Chapter 4 Design Basis Accidents

4.1 Introduction

4.1.1 Chapter Content

This chapter presents a methodology for generating design basis accidents and provides a example.

For the purposes of this course, the delineation of each and every event to consider is secondary to the need to present a methodology to follow.

Consequently, the events identified here are illustrative and by no means complete.

4.1.2 Learning Outcomes

The overall objectives for this chapter are as follows:

Objective 4.1	The student should be able to identify the typical design basis events for various reactor types.					
Condition	Workshop based project.					
Standard	100% on main event categories.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a	a			

Objective 4.2	The student should be able to classify DBEs according to their relationship the the safety goals.					
Condition	Workshop based project.					
Standard	100% on main event categories.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a	a			

4.2 Accident Event Identification

There is no unique methodology to follow which will lead to the identification of all the possible events that are worthy of consideration from a safety point of view.

A systematic approach, however, is more likely that not to generate the most complete and applicable list.

Generally, events are pursued in a piece-wise refinement fashion, so typical of the engineering approach.

General categories are logically identified and are then progressively refined until specific events are reached.

The general categories used to group the events are less important than the systematic nature of the process.

Following the Darlington Safety Report, for instance, we identify the root category as the release of radionuclides.

This could occur due to releases from the reactor core or from other on-site sources like fuel storage and waste handling.

The core releases are the ones of interest here. Fission product and tritium releases are identified as the two main sources of core releases, the fission product releases being the larger of the two concerns. Fission products from the fuel can only be released if the fuel cladding is breached.

This can be caused by mechanical damage or by thermal damage.

Overheating can be caused by a loss of heat sink, a loss of coolant medium, flow impairment or a loss of reactor regulation. And so on.

Figure 4.1 illustrates the event generation sequence graphically.

It should be noted that although the tritium branch is not developed herein, moderator tritium can lead to significant releases and can pose a larger hazard than even the primary coolant accidents.

The events at the right side of Figure 4.1 represent the Design Basis Accidents that form the events to be considered in a PSA.

One could, then, analyze each DBA, such as a steam generator tube rupture, and determine its probability and (if necessary) its consequence.

Design changes might be necessary to keep the releases within the prescribed frequency, release and dose limits.

In actual practice, however, the nuclear designers and regulators have "been around the loop" often enough to be able to anticipate in most cases what safety systems and features are desirable or necessary.

Good engineering practice (such as defence in depth, redundancy, testability, group separation, etc) dictate design criteria irrespective of the detailed outcomes of PSA.

The regulatory documents, then, tend to be more prescriptive and deterministic in nature.

4.3 Design Considerations

[NAT85] states that accident analysis is

> "based on the concept that, in the event of an accident, a safety system either works or it does not".

Safety systems such as ECC and containment are divided into sub-systems which, for analysis purposes, can fail independently.

In this sense, partial safety system operation is permitted. However, within the sub-systems, no credit is given for partial functioning of that safety sub-system.

Further:

"Because there are two special shutdown systems, in addition to the normal regulating system shutdown, failure to shutdown the reactor would constitute a triple failure. Special safety systems are designed and tested during operation to demonstrate a demand availability of better than 999 times out of 1000. Hence a triple failure would imply a frequency of less than 10^{-7} events per year. Events of such low frequencies are not considered in the accident analysis. For this reason, analysis for anticipated transients without scram (ATWS) is not required in Canada.

As the containment and emergency core cooling (ECC) systems contain subsystems, it is necessary to consider the unavailability of each of the subsystems in turn. The containment subsystems are dousing and isolation. The ECC subsystems are loop isolation (normally open valve closes to isolate broken loop from intact loop on a loss-of-coolant signal), injection and steam generator cooldown.

Initiating events (process system failures) are thus analyzed with and without the availability of containment and ECC subsystems."

4.4 C6

C-6 identifies 5 event classes (with dose limits as already discussed in Chapter 3):

Class 1: Examples include failure of control, failure of normal electrical power, loss of feedwater flow, loss of service water flow, loss of instrument air, and a number of other significant but not catastrophic events.

Class 2: Examples include feeder failures, pressure tube failures, flow blockages, pump seal failures, and other events that involve mechanical failures that are significant but are somewhat localized in extent.

Class 3: Examples include major LOCA, earthquakes and other events that are global and severe in nature.

Class 4: Examples include Loss of ECC, failure of rapid cooldown of the steam generators, degraded containment performance and other events associated with the loss or impairment of primary and secondary heat sinks and containment.

Class 5: Examples include feeder failures plus flow blockages plus loss of ECC and other multiple failure events such as the traditional dual failures and those associated with Design Basis Earthquakes (DBE).

C-6 and other key AECB documents are supplied as ancillary material.

CANDU 9, a next generation reactor, is being designed to C-6.

4.5 Deterministic Failure Events

Tables 2-5 from TIN90 (see appendix 2) are a convenient summary of Category A (deterministic) events that are deemed necessary to analyze.

There are various renditions of these events, developed over the years.

For instance, Table 1 of [NAT85], included here as appendix 5, gives the single and dual mode failure events that are considered for CANDU reactors.

[LBD94] contains a similar set. All are based on the 5 main ways for a radioactive release from the core to be initiated:

1. Loss of primary coolant inventory
2. Loss of primary coolant flow
3. Loss of reactor power control (in a positive sense)
4. Loss of heat sink
5. Common cause events (both external and internal).

System design details influence the event selection, as illustrated in Section 4.3, and the event sequences.

4.6 Beyond DBA

In addition to the prescribed events that must meet the dose criteria, typically the nuclear design organizations volunteer to analyze certain severe events that are beyond the DBAs.

The PSAs pick up accidents beyond DBAs (severe core damage) and these are analyzed on an ongoing basis.

The AECB judges the acceptability of these events case-by-case.

Systematic Plant Reviews are also conducted with an emphasis on system interaction and with a goal more related to overall plant safety and performance. Because the scope is broader, the coverage of events in any particular area is not as exhaustive.

4.7 Exercises

1. Generate a chart of design basis accidents for a small research reactor such as MNR.

2. Assign an event class (as per C-6) to each of the DBAs identified in question 1.

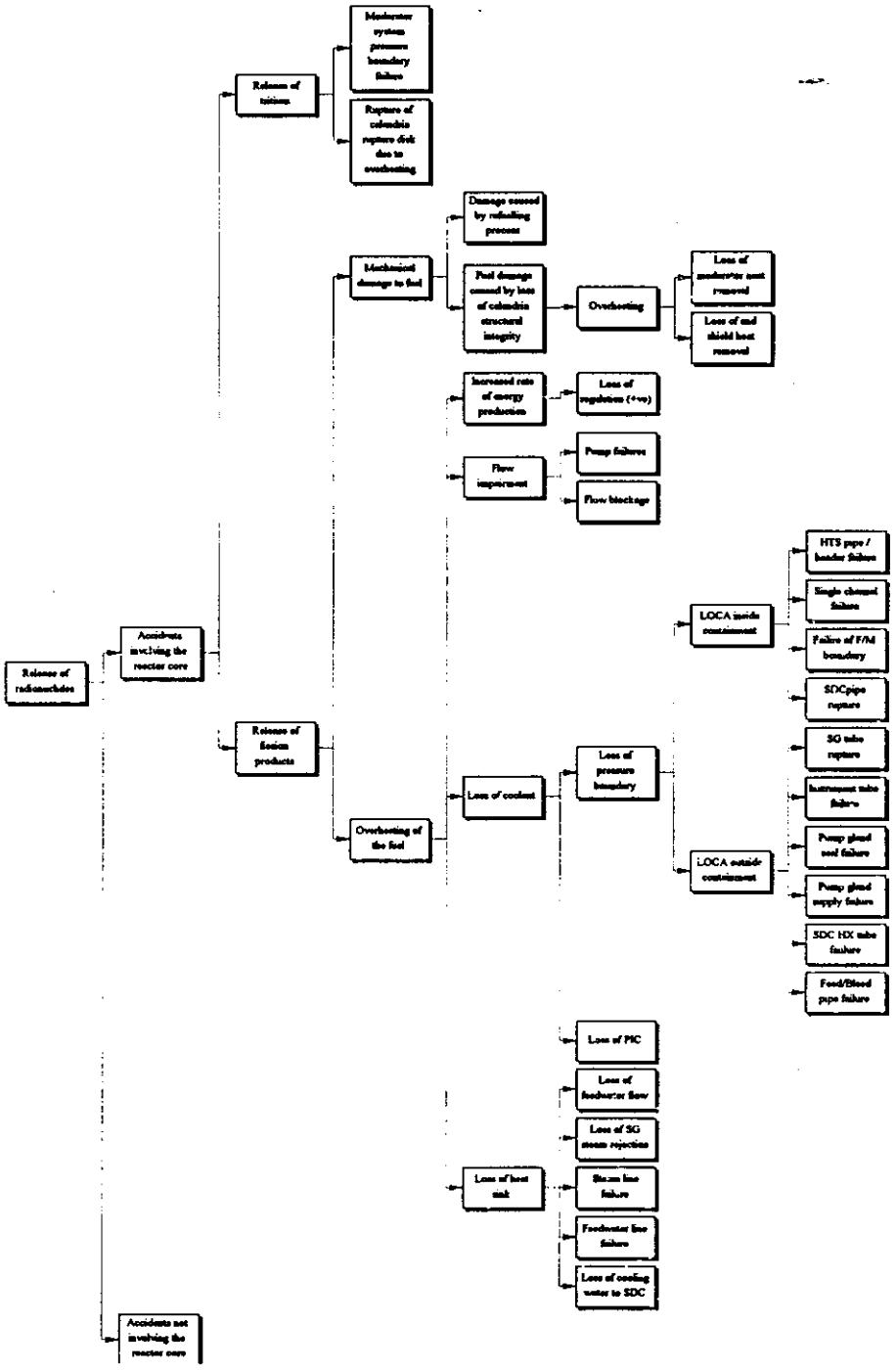

Figure 4.1 Accident Event Generation