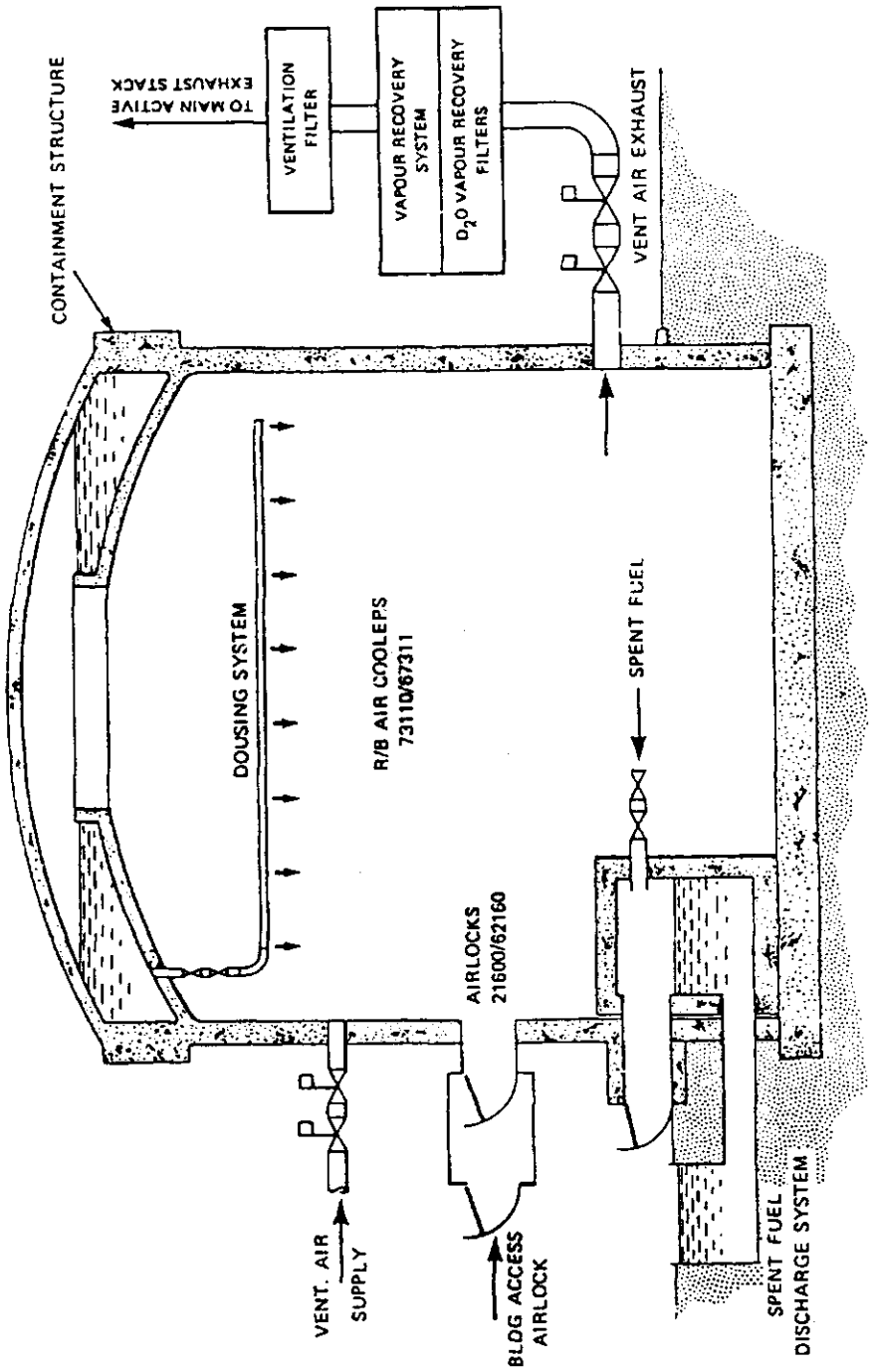

Figure 7.4 Simplified diagram of containment envelope [NAT85b, figure 21]

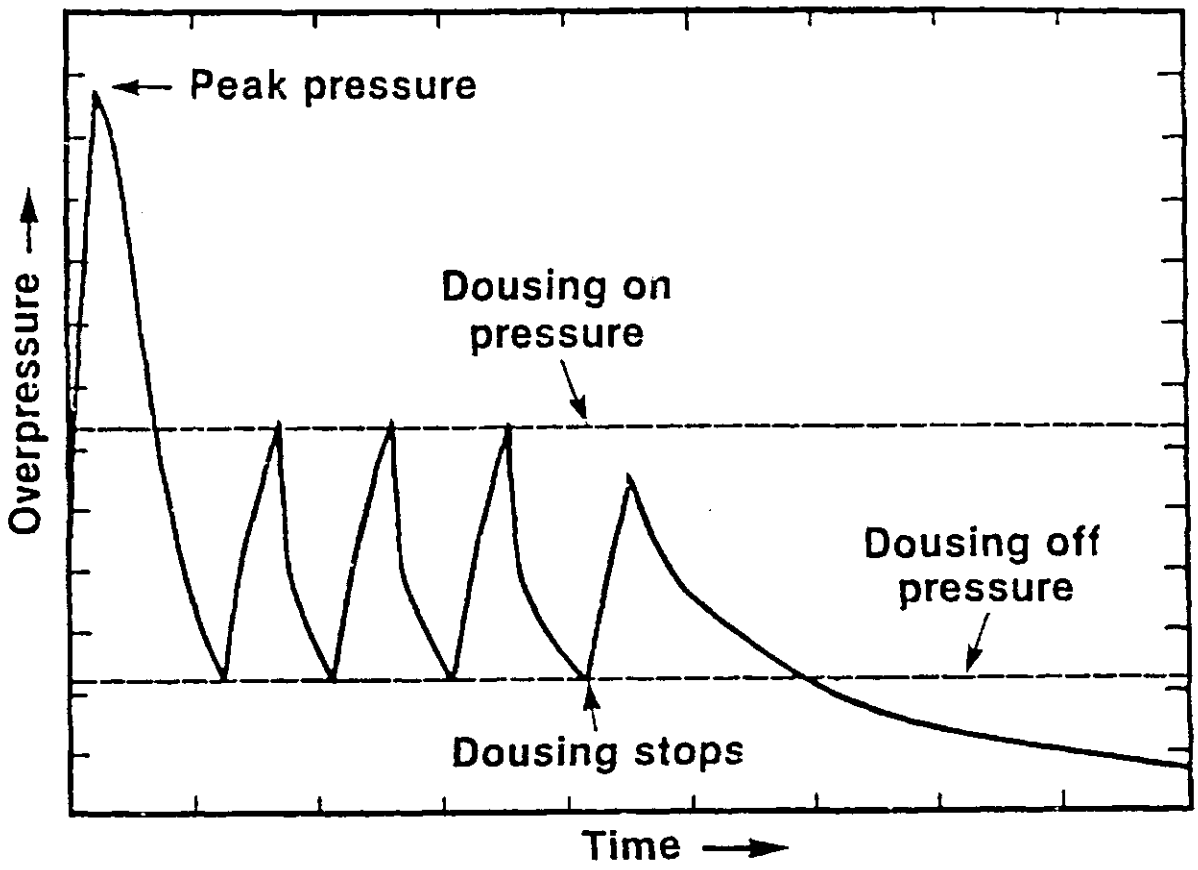

Figure 7.5 Cyclic dousing operation in single unit containment [NAT85b, figure 19]