# Chapter 7 - Accident Analysis

## Introduction

This Chapter provides more specific information on performing accident analysis for CANDU. The process by which initiating events are selected is first discussed - some of this will review what we covered in Chapter 1. The various initiating events fall into a rather small number of groups in terms of phenomena, and these are described. Next an example is given of high-level physical acceptance criteria used in the most recent CANDUs. The technical capabilities that computer codes used in CANDU safety analysis should possess is then described. Analysis of individual "design basis" initiating events is then reviewed, on an event-by-event basis. The list follows the format of a CANDU Safety Analysis Report, which is felt to be convenient to the reader but does lead to some repetition between subsections. Next, Severe Accident phenomena and analysis are summarized, followed by a discussion on uncertainty analysis.

The accident-specific sections of this Chapter form more of a reference list than a narrative - the reader wishing to understand just the concepts is recommended to read up to and including the large LOCA section only.

The objective for this Chapter is that the reader should have a good understanding of how assumptions and data are chosen in accident analysis, and in particular how one goes about establishing that the answer is pessimistic - in other words, what 'conservative' means and how it is achieved. The choice of appropriate assumptions can be somewhat subtle; the Chapter elucidates typical traps where what *seems* to be conservative is not necessarily so.

Although focussed on CANDU, the methodology and 'mind-set' is common to accident analysis of all reactor types. As with many of the topics in this lecture series, a good safety analyst must be failure-oriented - his/her bywords being "Think negatively!".

The reader wishing more detail on accident phenomena is referred to the CANDU Safety Reports, which are available for public inspection in the offices of the Canadian Nuclear Safety Commission, and usually at each utility.

We have covered the methodology of selection of initiating events fairly thoroughly in Chapter 1. These methods covered selection by event frequency (bottom up / top down approaches). However in describing the characteristics of an accident, grouping by event phenomena is more useful. We now describe both approaches.

## Selection of Initiating Events by Pseudo-Frequency

We briefly review material covered in Chapter 1:

CANDUs that were licensed up to the Darlington station used the "single-dual" failure philosophy, sometimes referred to as the "siting guide"[1]. Safety analysis would be performed for the failure of each process system in the plant; then would be performed for each such failure combined with the unavailability or impairment of each special safety system in turn (shutdown system 1, shutdown system 2, containment, emergency core cooling). In general any mitigating process system action (e.g. stepback, auxiliary boiler feedwater pump) could not be credited in demonstrating the effectiveness of the special safety systems, with the exception that continuously-running systems, which did not have to change state, could be assumed to continue working (e.g. moderator, steam generators). This approach was comprehensive but required supplementary techniques to cover all accidents. Failures in the safety support systems (such as instrument air) were addressed using early probabilistic techniques (Safety Design Matrices), and later in the Probabilistic Safety Assessment (PSA). The requirements for safety analysis were further generalized in CNSC Consultative document C-6[2], used on a trial basis in the licensing of Darlington. This document lists a large number of potential initiating events and event combinations sorted into five Event Classes (roughly grouped according to event frequency), and requires analysis of each one. Furthermore, the designer is required to perform a systematic evaluation of the plant to show that no significant initiating events or event combinations have been missed. Consultative document C-6 has been superseded for new build by the CNSC document RD-337[3], issued in November 2008; it reflects international requirements in that it is based on the IAEA report NS-R-1[4]. RD-337 is expected to change the approach described below fairly substantially, particularly in the introduction of Anticipated Operational Occurrences, and the greater emphasis on severe accidents, but in this Chapter we describe how the safety analysis has been done for the majority of operating CANDUs. Appendix A lists the classification scheme from RD-337.

A number of techniques are used in the systematic evaluation. Lists of initiating events can be compiled by writing down all the plant systems and assuming the failure of each system in turn; the most systematic method to identify such failures (and failure combinations) is the Probabilistic Safety Assessment (so-called "bottom-up method"). Another method is to determine all sources of radioactivity in the plant and postulate failures which would cause them to be relocated ("top-down method").

Two other types of events need to be considered: external events and very rare events.

External events include tornadoes, earthquakes, tsunami, temperature extremes, fire, explosions, hostile attack, aircraft crash, etc. Generally these are addressed in the design by hardening or

separating essential systems, or by choice of siting, so that safety analysis is not normally required. Some accidents are combined with external events on the basis of probability. For example a Loss of Coolant Accident is assumed to be followed 24 hours later by a Site Design Earthquake[a]. While in principle this event combination could be subject to safety analysis (assuming various combinations of system failures, and deriving associated probabilities and consequences), in practice it is addressed by seismically qualifying the appropriate portions of the plant so that the systems required to maintain the plant safe after a LOCA do not fail in a Site Design Earthquake.

Very rare events include failure of pressure vessels (e.g., pressurizer, steam generator shell), failure of structural supports, turbine breakup etc. Pressure vessel and structural failures are precluded[b] in the design by use of the appropriate level of design and manufacturing codes and standards, quality assurance, in-service inspection, etc. Again safety analysis is not required. Turbine missiles are usually dealt with on the basis of proving a low probability that a missile from turbine disintegration could damage safety-critical components or penetrate containment. Recent designs such as ACR-1000 orient the turbine radially to the reactor building rather than tangentially, to make a stronger safety case for limiting damage from turbine missiles.

Finally CANDU practice requires consideration of common cause events. These are identified either by the systematic plant review or the PSA. The analysis thereof is usually reported as part of the PSA.

## Categorization of Initiating Events by Phenomena

The previous section discussed categorization of initiating events by frequency of occurrence. Once selected, initiating events can also be grouped in terms of the major phenomena, as follows (grouped by *primary* or *direct* cause):

1. **Reactivity Accidents**
   - Bulk Loss of Reactivity Control
   - Loss of Reactivity Control from Distorted Flux Shapes

---

[a] Site Design Earthquake (SDE) is an earthquake with a return frequency of 1 per 100 years, hence of lower intensity and higher frequency than the Design Basis Earthquake or DBE, which is expected to have a return frequency at least an order of magnitude less..

[b] This is an assumption, not a fact: it really means that if all the engineering requirements listed are followed, the probability of the failure is very low and there need not be systems designed specifically to mitigate it. How did the event at Davis Besse challenge this assumption?

2. **Decrease of Reactor Coolant Flow**
    - Loss of Class IV Power
    - Partial Loss of Class IV Power
    - Single Pump Trip or Single Pump Seizure

3. **Increase of Reactor Coolant Pressure**
    - Loss of Primary Pressure and Inventory Control (increase)

4. **Decrease of Reactor Coolant Inventory**
    - Large Heat Transport System LOCA
    - Small Heat Transport System LOCA
        - Single Channel Events
        - Single Steam Generator Tube Rupture
        - Multiple Steam Generator Tube Rupture
    - Loss of Primary Pressure and Inventory Control (decrease)

5. **Increase of Secondary Side Pressure**
    - Loss of Secondary Side Pressure Control (increase)

6. **Loss of Secondary Side Heat Removal**
    - Main Steam Line Break
    - Feedwater Line Break
    - Loss of Feedwater Pumps
    - Spurious Closure of Feedwater Valves
    - Loss of Secondary Side Pressure Control (decrease)
    - Loss of Shutdown Heat Sink

7. **Moderator & Shield Cooling System Failures**
    - Pipe Break
    - Loss of Forced Circulation
    - Loss of Heat Removal

8. **Fuel Handling Accidents**
    - Fuelling Machine On-Reactor
    - Fuelling Machine Off-Reactor

*Severe core damage accidents* involving an initiating event and failure of at least two mitigating systems fall into a separate category, since the phenomena of severe core damage are not strongly coupled to the initiating event.

## High-Level Acceptance Criteria

Once the events are identified, they must be put into the appropriate Event Class and compared to the dose acceptance criteria for that Event Class. There are two Event Classes in the siting guide (single failures and dual failures), five in CNSC document C-6, and three in RD-337 (Appendix A). Whatever the licensing basis of the plant, the safety analysis must show that the resulting dose to the public meets the dose limit for its Event Class (Figure 7-1 as an example, using C-6). In addition, for new plants, the safety goals in RD-337 must also be shown to be met - see Chapter 6.

The approach for CANDU has been to use "best-estimate" physical models combined with conservative[c] values of the key input parameters to give a conservative, but physically reasonable, prediction of accidents. This is different from LWR practice, in which conservative models *and* assumptions are prescribed. The LWR practice *seems* to be 'safer' but has three disadvantages:

- If models and assumptions are all prescribed by the regulator, the designer feels less obligation to ask tough questions as to whether the model is correct or not.
- A model which is 'conservative' in one aspect may be non-conservative in another (e.g., a model which maximizes heat transport system pressure to get a 'conservative' estimate of its peak value in an accident also leads to an unrealistically earlier trip on high pressure. This is so obvious that two calculations are done: one to maximize pressure (to determine peak pressure) along with one to minimize pressure (to determine trip time). The two are then combined to give the 'worst of all possible worlds'. So far so good, but not all problems are so easily recognized.
- Conservative models predict unrealistic plant behaviour, so that the accident analysis is useless or misleading in training an operator to deal with a real accident; and may suggest signals which do not occur, or omit some which do.

[c] "Conservative" means an assumption, model or datum which makes the answer more pessimistic with respect to safety acceptance criteria - e.g.: increases dose; or increases fuel temperature; or increases (or decreases) pressure depending on the accident. The opposite is "optimistic". A "best-estimate" approach uses realistic models, assumptions and data.

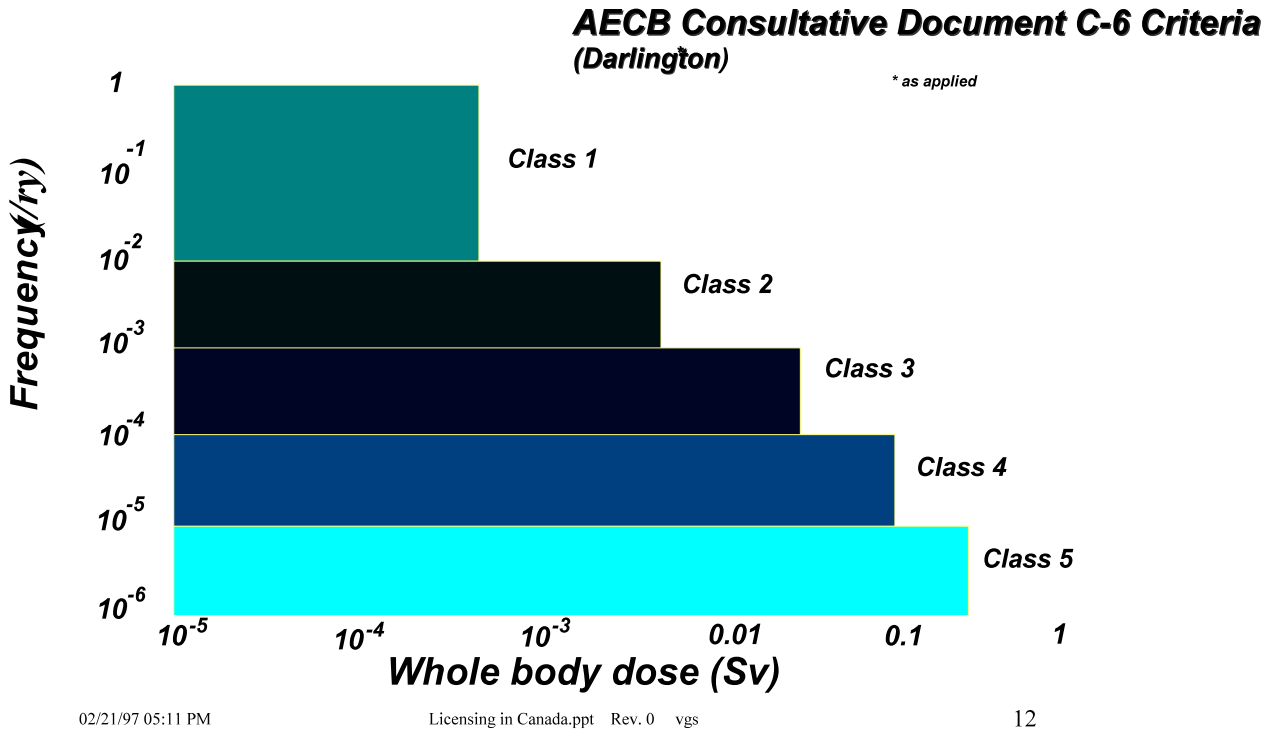


**Figure 1**

The models used start from reactor physics, through system thermohydraulics, through fuel and fuel channel response, through moderator and containment response, and to atmospheric dispersion and dose, as discussed in Chapter 8.

CANDU regulatory practice has not (for existing plants) demanded a "stylized" source term into containment nor a stylized containment pressure transient; instead the release of fission products to containment, the containment pressure transient, the resulting leakage of radionuclides from containment, the dilution by atmospheric dispersion and effects of ground deposition, and the dose to the public are all predicted using realistic physical models and conservative input data or system assumptions.

However for new plants RD-337 requires the designer to identify both a radiological and a combustible gas accident source term for use in the specification of the design features for severe accidents. This source term is based on a set of representative core damage accidents established by the designer.

Note that both the siting guide and Consultative Document C-6 include some severe accidents[d], which therefore were considered to be within the CANDU "design basis". For example, large LOCA plus Loss of ECC is a dual failure in the siting guide, and is an Event Class 5 in C-6, and the whole-body dose to the most exposed individual member of the public must be less than 0.25 Sv. This requirement can be met because the moderator arrests the damage at the channel boundary. Other severe accidents (such as LOCA + LOECC + loss of moderator cooling) are excluded from C-6 but need to be considered for new plants to show the RD-337 safety goals are met. This topic is covered in more detail later. The net result of applying the siting guide, or C-6, was that an accident class (a group of accidents with similar loss of function) with a frequency of about $10^{-6}$/year or larger becomes part of the "design basis" and in practical terms must be shown to stop short of severe core damage[e], although fuel itself may be severely damaged. Some containment designs are so powerful, however (e.g. multi-unit vacuum containment), that the dose can be kept below 0.25 Sv even for some severe core damage accidents.

In Canada, public dose is the primary acceptance criterion. The designers also define subsidiary effectiveness criteria, which are intended to be chosen as sufficient but not necessary to meet the primary acceptance criterion of dose. For example prevention of fuel failures is a subsidiary effectiveness criterion for a small LOCA. These criteria may be endorsed, or adopted, or disputed, or re-set by the regulator; some are specified in CNSC documents[f]. The subsidiary acceptance criteria defined by the designers are discussed in this Chapter under each individual accident, as they were applied to the most recent CANDU 6 plants.

Shutdown systems have a separate acceptance criterion. Modern CANDUs have two independent, redundant, separated and diverse shutdown systems[5]. Each system, on its own, must be capable of shutting the reactor down after any accident, independent of the mitigation provided by the normal reactivity control devices. Generally two diverse trip parameters have been required on each shutdown system for each accident over the range of operating conditions

---

[d] specifically defined for CANDUs as an accident where there is no heat removal by water in the fuel channels. There will be severe fuel damage (partial loss of bundle geometry) but, depending on the availability of the moderator as a backup heat sink, there may or may not be severe core damage (q.v.).

[e] defined as loss of the channel geometry in the calandria

[f] The CNSC originally had a document classification scheme consisting of "R" documents, which were high level requirements, and "C" or Consultative documents. This scheme was partially replaced by another one consisting of five levels, of which the three most important are Regulatory Policies, Standards, and Guides. The "RD" series is new, and stands for "Regulatory Document" so that the document structure is again changing. At the moment documents in all three schemes exist and apply to varying degrees.

(unless it is impracticable or detrimental to safety to provide dual parameter coverage[g]). As a result, it is not required to perform analysis of either transients or accidents without shutdown[6].

This Chapter summarizes information from the most recent safety analysis of CANDU 6s, specifically the Wolsong 2,3&4 plants in Korea and Qinshan 1&2 in China. In some areas (e.g., classification of single and multiple steam generator tube ruptures), Regulatory Document C-6 has required interpretation or modification in practice. The safety analysis technology and acceptance criteria in these latest stations, including interpretations of C-6, has been used extensively.

## Major Computer Analysis Tools Required for DBAs

Following from the philosophy described above, CANDU safety analysis requires a comprehensive suite of physical models. The mathematical foundations of these models are presented in simplified form in Chapter 8.

*Reactor physics* analysis requires a transient three-dimensional model, especially for the larger CANDU cores. The most demanding application is large LOCA, because the positive void coefficient leads to relatively fast kinetics and because of the spatial effects associated with flux tilts and shutoff rod (or liquid absorber) insertion. Three dimensional effects are also important in slow loss of reactivity control starting from distorted flux shapes.

The *system thermohydraulics* code is typically a **two-fluid, one-dimensional non-equilibrium network** code. The **two fluids** are water and steam, of course; recent codes also incorporate a third non-interacting fluid - e.g., hydrogen as produced in severe accidents. **One spatial dimension** suffices nicely for CANDU, since the system consists largely of linear flow in pipes (feeders, channels, large pipes above the core) and there are no vessels in which complex three-dimensional behaviour occurs. However the flow in the headers can be quite complex and tools, based on tests, are being developed to model it more accurately. The thermodynamic **non-equilibrium** aspect is important in modelling rewet and refill of the channels, since the flow can be stratified (steam and water flowing separately due to the effect of gravity) during that time, and each phase can have its own temperature and flow. Finally a **network** capability is clearly a necessity in CANDU, with its multiple parallel paths (many channels connected to one header, ECC connected via parallel paths to each header).

---

[g]RD-337 relaxes this requirement for new plants and requires redundant trip parameters only if the first one is not a direct measurement of the parameter of safety interest

Recent practice has been to incorporate the reactor physics calculation into the system thermohydraulics code for large LOCA, since the voiding transient determines the power pulse, which in turn has a second-order effect on the voiding transient.

*Fuel thermomechanical* models consist of a code for normal operation, which predicts the initial fuel conditions before the accident (sheath strain, fuel-to-sheath heat transfer coefficient, fission gas release, initial fuel and sheath temperatures, etc.) and a transient thermomechanical code for accidents. The latter includes sub-models for fuel failure mechanisms, due to: fuel sheath strain, beryllium braze penetration, sheath embrittlement due to oxidation, athermal strain, and excessive fuel energy content. Because of the need to predict the dose for each accident, the models must be able to estimate the percentage of fuel that fails in an accident (if any), and the release of fission products to the channel.

Under certain circumstances, such as a large LOCA combined with a loss of ECC injection, the pressure tube will overheat and (depending on the internal pressure) sag or strain into contact with the calandria tube. This requires models of the *pressure tube thermal-mechanical* transient behaviour, to predict the extent of deformation and the pressure tube temperature and internal pressure when/if it contacts the calandria tube. Separate channel thermal/mechanical models have been used to date, using very pessimistic and artificial boundary conditions (fixed 'worst' steam flowrate); now the system thermohydraulic codes incorporate channel deformation capability, allowing coupling of the more realistic prediction of the distribution of flow to each channel from the thermohydraulics portion, with the actual channel deformation due to those conditions.

The behaviour of a channel subsequent to such contact depends on the heat transfer from the calandria tube to the moderator. Further deformation will not occur if the calandria tube outer surface does not dry out, or at least does not go into widespread film boiling. This in turn depends on the local moderator subcooling. A two- or three-dimensional prediction of *moderator temperatures* (hence flows) is therefore required. Of most interest is the steady state distribution at the time of contact, although transient calculations are required for in-core breaks.

Following the release of *fission products* from the fuel, their transport through the heat transport system (HTS) to containment, and within containment, should be predicted. To date CANDU safety analysis has not used models for the transport within the HTS, and for deposition on surfaces such as end fittings and feeder piping, although this is clearly an area which could be included and has been the subject of intensive R&D over a number of years. However the partitioning of fission products between steam and water phases at the break, and within containment, has been modelled, as has long-term formation and transport of organic iodides within and from the water pool. Release of airborne radionuclides from containment can occur through the "normal" leakage paths if the containment is assumed to be intact, or through containment impairments in dual failures such as LOCAs with failure of the containment ventilation system to isolate, or LOCAs with deflated containment airlock door seals.

The *containment pressure* transient calculation uses the transient energy release from the break, and includes sub-models for dousing, containment air coolers, fission product and hydrogen transport, and natural and forced circulation, as well as models for containment impairments such as open ventilation dampers. Multi-node, multi-fluid (water, steam, air, hydrogen) one-dimensional containment models are used for this analysis. These one dimensional models treat containment as a series of uniformly mixed linked volumes and are adequate for overall pressure prediction. For predicting the hydrogen distribution in large volumes, a three dimensional model is required and such models are now being deployed.

The final step is calculation of *dose* to the public. The atmospheric dispersion model[7] typically uses a Gaussian plume model to predict exposure as a function of distance from the station; the input is the predicted transient release of radionuclides from containment for each accident. The weather assumed is traditionally the worst weather occurring more than 10% of the time at the site. Exposure-to-dose calculations use standard ICRP-recommended conversion factors.

Figure 7-2 shows the whole process as a flow-chart.

# Accident Analysis Flow Chart

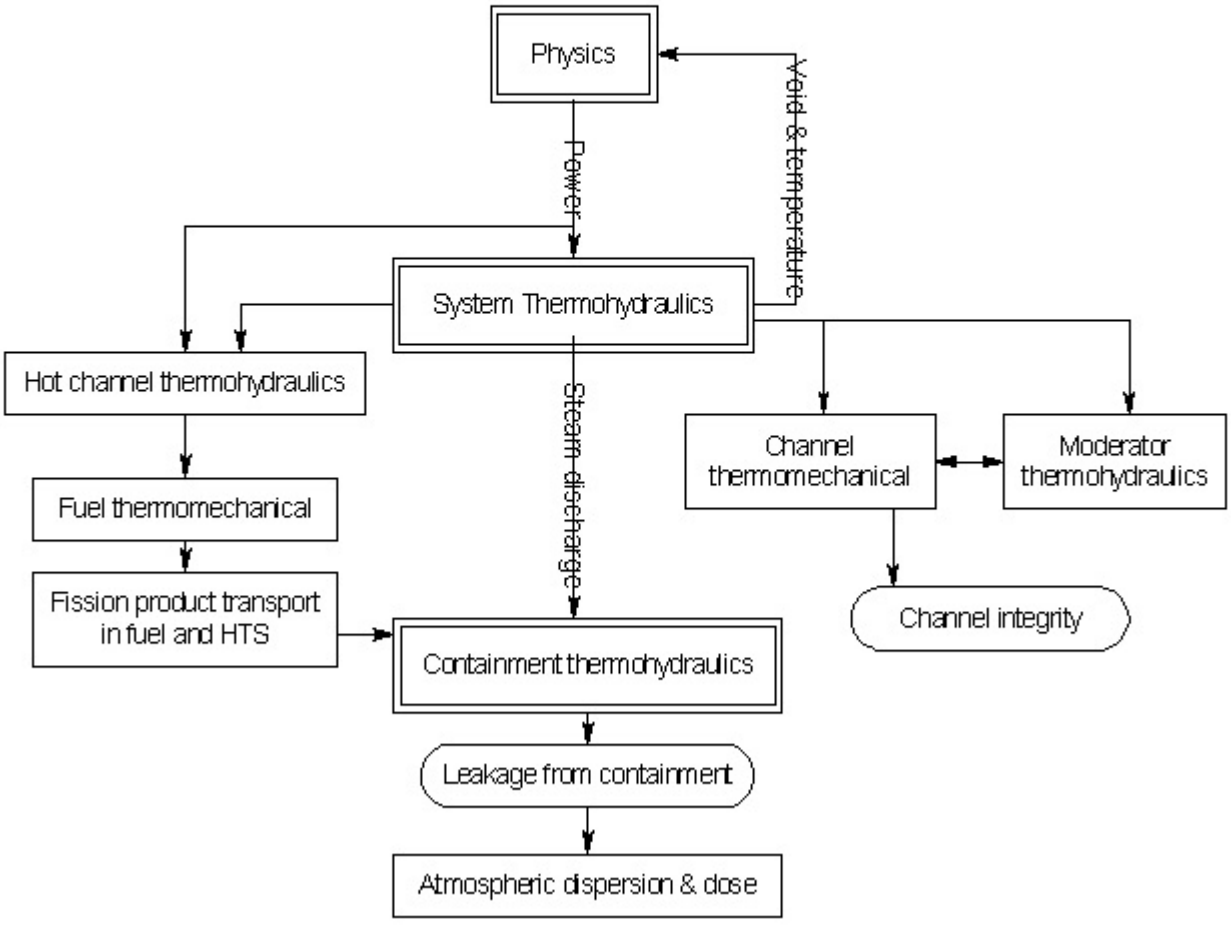


**Figure 2** - Accident Analysis Flow Chart

Selection of Initial Conditions

A number of key parameters are chosen in a "conservative" direction for licensing analysis. These include fundamental core property parameters, initial plant conditions, system performance measures, and assumptions on the unavailability of portions of mitigating systems. There is no unique conservative choice of a parameter; as noted previously, what is conservative in one application (e.g., minimizing the number of containment coolers credited, in calculating peak containment pressure) may be non-conservative in another (calculating high containment pressure trip effectiveness). In addition there is an 'art' to choosing the appropriate level of conservatism: too much conservatism may require unnecessary design changes; too little may not cover uncertainties in the models used or the station parameters. This dilemma is mostly removed by a 'best-estimate + uncertainty analysis' (BE+UA), in which all parameters are set at their best estimate values, and the uncertainties are combined and propagated through the calculation. However such a methodology is not well recognized in Canadian licensing. This section will therefore deal with 'conservative' analysis; at the end of the Chapter we summarize the BE+UA.

Since many parameters are chosen in a similar way for many accidents, the following table lists the most common choices along with a simplified rationale:

**TABLE 7-1 - KEY SAFETY ANALYSIS PARAMETERS**

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Reactor thermal power | High | Minimize time to use up cooling water inventory, minimize margins to critical heat flux, etc. |

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Reactor regulating system | Normal operation or inactive, whichever is worse; setback is generally not credited unless it tends to "blind" the trip | Choose so as to delay reactor trip |
| Radionuclide operating load in the HTS | Highest permissible operating iodine burden (and associated noble gases) plus any 'spiking'[h] at the time of reactor shutdown; and end-of-life tritium concentration | Maximize radionuclide release from station and public dose |
| Pressure tube radial creep | Highest expected over the timescale over which the safety analysis is to be valid | Reduce margin to critical heat flux (due to flow bypass around the fuel bundle in a crept tube) and increase value of void reactivity |
| Steam generators | Clean & fouled cases | Reduce reactor trip effectiveness |
| Steam generator tube leak rate | Maximum permitted during operation, plus assessment of any consequential effects due to the accident | Increase radioactivity release |

[h] The spike, or the increase in release of radionuclides from defective fuel, is sometimes seen on rapid reactor shutdown, due to the sudden changes in stress on the fuel.

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| HTS flow | Low | Reduce margins to critical heat flux |
| HTS Instrumented channel flow | High | Reduce low flow trip effectiveness |
| Coolant void reactivity coefficient | High; | Maximize overpower transient; |
| | Low | Delay HTS high pressure trip |
| Fuel loading | Equilibrium; | Maximize fuel temperatures, radioactivity releases; |
| | Fresh | Maximize overpower transient |
| Shutdown system | Backup trip on less effective shutdown system using the last of three instrumentation channels to trip | Delay shutdown system effectiveness |
| SDS2 injection nozzles | Most effective nozzle unavailable | Reduce shutdown system reactivity depth |
| SDS1 shutoff rods | Two most effective rods unavailable | Reduce shutdown system reactivity 'bite' and depth |
| Maximum channel/bundle power | High | Maximize fuel & sheath temperature |

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Reactor decay power | High | Minimize time to use up cooling water inventory |
| Initial flux tilt | High | Maximize fuel & sheath temperature |
| Moderator initial local maximum subcooling | Low | Minimize margin to critical heat flux on calandria tube |
| Number of operating containment air coolers and other heat sinks | Low; | Maximize containment pressure; |
| | High | Delay high pressure trip; and maximize likelihood of hydrogen combustion, due to rapid condensation of steam |
| Number of containment dousing spray headers | Low (typically 4 out of 6); | Maximize short-term containment pressure; |
| | High | Maximize long-term containment pressure and leak-rate, maximize likelihood of long-term hydrogen combustion |
| Containment leak rate | High (typically 2x to 10x design leak rate); | Maximize public dose; |
| | Low | Maximize containment pressure |

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Containment bypass leakage | Pre-existing steam generator tube leak | Maximize public dose |
| Weather | Least dispersive weather occurring >10% of the time | Maximize public dose |
| Operator Actions | Not credited before 15 minutes after a clear indication of the event, for actions that can be done from the control room; and not credited before 30 minutes, for actions that must be done "in the field" | Ensure adequate time for diagnosis |

Where the "conservative" assumption is particular to one type of accident, it is listed in the discussion on the individual accident below.

Note that whatever safety analysis *assumptions* are made become *limits* to operation: so for example, if the moderator subcooling is at some time during operation less than that assumed in the safety analysis, the plant is said to be in an 'unanalyzed' state and the state must be rapidly demonstrated to be acceptable (through re-analysis) - or the plant derated to the point where the subcooling is again within the range assumed in the accident analysis. This course of action is relatively straightforward on a single parameter, but can become very complex when a number of parameters deviate from their assumed conditions.

## Typical Initiating Events

This section summarizes typical initiating events for CANDUs, indicating safety issues of interest and any key safety parameters not already covered in the Table 7-1; acceptance criteria used by designers and/or required by the regulator; and relevant event combinations. Because there are a number of different CANDU designs, different organizations doing safety analysis, different computer codes and different regulatory frameworks, the specific information in this section may not apply in every case. Furthermore some issues are still under dispute with the regulatory body. There is also a practical limitation on the amount of detail that can be presented here on acceptance criteria and key safety parameters, for which the individual plant Safety Reports are the ultimate source of information. Instead the more important acceptance criteria and key safety parameters have been selected, so these lists, while typical, should by no means be considered complete.

Note that the discussion under each accident assumes the licensing rules of Darlington, Wolsong 3&4 and Qinshan 1&2 - i.e. CNSC Consultative Document C-6. The list of events, their classification, and in particular the dose acceptance criteria would be different under RD-337.

The complete listing is rather dry and is a source of reference rather than a learning tool. The reader should go thoroughly through at least one accident (large LOCA for example) to get a sense of the approach.

## 1. Large Heat Transport System LOCA

### *1.1. Initiating Event*

A large LOCA in a CANDU is conventionally defined as one where the break area is larger than twice the cross-sectional area of the largest feeder pipe. Because there are two feeder pipes connected to each channel, there is a lot of small-bore piping in CANDU - hence the probability of a pipe break drops by about two to three orders of magnitude for break area exceeding twice that of the largest feeder pipe. Thus any "large LOCA" can only be located in the large piping above the core, and is analyzed separately from small LOCAs. There are three representative locations: reactor inlet header (RIH), reactor outlet header (ROH), and pump suction line[i] (PSH). Other locations are lines connected to the pressurizer, shutdown cooling lines and the header interconnnect lines.

Breaks at the low end of the large LOCA size range (so-called transition breaks) behave in an intermediate fashion between large and small LOCAs.

### *1.2. Safety Aspects*

Safety aspects are as follows:

- Jet forces from the broken pipe, and reaction forces causing pipe whip. The effect of these on other pipes, on the shutdown systems, and on containment must be assessed.
- Voiding of the channels, and decrease in flow in the downstream core pass. Normally break size is treated as a parameter to find the break with the most severe and prolonged flow stagnation (the "critical" break) in the downstream core pass. A power increase results from core voiding, causing a fuel temperature increase, and requires a shutdown system trip.
- Continued fuel heatup after reactor trip, as the channels continue to empty prior to ECC injection. There is a potential for fuel damage due to excessive sheath strain or sheath embrittlement; and for channel flow area reduction due to sheath strain.
- For the critical breaks, a number of pressure tubes may overheat and sag or strain into contact with the surrounding calandria tube.
- Heat transfer to the moderator from any channels with pressure tube/calandria tube contact, so that further channel deformation is prevented.

---

[i] For the Bruce plant, pump discharge breaks are also considered because there are two core passes connected to each pump

- Containment pressure increase, and differential pressures within containment compartments.
- Leakage of radionuclides from containment and resulting public dose.

*1.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below the Event Class 3 limit in Figure 1.
2. Pipe whip is limited so that:
   - there is no impairment of either of the shutdown systems below their minimal allowable performance standards
   - there is no break induced in the piping of the other HTS loop (for two loop plants)
   - there is no shearing off of large numbers of feeder pipes
   - there is no damage to the containment boundary
   - there is no break induced in ECC piping (not connected to the broken pipe)
3. The channel geometry must remain coolable. There are two sufficient criteria: the amount of fuel sheath oxidation must not embrittle the sheaths on rewet, and the amount of sheath strain must be limited so that coolant can flow through the channel.
4. Channel integrity is maintained.
   Sufficient conditions include:
   - there is no fuel melting
   - there is no sheath melting
   - there is no constrained axial expansion of the fuel string[j]

   For cases where the pressure tube strains or sags, it is sufficient if:
   - the pressure tube does not fail prior to contacting the calandria tube. This criterion is satisfied if the pressure tube local strain is less than 100% at any location.
   - the calandria tube remains intact after pressure tube contact. This criterion is satisfied if the calandria tube outer surface does not go into prolonged film boiling.
5. Pressure within containment is below design pressure.
6. Pressure within containment compartments does not cause internal structural failures.

*1.4. Relevant Event Combinations*

A large LOCA is also analyzed in combination with other impairments, including in turn the ECC, containment systems, and loss of normal AC power (Class IV).

---

[j] As the fuel heats up, the 'string' of 12 fuel bundles will lengthen due to thermal expansion; the amount must not cause it to come up hard against the end-fittings and buckle.

The following **ECC system impairments** are analyzed in turn: failure of injection, failure of loop isolation, failure of steam generator secondary side "crash" cooldown[k]. The first case is generally limiting and is a severe accident within the design basis.

The combination of a large LOCA with a loss of ECC gives rise to additional or changed *safety aspects* from those listed in Section 1.2 as follows:

- the moderator is required to remove reactor decay heat in the long term
- hydrogen is produced by oxidation of the fuel sheaths and of part of the pressure-tube, and is released to containment
- since ECC makeup is not available to the broken loop, long-term fuel cooling and channel integrity must be assured for this loop also.

The result of a LOCA + LOECC calculation is highly sensitive to the assumed steam flow rate in the channel (the worst being a few grams per second per channel); thus the imposed channel flowrate is a *key safety parameter* which is varied parametrically[l].

Similarly LOCA + LOECC has additional or changed *acceptance criteria* from those listed in Section 1.3 as follows:

- Acceptance criterion 1 becomes: Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1.
- Acceptance criterion 3 for large LOCA does not apply. There is no limit on sheath embrittlement, and the fuel bundle geometry is not required to be "coolable" by fluid within the channel.
- Acceptance criteria 2, 4, 5, and 6 apply to this event as written.
- Gross $UO_2$ melting does not occur. This is a necessary condition to preserve channel integrity.
- Hydrogen detonation within containment does not occur; if hydrogen combustion occurs, the pressure stays below design pressure. As a sufficient condition, one can require that the concentration of hydrogen inside containment remains below the lower limit for

---

[k] unless the instrumentation consists of two redundant independent sets, each having three channelized signals, in which case failure of crash cooldown is considered very low probability and need not be explicitly designed for.

[l] Not a very satisfactory approach as it leads to unrealistically high hydrogen concentrations in containment and over-design of hydrogen mitigation equipment. In future LOCA +LOECC will be treated more realistically - in RD-337 it is simply part of the severe accident set and analyzed using *realistic* models and assumptions.

downward flame propagation, or about 9% by volume. (There are further issues related to the effect of fast flames on local pressures, and the effect of a standing flame on mitigating equipment.)

The following **containment system impairments** are analyzed in turn: loss of air coolers; loss of dousing; open ventilation dampers; deflated airlock door seals; open airlock doors. The multi-unit stations in Canada have a vacuum containment, so a number of additional containment impairments are considered: partial or total loss of vacuum; failure of the instrumented containment pressure relief valves to open or close; failure of one bank of self-actuating containment pressure relief valves.

The combination of a large LOCA with a containment system impairment gives rise to additional or changed *safety aspects* from those listed in Section 1.2 as follows:

- the assumption of impairment of the containment heat sinks increases the internal containment pressure and reduces the margin to design pressure
- fractional releases from containment are larger, so for single-unit plants, the ECC must be designed to limit the number of fuel failures and associated fission product release.

Similarly LOCA + impaired containment has additional or changed *acceptance criteria* from those listed in Section 1.3 as follows:

- Acceptance criterion 1 becomes: Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1. However the cases of loss of *all* air coolers, and of open airlock doors, are submitted for information only and do not fall into any Event Class.

Large LOCA cases also are analyzed assuming failure of normal AC electrical power from the grid or the turbine-generator (Class IV power). *Safety aspects* are generally similar to the cases with Class IV Power available. Differences usually are matters of degree: the pump rundown is faster, the critical break size shifts, secondary side cooling is reduced, the flow in the intact loop[m] is smaller and the moderator cooldown is slower. *Acceptance criteria* relative to Section 1.3 are changed as follows:

- Acceptance criterion 1 becomes: Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1.

[m]For two-loop plants - Bruce A & B have one HTS loop.

The classification of event combinations involving an induced Loss of Class IV power assumes a reasonably reliable electrical grid (such as in Canada or Korea), so that the likelihood of losing Class IV power as a result of a reactor trip is small. This is however site-dependent, and the Event Class might need to be changed if the external grid reliability is poor, particularly if there is only one unit on the site.

## 2. Small Heat Transport System LOCA

In this and subsequent sections, the differences from the large LOCA section are highlighted. The common material is not duplicated.

### *2.1. Initiating Event*

A small LOCA is a break in any pipe, with an area up to the size of twice the cross-section of the largest feeder pipe. Spurious opening of a Liquid Relief Valve is included in this category. Events affecting a single reactor fuel channel or one or more steam generator tubes are also small breaks, but because of their specific phenomenology are covered separately.

### *2.2. Safety Aspects*

Safety aspects are as follows:

- potential for fuel sheath dryout at *high* power as the circuit depressurizes (see Chapter 8).
- potential for fuel sheath dryout or pressure tube local overheating at *decay* power prior to ECC injection. This could be caused by flow stratification in the reactor inlet header or in the channel. The combination of a small LOCA with an assumed loss of Class IV power is the limiting case.
- fuel cooling in the long term without forced circulation. For two-loop reactors, cooling of the "intact" loop must also be analyzed because it will be isolated from the other loop and operate with reduced inventory until it is refilled by ECC[n].

Since normal action of the reactor regulating system (RRS) can compensate for the slow increase in reactivity due to coolant void, and delay the trip on high power, two cases are considered: RRS inactive, and RRS operating normally.

### *2.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below the Event Class 2 limit in Figure 1.
2. There should be no systematic fuel failures (this is sufficient but not necessary to meet the dose limit; it also reduces the economic risk from a small LOCA). There are two periods of interest: at high power (before reactor trip), and at low power (due to prolonged dryout at low flows). The fuel sheath will remain intact if:
   - there is no fuel centreline melting (centreline temperature < 2840C)

---

[n]On some two-loop plants, loop isolation has been disabled for this reason.

- there is no excessive strain (uniform sheath strain less than 5% for temperatures <1000C)
- there are no significant cracks in the surface oxide (uniform sheath strain less than 2% for temperatures >1000C)
- there is no oxygen embrittlement (oxygen concentration < 0.5% by weight over half the sheath thickness)
- there is no penetration by the beryllium braze at spacer and bearing pad locations

3. Criteria 4,5&6 listed in Section 1.3 also apply.

*2.4. Relevant Event Combinations*

As with large breaks, small LOCAs are combined (separately) with impairments of ECC and of containment. The behaviour is bounded by, or similar to, large LOCAs with the same impairments. The acceptance criteria are likewise the same.

Small LOCAs also are analyzed assuming failure of Class IV power. *Safety aspects* are generally similar to the cases with Class IV Power available. As with large LOCA, differences usually are matters of degree: the most important safety aspect is ensuring sufficient thermosyphoning flow in both HTS loops to maintain channel integrity. *Acceptance criteria* are changed relative to those identified in Section 2.3 as follows:

- Acceptance criterion 1 becomes: Dose to the most exposed individual in the critical group is below the Event Class 4 limit in Figure 1.
- Acceptance criterion 2 becomes: There should be no systematic fuel failures before or immediately after reactor trip. However some fuel failures may occur during the ECC phase.

## 3. Single Channel Events

### *3.1. Initiating Event*

Single Channel Events are a particular subset of small LOCAs affecting only one reactor fuel channel. They consist of:

- a "spontaneous" pressure tube rupture, assumed for the purpose of analysis to result also in rupture of the calandria tube[o].
- a break in an individual feeder pipe. A special case is a break in an inlet feeder of exactly the right size to temporarily stagnate the flow in the channel. This can then result in channel overheating and failure.
- failure of the end-fitting attached to the pressure-tube, and assumed ejection of the fuel.
- blockage of the flow in a channel, assumed to be complete enough to cause channel overheating and failure.

### *3.2. Safety Aspects*

The safety aspects are similar to a small LOCA as far as the reactor HTS is concerned. There are additional safety aspects for in-core breaks:

- the potential for damage to in-core components such as reactivity mechanisms, and the effect on the available shutdown margin. The worse case is LOCA with loss of ECC (since the ECC utilizes light water and introduces negative reactivity).
- the potential for propagation of the break to other reactor fuel channels
- the potential for ejection of the end-fitting (or both end-fittings), causing a loss of moderator
- calandria overpressure due to the discharge of high-enthalpy fluid into the moderator
- for the case of flow blockage or inlet feeder stagnation break, calandria overpressure due to the interaction of hot and possibly molten fuel with the moderator
- safety system initiation signals (since high building pressure may not be effective for an in-core break)
- fission product release in an end-fitting failure with fuel ejection, since the bundles are exposed directly to the containment atmosphere; and in flow blockage, since a large fraction of the bound fission product inventory in the fuel can be released to containment
- fission product washout in the moderator

---

[o] For ACR-1000, the calandria tube will withstand a pressure-tube spontaneous break, although the combined failure of both tubes is still used as the design basis for the calandria structure and relief ducts.

For in-core breaks, given the potential for damage to shutoff rod guide tubes and the displacement of moderator poison, a number of assumptions are made to maximize net reactivity:

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Initial reactor operating state | Startup after a long shutdown | Maximize reactivity due to decay of neutron-absorbing isotopes in the fuel |
| Fuel burnup | Plutonium peak | Maximize reactivity due to fuel |
| Moderator poison load | High | Maximize reactivity due to displacement of moderator |
| Coolant isotopic purity | High | Maximize reactivity due to displacement of moderator |
| Failed channel location | Near most effective shutoff rods | Maximize loss of shutoff rod reactivity |

For the ACR-1000, the use of light-water as a coolant removes the issue of shutdown margin for this case, since the light water will mix with the heavy-water moderator after channel failure, and produce a large negative reactivity.

### *3.3. Acceptance Criteria*

1. The small LOCA acceptance criteria identified in Section 2.3 apply. However fuel damage may occur in the affected channel.
2. The in-core failure does not damage reactivity mechanisms to the extent that the reactor cannot be shutdown by each shutdown system acting alone, assuming the most pessimistic operating state prior to the accident. Manual poison addition to the moderator may be credited 15 minutes after a clear indication of the event.
3. The failure does not propagate to other reactor fuel channels.

4. The calandria vessel pressure transient does not cause vessel failure or loss of moderator (other than through the relief pipes), and any vessel deformation does not prevent operation of the shutdown systems.

### *3.4. Relevant Event Combinations*

Single channel events are also combined with the impairments of containment, ECC and Class IV power. Safety aspects and acceptance criteria are the same as the small LOCA combined-event cases, with the exception that there is no requirement on the integrity of the affected channel or its fuel. For in-core breaks, particular attention is paid to moderator temperature, which will initially rise due to the discharge of coolant into the moderator. If an in-core break is combined with an impairment in ECC, some of the other channels may sag or strain (eventually) into contact with their calandria tubes. Thus the moderator temperature must be kept low enough to prevent prolonged dryout of the calandria tube. Finally if one or both end fittings are ejected, the moderator will drain through the broken calandria tube, and if ECC is not restored in time, the accident may progress to severe core damage. This is currently a CNSC Generic Safety Issue.

## 4. Single Steam Generator Tube Rupture

### *4.1. Initiating Event*

A guillotine rupture of a single steam generator tube is assumed.

### *4.2. Safety Aspects*

The safety aspects are similar to a leak[p] as far as the reactor HTS is concerned, but also include:

- release of the radionuclides contained in the HTS coolant outside containment
- the break must be isolated in the longer term, since the loss of water through the steam generator is unrecoverable.

The analysis focusses on ensuring there is adequate operator action time to perform HTS cooldown and steam generator isolation. Back-flow of (light) water from the secondary side to the primary side, after the latter is cooled down and depressurized, causes negative reactivity and is not a safety concern. Recent CANDUs have manually-operated main steam isolation valves, which can be used as one of the means to isolate the affected steam generator in the longer term.

### *4.3. Acceptance Criteria*

The acceptance criteria are identical to those of the small LOCA[q].

### *4.4. Relevant Event Combinations*

Since ECC is not required and the discharge of radionuclides is to the secondary side, outside the containment envelope, there are no relevant event combinations associated with ECC or containment impairments. However the effect of loss of Class IV power at the time of trip is assessed.

---

[p] A leak is defined as a loss of coolant small enough so that it can be compensated by the $D_2O$ makeup system; ECC is not required.

[q] Note that the C-6 Class of this event is in dispute between the CNSC and the industry - the former has requested Class 1 and the industry maintains it should be Class 2 based on experience to date. Such disputes are not unusual in a non-prescriptive regulatory framework, as discussed in Chapter 1.

## 5. Multiple Steam Generator Tube Failure

### *5.1. Initiating Event*

It is postulated that a number of steam generator tubes (up to 10) fail simultaneously.

### *5.2. Safety Aspects*

- The effect on the HTS is similar to a small break (0.5% of the largest inlet header break).
- As with a single steam generator tube rupture, there is a discharge of radionuclides outside containment.
- The accident time scale is much shorter than for a single steam generator tube rupture, so automatic action of the shutdown systems and of ECC is required.
- The operator is required in the longer term to valve in an alternate heat sink and stop further discharge outside containment.

### *5.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1.[r]
2. The fuel channels should not fail due to overheating.

### *5.4. Relevant Event Combinations*

None, since the initiating event is already Event Class 5.

[r] This reflects the designer interpretation of C-6 Rev. 0 in the safety analyses of all recent plants.

## 6. Loss Of Forced Circulation

### *6.1. Initiating Event*

A loss of Class IV electrical power to the HTS pumps causes them to run down and eventually stop. Particular cases of partial loss of forced circulation include a partial loss of Class IV power, a single HTS pump shaft seizure and a single pump trip.

### *6.2. Safety Aspects*

A flow reduction causes a mismatch between reactor power and coolant flow that can lead to fuel overheating and HTS pressurization. The power mismatch also causes void formation in the channels, leading to an increase in reactor power.

Note that, contrary to previous prediction, a Loss of Class IV power at Gentilly 2 some years ago led to a trip on high neutron log rate. The power rise was more rapid than predicted, and seems to have been caused by subcooled nucleate boiling in the channels prior to trip, a phenomenon which up until then had not been accurately modelled. There are always lessons to be learned from real events.

Normal operation of the RRS can delay a reactor trip or make one unnecessary; shutdown system effectiveness must be shown whether the RRS operates normally or fails to respond.

### *6.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below the limits listed below:
   Loss of Class IV Power: Event Class 1 limit in Figure 1
   Pump Seizure: Event Class 2 limit in Figure 1

2. The heat transport system must remain intact. Thus it must not fail due to:
   - overpressure
   - overheating of the pressure tubes.

3. For loss of Class IV power and single pump trips: The service limit for SDS1 high pressure trip is ASME Level B (“upset”) crediting the liquid relief valves (LRVs). This is interpreted as 110% of design pressure. The service limit for SDS2 high pressure trip is ASME Level C (“emergency”) with and without crediting the LRVs. This is interpreted as 120% of design pressure. The first trip parameter may be credited in the case where this trip parameter is high pressure.[8]

4. For single pump seizure: The service limit for SDS1 high pressure trip is ASME Level C ("emergency") crediting the liquid relief valves (LRVs). This is interpreted as 120% of design pressure. The service limit for SDS2 high pressure trip is ASME Level D ("faulted") with and without crediting the LRVs. This is interpreted as 120% of design pressure. The first trip parameter may be credited in the case where this trip parameter is high pressure.
5. Systematic fuel failures are prevented[s]. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.

### *6.4. Relevant Event Combinations*

Since there is no fuel damage for these events, there are no relevant event combinations with impairments of ECC or containment.

[s] This is sufficient but not required for single pump seizure.

## 7. Loss Of Reactivity Control (LORC)

### *7.1. Initiating Event*

A malfunction in the Reactor Regulating System (RRS) is assumed to drain zone controllers and/or drive out absorber/adjuster rods. Two types of accidents are considered: continued increase in reactivity at up to the maximum possible rate, and to the maximum degree allowed by the physical configuration of the devices; and a slow power increase from both normal and distorted flux shapes that terminates just below the overpower trip setpoints.

### *7.2. Safety Aspects*

An increase in reactor power causes a flow/power mismatch which has the potential to damage fuel.

Reactivity ramps from malfunctions in the RRS or its components are inherently slower than those caused by a LOCA. Since large LOCA determines the setpoints of the bulk overpower and rate trips on each shutdown system, loss of reactivity control ramps are not limiting.

However a slow increase from a distorted flux shape could permit fuel to be in dryout even if the bulk reactor power is below the average overpower trip setpoint. Analysis of such events determines the trip setpoints for the spatially-distributed Regional Overpower (ROP) flux detectors on each shutdown system.

The setback and stepback functions (which reduce power if an abnormal situation is sensed) are not credited in the analysis. However the following systems may, by their normal action or inaction, delay a reactor trip; therefore both cases are analyzed:

- HTS pressure and inventory control working or failed
- steam generator pressure control working or failed
- steam generator level control working or failed

The reactivity rates of the control devices in the analysis are varied parametrically over the complete physically possible range, to ensure that trip parameter coverage is comprehensive. For reactivity rates from distorted flux shapes, flux shapes are selected to cover all expected modes where continued operation is permitted - e.g., operating with a stuck absorber rod.

### *7.3. Acceptance Criteria*

Similar to Loss of Forced Circulation:

1. Dose to the most exposed individual in the critical group is below the Event Class 1 limit in Figure 1.

2. The heat transport system must remain intact. Thus it must not fail due to:
   - overpressure
   - overheating of the pressure tubes.

3. The service limit for SDS1 high pressure trip is ASME Level B ("upset") crediting the liquid relief valves (LRVs). This is interpreted as 110% of design pressure. The service limit for SDS2 high pressure trip is ASME Level C ("emergency") with and without crediting the LRVs. This is interpreted as 120% of design pressure.

4. Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.

### *7.4. Relevant Event Combinations*

Since there is no fuel damage for these events, there are no relevant event combinations with impairments of ECC or containment.

## 8. Loss Of Pressure And Inventory Control (Primary)

### *8.1. Initiating Event*

Pressurization events can result from:
- feed valves fail open / liquid bleed valves fail closed
- pressurizer heaters fail on / steam bleed valves fail closed

Depressurization events can result from:
- feed valves fail closed / liquid bleed valves fail open
- pressurizer heaters fail off / steam bleed valves fail open
- HTS liquid relief valves fail open

### *8.2. Safety Aspects*

Pressurization events test the capability of the liquid relief valves and the ability in the long term to stop any unrecoverable loss of coolant. Depressurization events are similar to a small LOCA. Since in the depressurization sequences there may be no immediate discharge to containment, appropriate signals must be identified for reactor trip and/or operator alarms and, if necessary, for ECC.

### *8.3. Acceptance Criteria*

Similar to Loss of Pressure Control and Loss of Reactivity Control:

1. Dose to the most exposed individual in the critical group is below the Event Class 1 limit in Figure 1.

2. The heat transport system must remain intact. Thus it must not fail due to:
   - overpressure
   - overheating of the pressure tubes.

3. The service limit for SDS1 high pressure trip is ASME Level B (“upset”) crediting the liquid relief valves (LRVs). This is interpreted as 110% of design pressure. The service limit for SDS2 high pressure trip is ASME Level C (“emergency”) with and without crediting the LRVs. This is interpreted as 120% of design pressure. The first trip parameter may be credited in the case where this trip parameter is high pressure.

4. Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.

### *8.4. Relevant Event Combinations*

Since there is no fuel damage for these events, there are no relevant event combinations with impairments of ECC or containment.

## 9. Main Steam Line Breaks

### *9.1. Initiating Event*

This event class includes rupture of the steam piping inside or outside the reactor building, up to the complete guillotine rupture of the steam balance header.

### *9.2. Safety Aspects*

The first safety aspect for all main steam line breaks is the potential loss of a reactor heat sink as the secondary side inventory is exhausted through the break. For main steam line breaks outside containment, in the turbine hall, one must show that equipment which is required and assumed to mitigate the event is not damaged by the forces, the steam, or the high temperature caused by the break, nor is there damage to the turbine hall structure. For main steam line breaks inside containment, the pressure rises rapidly and the safety aspect is the building integrity, including the integrity of reactor building internal walls. The depressurization of the secondary side causes a corresponding depressurization and cooling (initially) of the primary side; this causes a negative reactivity and a power *decrease* and is not a safety concern. Both symmetric breaks affecting all steam lines equally (e.g., steam balance header break) and asymmetric breaks (affecting only one steam line) must be considered.

Large steam line breaks are limiting in terms of early containment peak pressure and time available to introduce an alternate heat sink. Small steam line breaks test the trip coverage and can lead to a long-term containment pressurization after the containment dousing water is exhausted.

Since the HTS pumps are tripped on low HTS pressure, the ability to remove heat from the HTS through thermosyphoning, particularly if the HTS is two-phase, must be confirmed.

Note that since CANDUs have a high-pressure backup heat sink (the Shutdown Cooling System), it is not necessary for the operator to depressurize the HTS before valving in this alternate heat sink in emergencies.

### *9.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below the Event Class 3 limit in Figure 1.
2. The heat transport system must remain intact. Thus it must not fail due to:
    - overpressure
    - overheating of the pressure tubes.

In practice this means that the secondary side inventory must be sufficient so that a manually-initiated alternate heat sink can be initiated within 15-30 minutes of the break, depending on whether the action can be taken from the Main Control Room or must be taken from the field.

3. Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.
4. For main steam line breaks within containment, the containment pressure must stay below the threshold pressure for through-wall cracking of the perimeter wall.
5. The transient differential pressure across the reactor building internal walls should not impair the structural integrity of the walls.
6. The turbine hall wall structural integrity is maintained (if necessary to protect equipment credited in the accident mitigation).

*9.4. Relevant Event Combinations.*

A main steam line break is analyzed in combination with the following impairments in the special safety systems:

The following **ECC system impairments** are analyzed in turn: failure of injection, failure of loop isolation, failure of steam generator secondary side "crash" cooldown[t]. The combination of a main steam line break with a loss of ECC gives rise to additional or changed *safety aspects* relative to Section 9.2 as follows:

- ECC may not be automatically initiated, in which case there is no change from the single failure
- where ECC is automatically initiated, it acts as a makeup to the HTS as the latter cools down and shrinks. In the absence of such a makeup, adequate two-phase thermosyphoning must be demonstrated to remove decay heat. Note that ACR has Core Makeup Tanks, one connected to each loop, to makeup for shrinkage for such events.

Similarly a main steam line break + LOECC has additional or changed *acceptance criteria* relative to Section 9.3 as follows:

- Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1.

[t] unless the instrumentation consists of two redundant independent sets, each having three channelized signals.

The following **containment system impairments** (for main steam line breaks inside containment) are analyzed in turn: loss of air coolers, loss of dousing, open ventilation dampers, deflated airlock door seals, open airlock doors.

The combination of a main steam line break with a containment system impairment gives rise to additional or changed *safety aspects* as follows:

- the assumption of impairment of the containment heat sinks increases the internal containment pressure
- containment envelope impairments reduce the peak pressure but may (depending on the setpoints) decrease the trip coverage provided by containment high-pressure trips.

Similarly a main steam line break + impaired containment has additional or changed *acceptance criteria* as follows:

- Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Figure 1.
- The structural integrity of the containment must not be impaired to a degree that consequential damage to the reactor systems could result (note since the radioactivity releases are small, there is no requirement for existing plants for staying below containment design pressure).

A main steam line break inside containment combined with failure to isolate the containment ventilation results in lower peak pressures within containment but may delay the reactor trip on high building pressure. The same is true for deflated airlock door seals. ECC may be initiated for a main steam line break (on low HTS pressure conditioned on high building pressure) but is not required for accident mitigation.

Main steam line breaks are also analyzed assuming failure of Class IV power. *Safety aspects* are generally similar to the cases with Class IV Power available, with the focus being on demonstration of the effectiveness of natural circulation in the HTS. Other differences usually are matters of degree: containment air coolers and secondary side feedwater are temporarily lost until Class III power is established, and the HTS pumps run down earlier. The *acceptance criteria* are the same as for a main steam line break plus containment system impairments.

## 10. Feedwater System Failures

### *10.1. Initiating Event*

Loss of feedwater can result from a break in a feedwater line, loss of the feedwater pumps, or spurious closure of one or more feedwater valves.

### *10.2. Safety Aspects*

Similar to main steam line breaks: The first safety aspect for all feedwater system failures is the potential loss of a reactor heat sink as the secondary side inventory is depleted. For feedwater line breaks inside containment, the containment pressure rises and the safety aspect is the building integrity, including the integrity of reactor building internal walls. Both symmetric breaks affecting all feedwater lines equally (e.g., break upstream of the feedwater control valves) and asymmetric breaks (affecting one steam generator more than the others - e.g., breaks downstream of the control valves) must be considered.

Large steam line breaks are more limiting (in terms of early containment peak pressure and in terms of differential pressures within the reactor building) than large feedwater line breaks. Large steam line breaks are also limiting in terms of public dose.

Because the Shutdown Cooling System can be brought in at full system pressure, it is not necessary for the operator to depressurize the HTS before bringing in this alternate heat sink in emergencies.

### *10.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below:
   - Event Class 1 limit in Figure 1 for failures of feedwater control;
   - Event Class 3 limit in Figure 1 for breaks in the feedwater piping.

2. The heat transport system must remain intact. Thus it must not fail due to:
   - overpressure
   - overheating of the pressure tubes.

   In practice this means that the secondary side inventory must be sufficient so that an alternate heat sink can be initiated within 15-30 minutes of the break, depending on whether the action can be taken from the Main Control Room or must be taken from the field.

3. The following overpressure criteria apply:

- For loss of flow feedwater failures, the service limit for SDS1 trip is ASME Level B ("upset") crediting the liquid relief valves (LRVs). This is interpreted as 110% of design pressure. The service limit for SDS2 trip is ASME Level C ("emergency") with and without crediting the LRVs. This is interpreted as 120% of design pressure.
- For feedwater pipe breaks, the service limit for SDS1 high pressure trip is ASME Level C crediting the liquid relief valves (LRVs). The service limit for SDS2 high pressure trip is ASME Level D ("faulted") with and without crediting the LRVs.

The first trip parameter may be credited in the case where this trip parameter is high pressure.

4. Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.
5. For feedwater pipe breaks within containment, the containment pressure must stay below the threshold pressure for through-wall cracking of the perimeter wall.
6. The transient differential pressure across the reactor building internal walls should not impair the structural integrity of the walls.

### *10.4. Relevant Event Combinations*

The ECC is neither initiated nor required for a feedwater system failure. Large steam pipe breaks together with containment system impairments bound the containment behaviour for feedwater system failures.

Feedwater failures are analyzed assuming failure of Class IV power. *Safety aspects* are generally similar to the cases with Class IV Power available, with the focus being on demonstration of acceptable thermosyphoning behaviour in the long term. The *acceptance criteria* are similar to those with Class IV power available, except that the public dose limits are:
Dose to the most exposed individual in the critical group is below:

- Event Class 3 limit in Figure 1 for failures of feedwater control;
- Event Class 5 limit in Figure 1 for breaks in the feedwater piping.

## 11 Loss of Secondary Side Pressure Control

### *11.1. Initiating Event*

Depressurization of the secondary side could result from inadvertent opening of the Atmospheric Steam Discharge Valves (ASDVs), or the Condenser Steam Discharge Valves (CSDVs), or the Main Steam Safety Valves (MSSVs); or failure to unload the turbine after a reactor trip. Pressurization of the secondary side could result from a loss of condenser vacuum.

### *11.2. Safety Aspects*

Since the HTS boundary is preserved, the safety aspect is release of a portion of any radioactivity contained in the secondary side. Generally the behaviour is bounded by steam and feedwater line failures. The secondary side controls are modelled in some detail to ensure that either their proper functioning, or lack of response, does not impair any safety system actions. Both normal and alternate modes of plant control are assessed.

### *11.3. Acceptance Criteria*

Same as for a loss of feedwater control.

### *11.4. Relevant Event Combinations*

None.

## 12 Loss of Shutdown Heat Sink

CANDU shutdown heat sinks include auxiliary feedwater, the shutdown cooling system, and ECC. Loss of a heat sink when the reactor is shutdown is usually analyzed by hand calculations of heatup rate, to show that there is sufficient time[u] for the operator to diagnose the event and valve in one of the backup heat sinks.

Note that during shutdown a number of heat sinks normally available during power operation may no longer be available (they, or their support systems, may be under repair). An important aspect of loss of shutdown heat sink analysis is to show that there are enough back-up systems should the primary means of heat removal fail, accounting for the possibility of reduced redundancy and the increased time required to bring them into operation (e.g., if the HTS is open and depressurized, it may be necessary to close it before a backup heat sink such as the steam generators can be brought in).

[u] As defined in Table 7-1

## 13. Moderator System Failures

### *13.1. Initiating Event*

Moderator system failures include:

- moderator pipe break
- loss of forced circulation
- loss of heat removal

### *13.2. Safety Aspects*

The safety aspects are as follows:

- doses resulting from the release of tritiated heavy water from the moderator after a pipe break, or due to moderator boiling after a loss of heat sink
- distortion of the reactor flux as the moderator boils down, leading potentially to excess power in some reactor fuel channels
- release of deuterium gas to the moderator cover gas and the potential for ignition.

A number of assumptions are made in safety analysis pertaining to the aspects unique to this type of event:

| Parameter | Conservative Direction | Rationale |
|---|---|---|
| Number of calandria rupture disks that burst | Low | Maximize calandria pressure |
| Moderator temperature | Low; | Delay high building pressure trip; |
| | High | Maximize tritium release and extent of deuterium degassing |
| Moderator heat load | Low; | Delay high building pressure trip; |
| | High | Maximize dose |
| Tritium concentration in moderator | High | Maximize |

| | | |
|---|---|---|
| | | radioactivity release |
| Cover gas purging | Not credited | Maximize combustible gas concentration |

*13.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below:
   - the Event Class 1 limit in Figure 1 for loss of moderator heat removal;
   - the Event Class 3 limit in Figure 1 for breaks in the moderator piping.

2. The heat transport system must remain intact. Thus it must not fail due to:
   - overpressure
   - overheating of the pressure tubes.

3. Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.

4. Deuterium deflagration in the cover gas does not damage the calandria nor impair the effectiveness of the shutdown systems. It is sufficient to show that deflagration does not occur. A lower limit of $D_2$ concentration, below which deflagration cannot occur, may be used for screening purposes (e.g., 4.5%).

*13.4. Relevant Event Combinations*

None.

## 14. Shield Cooling System Failures

### *14.1. Initiating Event*

Loss of shield cooling could occur through a break in the piping, a loss of forced circulation, or a loss of secondary side cooling water.

### *14.2. Safety Aspects*

The safety aspect is excessive shield tank distortion if the accident is not terminated. Generally the analysis is focussed on determining the time before operator action is required. There is no significant release of energy nor radionuclides to containment.

### *14.3. Acceptance Criteria*

1. There must be no consequential failure of the HTS pressure boundary. Thus the operator must have enough time after the first clear signal of the event to shut the reactor down and cool down the HTS. A stress analysis may be done, or an upper limit on the temperature difference between the inner and outer tubesheets can be used as a sufficient criterion.
2. There must be no distortion of the reactor assembly sufficient to impair the effectiveness of the shutdown systems.

### *14.4. Relevant Event Combinations*

None.

## 15. Fuelling Machine Accidents

### *15.1. Initiating Event*

A fuelling machine (F/M) carrying spent fuel may be either on the reactor, attached to a channel, or off the reactor, in transit to the spent fuel port, or attached to the spent fuel port and discharging fuel. The spent fuel must be kept cooled, and hoses are attached to the fuelling machine through which high-pressure $D_2O$ cooling water is pumped. Should one or more hoses fail, the integrity of the contained fuel is threatened.

Safety Analyses normally considers both cases: F/M on reactor, and off-reactor. The consequences to the reactor of a failure of a F/M on reactor (e.g., spurious detachment from a channel) are broadly similar to a single-channel event. This section deals with F/M accidents when off-reactor.

### *15.2. Safety Aspects*

The safety aspect is fuel overheating and failure if it cannot be cooled inside the F/M or in the transfer port. A F/M failure when off-reactor cannot be mitigated by reactor shutdown or ECC. The only safety system required is containment.

### *15.3. Acceptance Criteria*

1. Dose to the most exposed individual in the critical group is below:
   - the Event Class 1 limit in Figure 1 for F/M failures
   - the Event Class 3 limit in Figure 1 for F/M failures with simultaneous containment impairments

### *15.4. Relevant Event Combinations*

Only containment impairments are relevant, as discussed above.

## 16. Severe Accidents

### *16.1. Initiating Event*

Severe accident sequences are normally identified through a Level 1 Probabilistic Safety Assessment. However the event sequences discussed in previous sections of this report for existing CANDUs include a number of severe accidents (LOCA + LOECC, LOCA + impaired containment) *within* the design basis. In the first case the moderator can remove decay heat from the reactor in the absence of any coolant in the channels. Fuel is badly damaged but the $UO_2$ does not melt and channel integrity is preserved. Moreover for new build CANDUs, although dual failures are no longer a separate category of accidents, a comprehensive analysis of the frequency and consequences of beyond design basis and severe accidents is required. The tool used is a Level 2 PSA (Level 2 means it includes containment response) supported by consequence analysis.

It is useful on CANDU to distinguish three categories:

1. Severe accidents *within* the design basis, in which the core geometry is preserved (fuel remains inside intact pressure tubes). These have been already covered above. They are identified either explicitly in regulatory document C-6, or by the applicant as part of the systematic plant review required by C-6. RD-337 moves these to the "Beyond Design Basis" category - still requiring assessment but using more realistic assumptions.
2. Severe accidents *beyond* the design basis, in which the core geometry is preserved. They are not identified in C-6, which *ipso facto* defines design basis accidents. They are normally identified by a systematic plant review or by a PSA, and are too low in frequency to merit inclusion in the design basis set. RD-337 does require their analysis in order to show the safety goals are met.
3. Severe core damage accidents, *beyond* the design basis (by definition), in which the fuel channels fail and collapse to the bottom of the calandria. Again, RD-337 does require their analysis in order to show the safety goals are met.

An example of the second category would be loss of all secondary side heat sinks and shutdown cooling with the moderator available. Examples of the third category would be loss of coolant *plus* loss of ECC *plus* loss of moderator heat removal; or loss of Group 1 electrical power (Class IV *plus* Class III) *plus* loss of Group 2 Class III electrical power.

### *16.2. Safety Aspects*

Category 1 has been the subject of most of this chapter so far.

For Category 2, the analysis is generally similar to that for the severe accidents in category 1. For example, a loss of all heat sinks at high pressure would eventually result in the overheating and

failure of one or more pressure tubes; this would depressurize the HTS and allow the ECC and/or the moderator to act as a heat sink for the remaining channels.

Category 3 has new phenomena, and we summarize the severe core damage behaviour of CANDUs. Analysis of events in category 3 initially started from heat balance calculations[v] (to determine the times to boil off the water in the moderator, and then in the shield tank); followed by calculations of the characteristics of the debris once it collects in the bottom of the calandria vessel. Because of the large volumes of water in both the moderator and the shield tank, it takes about 20 hours (in the absence of active heat removal from either system) for the water to boil off, and for the debris to end up on the vault floor[9]. Unlike Design Basis Accidents, severe accident analysis uses realistic assumptions on initial plant states, plant parameters, equipment performance etc.

For these residual risk sequences in which the moderator is assumed unavailable, the fuel channels would fail progressively as the moderator boiled off, and collapse to the bottom of the calandria. Blahnik[10], using the MAAP-CANDU code, has characterized the degradation of a CANDU core with no cooling and gradual boiling-off of the moderator. The uncovered channels heat up and slump under their own weight until they are held up by the underlying channels. Eventually, as successive layers of channels pile up, the supporting channels (still submerged) collapse and the whole core slumps to the bottom of the calandria vessel.

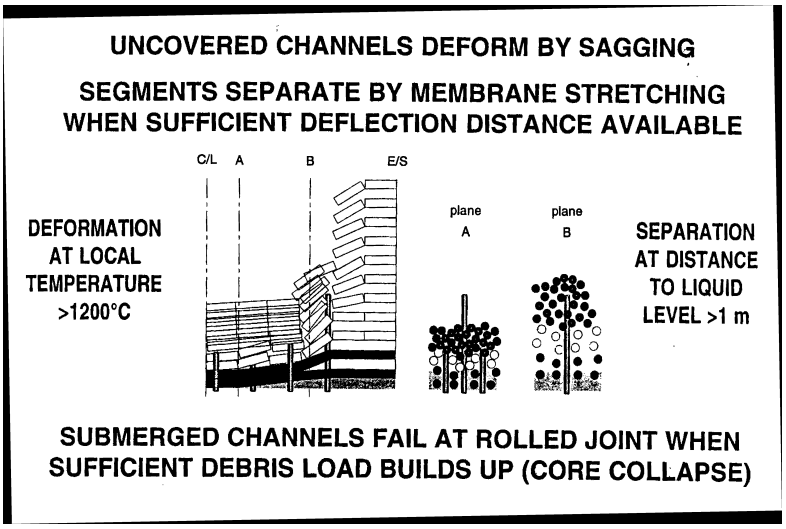


**Figure 3** - Postulated Channel Collapse Mode

Consider, for the purposes of discussing the phenomenology, a beyond-design basis severe accident that assumes loss of all heat transport system and emergency heat sinks at decay power levels (shutdown cooling system, main feedwater, auxiliary feedwater, Group 2 emergency feedwater, Emergency Core Cooling System, and moderator heat removal). In addition, assume an inability to depressurize the heat transport system (for which there are two independent signals). The analysis shows that only a very small number of channels are expected to fail at the high heat transport system pressures (~6 to 10 MPa). Such a failure would first occur due to local

[v] including the effects of metal-water reaction heat

straining in a high decay power channel located at a high elevation in the reactor core. The fuel in the channel will either remain there, or will fall to the bottom of the calandria vessel, where it will be cooled by the surrounding moderator. The failure of one or two channels would induce rapid depressurization of the partially voided heat transport system and allow the pressure tubes to strain into contact with the calandria tubes without failure. For the same accident at intermediate pressures (~1 to 6 MPa) the pressure tubes will balloon into full circumferential contact with the calandria tube. The channel will remain intact as long as the outside surface of the calandria tube does not undergo a prolonged period of film boiling or is surrounded by a void. With loss of moderator heat removal, the moderator will gradually boil off. Voiding around the channel outside surface occurs when the moderator level in the calandria vessel falls below the channel. Again, one or a few high power channels located at a high elevation and which were uncovered early could fail (Fig. 7-3). The number of channels that could fail by this mechanism is also expected to be very small. Therefore, as the moderator level falls further, the majority of channels at decay power levels are expected to fail under low system pressures (<1 MPa). The mechanisms of channel failure under those conditions are expected to be through excessive sag and/or local overheating.

To determine the mechanisms, a research program was initiated at AECL. The current understanding is as follows:

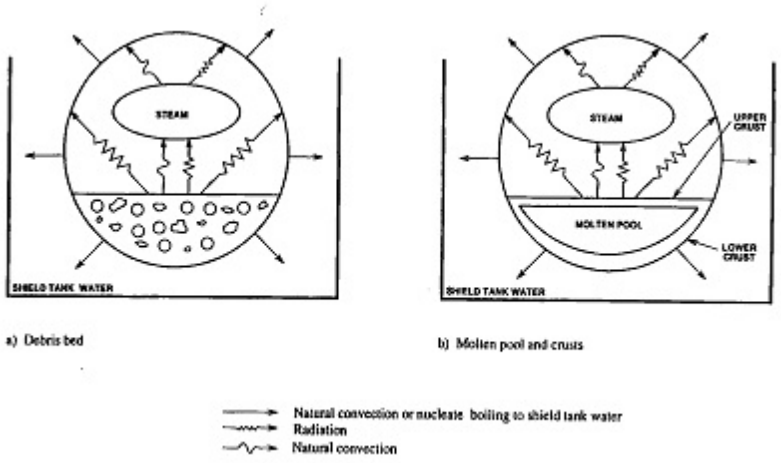


**Figure 4** - Mechanistic Model of Channel Collapse

As channels are uncovered during moderator boil-off, their temperatures rise and they begin to sag under gravity loads. The axial creep rate of the pressure tube material (Zr-2.5% Nb) increases rapidly with temperature and excessive sagging of the channel is expected to occur above ~1200C. In Blahnik's model, a sagging channel comes into contact with the next lower row of channels. The lower row of channels may or may not be cooled adequately by the moderator, depending on whether it is submerged in the moderator or not. As the moderator level continues to decrease, the lower row of channels is uncovered and sags under its own weight as well as that of the supported channels. This process continues as more channels are uncovered. As sagging increases, channel segments separate near the bundle junctions by sag-induced local strain. A suspended debris bed is thus formed which moves downward with the falling moderator level. Since a submerged channel can support only a certain number of channels, the ends of those channels are expected to fail by shear. This process will increase the loading on the channels

below leading to progressive failure of the channels resulting ultimately in the collapse of the reactor core into the water pool in the bottom of the calandria vessel.

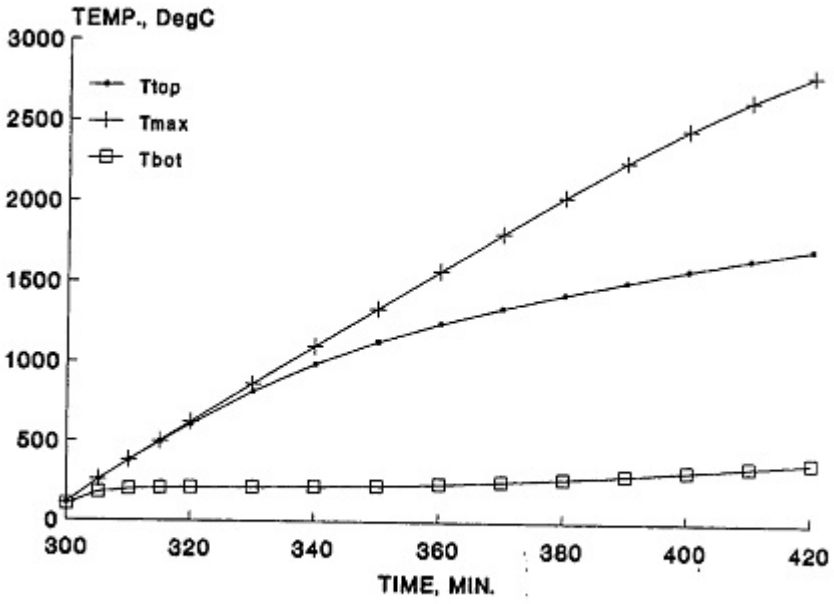


Figure 7 Heat Up of Core Debris in CANDU 6 Calandria, Reference Conditions

**Figure 5** - Debris Bed Temperatures (Rogers)

To address the plant state once the debris has collapsed to the bottom of the calandria, Rogers et al.[11] have developed an empirically-based mechanistic model (Fig. 7-4) of the collapse process, that shows that the end-state consists of a bed of dry, solid, coarse debris irrespective of the initiating event and the core collapse process. Heat-up of the debris bed is relatively slow, because of the low power density of the mixed debris and the spatial dispersion provided by the calandria shell, with melting possibly beginning in the interior of the bed about two hours after the start of bed heat-up. The upper and lower surfaces of the debris remain well below the melting point (Fig. 7-5) and heat fluxes to the shield tank water are well below the critical heat flux at the existing conditions (Fig. 7-6). The calandria vessel is protected by a solid crust of material on the inside, and by water on the outside, so it can prevent the debris from escaping. Should the shield tank water not be cooled, it will boil off, and the calandria vessel will eventually fail by melt-through, but this will not occur in less than about a day.

Clearly the analysis of such sequences is in its early stages, although the key characteristics of long times and the potential of arresting the accident at the calandria shell boundary are well recognized. Integrated system models have been developed to cover the transient behaviour from initiating event to quasi-steady state, supported by small scale experiments[12] aimed at phenomena unique to CANDUs such as channel collapse and core debris retention.

### *16.3. Acceptance Criteria*

CNSC document C-6, as noted, includes acceptance criteria for some severe accidents; but there are no formal requirements under the current regulations for severe core damage accidents.

However the CNSC Staff have stated that on new designs, they will expect explicit consideration of such accidents in the design (as outlined in RD-337) to show the safety goals are met, and have requested the utilities in Canada to develop severe accident management procedures using existing equipment.

This is consistent with world practice.

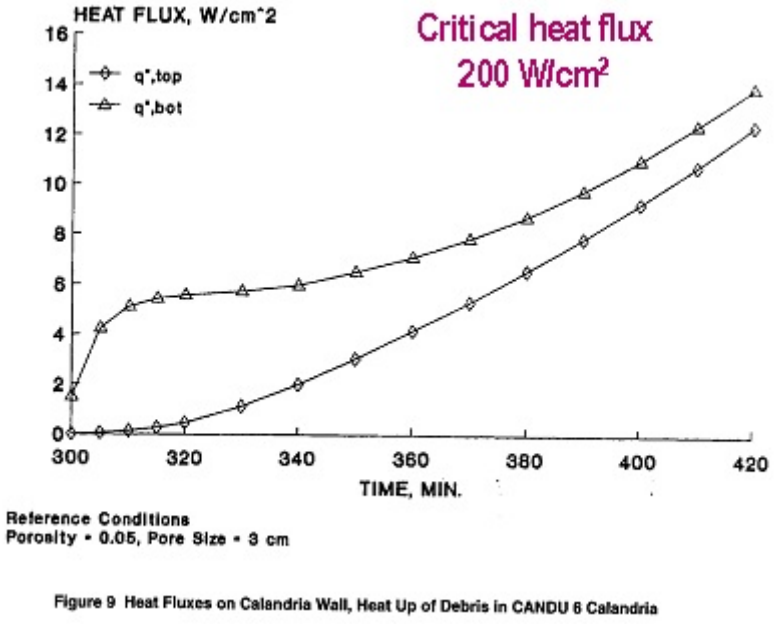


Figure 9 Heat Fluxes on Calandria Wall, Heat Up of Debris in CANDU 6 Calandria

**Figure 6** - Calandria Wall Heat Flux (Rogers)

As an example, the ACR design incorporates the following requirements and features and could be considered typical of how severe core damage issues are addressed in new plants:

1. The summed frequency of severe core damage event must be less than $10^{-5}$ /reactor year and is targeted to be less than $10^{-6}$ /reactor year
2. Gravity-driven makeup to either the steam generators, the reactor coolant system, the moderator or the shield tank, from an elevated Reserve Water Tank located high inside containment, can remove decay heat by steaming for several days. This prevents collapse of the fuel channels, or, if they do collapse, prevents penetration through the calandria shell. Long-term heat removal from containment for such sequences would be via either air coolers; or from containment sprays which are recirculated and cooled. Firewater could be used as a severe accident management tool for core makeup, as we saw in the Narora accident.
4. Hydrogen recombiners are used in containment for control of local and global hydrogen concentrations in the short- and long-term.

## Uncertainty Analysis

There are three different sources of uncertainty: the physical models used as expressed in the computer codes used for safety analysis, the plant model or idealization implemented in the codes, and the data used for plant parameters.

Although the physical models used are, where possible, "best estimate" models, and the plant idealization is likewise intended to be accurate rather than biassed, the input physical parameters and, more important, the assumptions on the plant state and action of mitigating systems, are highly conservative, as we have seen throughout this Chapter. Even though dose limits are met, the analysis gives a distorted and pessimistic picture of the plant response to abnormal events, with no measure of how far this response is from "expected" behaviour in an accident. Thus in recent years "best estimate plus uncertainty analysis" has been done in selected CANDU cases. Such analyses are doubly valuable since they also provide the basis for simulations used in operator training.

A true "best estimate" analysis needs a substantial amount of work since it requires developing realistic models of behaviour; it is often less costly to use conservative models. However the dominant conservatisms used in safety analysis are well-known; replacing them with more realistic assumptions is the first step toward a better estimate. The dominant conservatisms include:

- no credit for positive corrective action by operating staff for the first 15 to 30 minutes following the event
- no credit for the action of the reactor regulating system which is designed to match heat production and heat removal (and would mitigate the accident through power reduction)
- no credit for mitigation by process systems (e.g. HTS pressure and inventory control, steam generator level and pressure control)
- no credit for the first shutdown system to act
- no credit for the earliest trip on the second shutdown system
- no credit for the earliest instrumentation channel to trip on the second trip signal on the second shutdown system
- no credit for the negative reactivity introduced by light-water Emergency Core Coolant
- generally assuming about half the actual number of ECC valves, MSSVs, LRVs etc. are available
- use of a pessimistic bundle power/burnup envelope, over-predicting peak bundle powers
- assumption of the maximum operational total reactor overpower

- use of a two-standard deviation allowance on key physical parameters such as void reactivity coefficient
- use of worst weather occurring less than 10% of the time

To date the approach has been to perform a "best estimate" analysis by removing assumptions such as those listed above. Uncertainties in key parameters (e.g., void reactivity, shutdown system delay time) are then added back in, but rather than stacking independent uncertainties linearly, as is done usually in safety analysis for licensing, they are combined in a root-mean-square fashion to estimate the statistical uncertainty in the answer. To date the results of "best estimate plus uncertainty" analyses have shown much less severe consequences in accidents than have the extreme value analyses usually presented for licensing.

As noted, there are two additional sources of uncertainty beyond plant data: the physical model and the plant idealization. A full "best-estimate" analysis should be accompanied by uncertainty assessments not just of plant parameters, but also of code models[w] and the plant idealization. The scope of uncertainty analysis is defined and limited by the safety analysis. That is, the object of the safety analysis is to compare model predictions of certain safety parameters against acceptance criteria. It is the uncertainty in these specific predictions, not in the entire safety analysis output, that is most significant. These predictions then define, to a large extent, which aspects of the plant model and of the physical models need an uncertainty assessment in turn. For example, an acceptance criteria for a large LOCA is prevention of fuel centreline melting. Uncertainties in this prediction arise from uncertainties in fuel physical properties and the fuel model in the computer code, as well as in channel thermohydraulics and reactor physics. Those aspects of the data and models which influence strongly the prediction of fuel centreline temperature should have their uncertainty quantified and incorporated into the overall uncertainty calculation of fuel centreline temperature. It is less important to quantify other aspects, for this purpose. Thus an initially intractable problem becomes more manageable.

[w] Generally once one corrects for a code bias, there is no need to add a further code uncertainty since it would double-count the uncertainty due to the scatter of the experimental data.

## Exercises

Do either question 1 or question 2.

1. Estimate the evolution (using hand calculations if necessary) of the following severe accident in CANDU: small loss of coolant plus loss of ECC (assume crash cooldown is available since it is on a redundant signal) plus loss of moderator cooling. Write down the expected event sequence (based on the list below) and estimate the approximate time of:
   - reactor trip
   - start of fuel overheating
   - failure of first channel
   - core collapse
   - shield tank failure
   - containment behaviour

Only an approximate answer is sought (to do this accurately could take weeks). If you can't get the physical data in some cases, especially for the last item, use symbols to show how you would do the calculation.

2. Estimate the evolution (using hand calculations if necessary) of the following severe accident in CANDU: loss of all electrical power starting from full power. Assume there is *no electrical power* (i.e., no Class IV, no Group 1 Class III, no Group 2 Class III). Write down the expected event sequence (based on the list below) and estimate the approximate time of:
   - reactor trip
   - opening of LRVs
   - start of fuel overheating
   - failure of first channel
   - core collapse
   - shield tank failure

Only an approximate answer is sought (to do this accurately could take weeks). If you can't get the physical data in some cases, use symbols to show how you would do the calculation.

3. Go back again to the ZED-2 reactor and consider a loss of reactivity control caused by an unexpected moderator pump up. Identify as many of the key systems and parameters as you can for this accident and for each, list the 'conservative' assumptions that you would use to ensure your answer (reasonably) overestimates the consequences.

4. Consider a CANDU that has undergone a severe core damage accident. Assume that the core has collapsed into a debris bed at the bottom of the calandria and is being cooled by boiling of the shield tank water. Calculated the depth of the debris bed in the calandria

and the average heat flux through the calandria wall. You will need to look up some typical CANDU geometry. [If you're really keen, for an extra (optional) bonus mark, you can look up from *primary* sources the appropriate critical heat flux correlation from the outside of the calandria wall to the shield tank water, and compare with the actual heat flux].

## References


1. D. G. Hurst and F. C. Boyd, "Reactor Licensing and Safety Requirements", Paper 72-CNA-102, presented at the 12th. Annual Conference of the Canadian Nuclear Association, Ottawa; June, 1972.
2. "Requirements for the Safety Analysis of CANDU Nuclear Power Plants", AECB Consultative Document C-6, June 1980. This was applied to the licensing of Darlington. A revision (Rev. 1) was issued for public comment in September 1999 but is problematical as written and has not been, and will not be, applied to a new plant.
3. "Design of New Nuclear Power Plants", CNSC Report RD-337, November 2008.
4. "Safety of Nuclear Power Plants: Design", IAEA Safety Standard NS-R-1, September 2000.
5. "Requirements for Shutdown Systems for CANDU Nuclear Power Plants", AECB Regulatory Policy Statement R-8, February 1991.
6. "The Use of Two Shutdown Systems in Reactors", AECB Regulatory Policy Statement R-10, January 1977.
7. "Guidelines for Calculating Radiation Doses to the Public from a Release of Airborne Radioactive Material under Hypothetical Accident Conditions in Nuclear Reactors", CSA Standard N288.2, April 1991.
8. "Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems", AECB Regulatory Policy Statement R-77, October 1987.
9. V.G. Snell, S. Alikhan, G. Frescura, J.Q. Howieson, F. King, J.T. Rogers, and H. Tamm, "CANDU Safety Under Severe Accidents: An Overview", IAEA/OECD International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italy, March 1988. Also Atomic Energy of Canada Ltd. Report, AECL-9802.
10. C. Blahnik, et al., "Modular Accident Analysis Program for CANDU Reactors", Proc. 12th Annual Canadian Nuclear Society Conference, Saskatoon, Saskatchewan, Canada, June 9-12, 1991, p.235-242.
11. J.T. Rogers, et al., "Coolability of Severely Degraded CANDU Cores", ICHMT International Seminar on Heat and Mass Transfer in Severe Reactor Accidents, Cesme, Turkey, May 21-26, 1995. Also Atomic Energy of Canada Ltd. Report, AECL-11110.
12. L.A. Simpson, P.M. Mathew, A.P. Muzumdar, D.B. Sanderson & V.G. Snell, "Severe Accident Phenomena and Research for CANDU Reactors", Proc. of the 10th. Pacific Basin Nuclear Conference, October 20-21 1996, Kobe, Japan.

# Appendix A - Accident Classification for New Plants in Canada

This material is taken from the CNSC report RD-337, issued in November 2008.

RD-337 abandons both the single/dual failure approach (siting guide) for CANDUs licensed up to Darlington, and the Darlington 5-class approach defined in CNSC Consultative Document C-6. Instead it adopts international practice and defines three abnormal states:

*"Anticipated Operational Occurrence (AOO)*—a deviation from normal operation that is expected to occur once or several times during the operating lifetime of the NPP but which, in view of the appropriate design provisions, does not cause any significant damage to items important to safety, nor lead to accident conditions.;

*"Design Basis Accident (DBA)*—accident conditions for which an NPP is designed according to established design criteria, and for which damage to the fuel and the release of radioactive material are kept within regulated limits;and

*"Beyond Design Basis Accident (BDBA)*—accident conditions less frequent and more severe than a design basis accident. A BDBA may or may not involve core degradation."

Dose acceptance criteria are defined only for AOOs and DBAs as follows:

**Dose Acceptance Criteria**

| AOOs | DBAs |
|---|---|
| 0.5 mSv | 20.0 mSv |

Note that relative to single process system failures in the siting guide, AOOs have a lower dose acceptance criterion, and DBAs have a higher one. Basically the former category of accidents has been split into two, with the more frequent category having a lower dose acceptance criterion. Note also that there are no longer dose limits for iodine-131 and for collective dose. However the safety goals (see Chapter 6) address societal effects.

Dual failures are not treated as a separate class, but are included in the broader category of Beyond Design Basis Accidents, a subcategory of which are severe core damage accidents. Neither BDBAs nor severe accidents have dose acceptance criteria, but instead are limited by the safety goals, which give objectives and limits to their frequency and consequences (releases of key radiouclides).