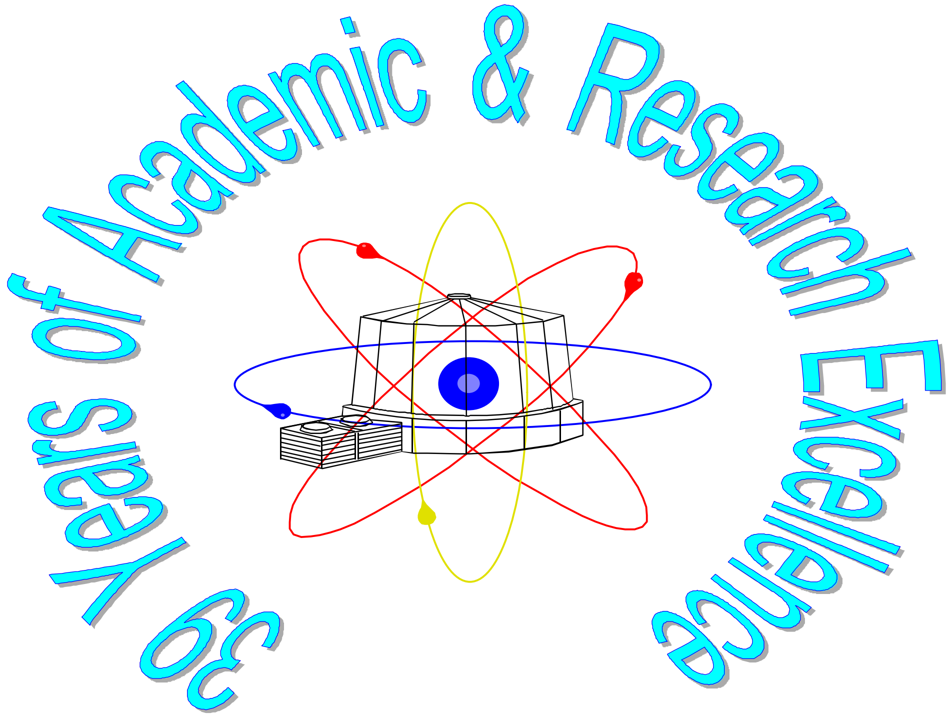
McMaster Nuclear Reactor
McMaster University
1280 Main Street West
Hamilton, Ontario   L8S 4K1

(905) 525-9140 Ext 24065
Fax: (905) 528-4339

Technical Report 1999-06

Safety Analysis Approach for the McMaster Nuclear Reactor



Prepared by: ______________________________ Date: _______________
Wm. J. Garland, Reactor Analyst

Reviewed by: ______________________________ Date: _______________
M. Butler, Chief Reactor Supervisor

Approved by: ______________________________ Date: _______________
Frank Saunders, Reactor Manager

April 21, 1999

Table of Contents:

List of Figures:

List of Tables:

Safety Analysis Approach
for the
McMaster Nuclear Reactor

1 Introduction

This document provides the approach adopted for the safety analysis section of the update of the 1972 Safety Analysis Report. It was agreed at the April 28, 1998 meeting with the AECB to follow the joint AECB - McMaster - AECL report *IAEA SRC-278* [ERNST 1989] on Canadian Small Reactor Safety Criteria and the subsequent summary paper *IAEA-SM-310/93* [ERNST 1990] as the basis of safety analysis for the McMaster Nuclear Reactor (MNR). This involves a pseudo-PSA approach.

MNR is an existing, well-established reactor with 40 years of operating history as of 1999. Margins to heat transfer crisis are much larger than that of typical power reactors. The seismically qualified building, full containment, large pool water inventory, sensitive safety shutoff rods, modest fuel inventory, metallic fuel bound fission products, robust and ductile fuel, low pressure and temperature operating conditions and large safety margins all contrive to make MNR a safe and benign facility. The current design and operation will be assessed with respect to the existing generous operational and safety limits.

To make the most of finite analysis resources, the current analysis focus is on scenario exploration in support of the revision of the Safety Analysis Report rather than the firm establishment of detailed design and analysis criteria at the outset; after all, the plant is not being designed; it exists. Thus, work will proceed to scope out (via deterministic analysis) the main scenarios that are deemed to be the largest contributors to risk and, in parallel, to prepare event trees and fault trees for these scenarios. The deterministic runs will provide timing and sequencing information that will guide the scenario development required for the event trees. Event tree and fault tree results will determine which events require further analysis. The scenarios of concern are those that lead to fuel failure and dose uptake that exceeds the dose limits specified in a later section.

2 Safety Analysis Methodology

The objective of safety analysis, in general, is to review the design and to determine if it is within safety limits. Classically, safety analysis was deterministic in approach; ie, a design should survive events A, B and C without exceeding limits X, Y and Z. This approach does not recognize the key role that probability plays in determining risk (typically defined as event consequence x event frequency).

More recently, deterministic analysis has been augmented with a probabilistic safety analysis (PSA) which recognizes that risk is a more meaningful measure for setting targets in safety analysis. Furthermore, it has been shown that there are diminishing returns in designing for events of negligible probability. The basic PSA objective can be stated quite succinctly:

> **Show that the consequences of the event are within acceptable limits**
>
> **or**
>
> **Show that the frequency of an event (normal or accident) is too incredible to consider.**

Acceptable limits are defined with respect to the event frequency. For example, frequent occurrences, like minor faults, should not stress the system or invoke protective systems. Very infrequent events, like a large loss of coolant, are permitted to push the physical systems into plastic deformation but not allow a radioactive release beyond a prescribed limit.

Incredible is defined as sufficiently low, say one in a million events per year.

The first task is to define all the possible initiating events that are deemed necessary to analyse. The range is everything from normal operation to accidents involving major core releases. These form the Design Basis Accidents or DBA. The worst conceivable accidents are to be investigated for completeness in due course but their probability is so low (by design) that they are not part of the DBA set.

Since events are classified by the frequency of occurrence, the reliability of systems has to be measured or analysed. Event scenarios, called Event Trees (ET), are developed. Each branch of the ET needs an associated probability if the event and its consequence are to be quantified. Fault trees (FT) are commonly used to determine failure probabilities.

The sequence, then, is to define the accident events to be analysed (DBA), then construct the event trees (ET) supported by the fault trees (FT) probabilities. If an event sequence is "incredible", then no further action is required (from a PSA standpoint). This constitutes a Level I analysis, that is, the analysis of event scenarios and their probability. Level II analysis calculates the source terms (radioactive releases inside and outside of containment) for those events identified in Level I that involve fuel damage or other means of radioactive release. A Level III analysis calculates the dispersion of the radioactivity and subsequent dose uptake and environmental damage. It is anticipated that there will be very few, if any, events that will require a Level II or III analysis.

Probabilistic Safety Analysis (PSA) as outlined above has proven to be very effective in ferreting out design and operation inadequacies. But it has not been completely successful on a number of fronts:

- We can only analyse events that we can conceive. What about the unknown?
- PSAs are sensitive to the choice of branch points in the cut sets of the event and fault trees and are sensitive to the measured equipment failure probability data which can often exhibit wide variability, especially for rare events and those events involving human factors.
- A full PSA requires an exhaustive analysis of even very low probability events. It is not a very practical tool in its full form.
- A strictly implemented PSA does not account for risk aversion, ie the notion that risk should decrease for accidents of increasing severity .

For power reactors, the safety criteria that have historically been used have their roots in a probabilistic approach but, for practical purposes, the criteria were deterministic in nature and were firmly founded in the principles of good engineering practice and experience. This has, in more recent years, been augmented and complemented by probabilistic analysis. Thus, actual practice has two parallel streams: the deterministic assessment path and the probabilistic path. In Deterministic Safety Analysis the acceptance criteria are not based on probability, but on a number of assumed faults. Typically a single/dual mode failure criterion is used. The acceptance criteria are more stringent for the more probable single failure and less stringent for the less probable single failure. Typically they are rooted in probabilistic arguments and are very simple to understand and to implement.

The approach used for MNR is based on the PSA methodology but is more prescriptive to address the shortcomings of PSA. As presented in [ERNST 1989], the basic safety objective is

> *“... to protect individuals, society and the environment ...”,*

from which is derived the specific risk objective, which is relevant herein,

> *“The frequencies and radiological consequences of accidents in small reactor facilities shall be within acceptable bounds.”.*

The quantitative acceptance criteria prescribe dose limits for three frequency bands as presented in the section on Level III analysis. However, before dose uptakes can be estimated, Level I and II analyses need to be performed in order to determine which events, if any, lead to releases and to determine the extent of the releases.

3 Level I Analysis

3.1 Initiating Events (IE)

There is no unique methodology to follow which will lead to the identification of all the possible events that are worthy of consideration from a safety point of view. A systematic approach, however, is more likely than not to generate the most complete and applicable list. Generally, events are pursued in a piece-wise refinement fashion, typical of the engineering approach. General categories are logically identified and are then progressively refined until specific events are reached. The general categories used to group the events are less important than the systematic nature of the process.

We identify the root category as the release of radionuclides. This could occur due to releases from the reactor core or from other on-site sources like fuel storage and isotope / waste handling. The core releases are the ones of current focus. Fission product release is identified as the main source of core releases. Fission products from the fuel can only be released if the fuel cladding is breached. This can be caused by mechanical damage or by thermal damage. Overheating can be caused by a loss of heat sink, a loss of coolant medium, flow impairment or a loss of reactor regulation, and so on. Figure 1 illustrates the event generation sequence. The figure does not include releases that do not involve the core, such as iodine, other radioisotopes handled on the experimental floor, and irradiated samples as this report focusses on core releases. Non-core releases will be studied subsequently.

3.2 Event Trees

The consequence of the various branches of the ET is set from none to large, depending on whether equipment status. The principal determiners of consequence (ie the extent of radioactivity release) are the power output, the availability of coolant and of containment. If the reactor is shutdown and both ECC and containment are available, there is no consequence. To be conservative, some small consequence is assigned to an uncovered shutdown core even though no fission products are released because a worker dose is possible. An uncovered core that is not shutdown will have significant consequences inside containment and large consequences if containment is not available. A summary is given in table 1. These consequence assignments are given only as a guide to which events to focus on in the Level II and III analyses. The event trees will be constructed initially based on the assumption of no operator intervention unless the intervention will worsen the situation.

Table 1 Consequence Assignment

Equipment Status			Consequence
Is the reactor shutdown?	Is long term ECC available?	Is containment intact?	
Don't Care	Yes	Yes	None
Yes	No	Yes	Small
No	No	Yes	Medium
No	No	No	Large

3.3 Fault Trees

Failure data for power reactors will be used to be conservative unless research reactors failure rates are available. Research reactors failure rates are significantly lower since pressures and temperatures are significantly lower than that of power reactors.

3.4 Level I Safety Criteria

No explicit criteria are offered by [ERNST 1989]. However good engineering practice dictates that there be no fuel failures during normal operation. Fuel integrity cannot be assured for sheath temperatures exceeding 450 °C and, further, flow instability and heat transfer crises lurk not too far beyond bulk boiling. Thus, useful targets to ensure fuel integrity are

- fuel sheath temperatures are not to exceed 450 °C
- no bulk boiling.

Exceeding these limits does not mean that fuel failures will occur, rather, it can be stated with some assurance that there will be no fuel failures for event scenarios that stay below those limits.

3.5 Modelling

The use of unqualified computer codes is unacceptable for licensing and safety analysis. It was agreed by all parties that the use of AECL codes where possible was the most expedient route. To support the scenario analysis, the following codes will be used:

- The commercially available computer program, FaultTree+ for fault tree and event tree analysis. This is a MS Windows based product from Item Software [ITEM 1995].
- CATHENA for thermalhydraulic analysis [CAT 1995].
- WIMS-AECL and 3DDT for reactor physics analysis.

The sub-channel code, ASSERT, will be used only if and when necessary. ASSERT is not needed for plate fuel since there are no sub-channels in plate fuel assemblies.

4 Level II Analysis

4.1 Inventory Modelling

The computer code SCALE 4.3 [CCC-545] will be used for estimating the fission product inventory in the fuel. Other codes for fuel damage and radioactivity release will be used as appropriate.

4.2 Fuel characteristics

MNR fuel is an U-Al metal alloy clad in Al. Because the metal alloy is contiguous, fission products do not migrate as they do in UO_2 fuel. Consequently, only the fission products in the immediate vicinity of damaged clad can be released. It has been demonstrated that the fission product detectors for noble gases are sufficiently sensitive to be able to detected a pin hole in the fuel clad. In addition, it has been shown that fission product releases stopped immediately upon shutdown.

4.3 Level II Safety Criteria

There are no safety criteria relevant to this level of analysis.

5 Level III Analysis

5.1 Dose Uptake Modelling

Discussion on a pathways analysis is beyond the scope of this document and is addressed elsewhere.

5.2 Level III Criteria

From [ERNST 1989], the following dose limits are adopted.

Table 2 Individual dose.

Dose to most exposed individual		
Frequency range	Dose Band	Example of Accident
3 x 10^{-1} to 3 x 10^{-2} / year	0.1 mSv to 0.5 mSv	Failure in experiment
3 x 10^{-2} to 10^{-4} / year	0.5 mSv to 5 mSv	Accident terminated by safety system
10^{-4} to 10^{-6} / year	5 mSv to100 mSv	Accident mitigated by pool / building

Table 3 Collective dose.

Collective dose	
Frequency range	Dose Band
3 x 10^{-1} to 3 x 10^{-2} / year	0.1 person-Sv to 1 person-Sv
3 x 10^{-2} to 10^{-4} / year	1 person-Sv to 10 person-Sv
10^{-4} to 10^{-6} / year	10 person-Sv to 100 person-Sv

6 Conclusion

The safety criteria developed for small reactors in Canada has been applied to the McMaster Research Reactor and the criteria have been cast in the context of Level I, II and III analysis.

References

CAT 1995 -, "CATHENA MOD-3.5 / Rev 0, Theoretical Manual", Atomic Energy of Canada Limited, ed. B.N. Hanna, RC-982-3, 1995.

CCC-545 -, "SCALE 4.3, Modular Code System for Performing Standardized Computer Analyses for Licensing Evaluation for Workstations and Personal Computers", RSIC Computer Code Collection, Oak Ridge National Laboratories, Oak Ridge Tennessee, 1995.

ERNST 1989 P.C. Ernst, P.M. French, D.J. Axford, V.G. Snell, "Development of Small Reactor Safety Criteria in Canada", International Symposium of Research Reactor Safety, Operations and Modifications, Chalk River, Ontario, Canada, 23-27 October 1989, IAEA-SM-310/93.

ERNST 1990 P.C. Ernst, P.M. French, D.J. Axford, V.G. Snell, "Canadian Small Reactor Safety Criteria", draft report 4, April 16, 1990, IAEA SRC-278.

ITEM 1995 FaultTree+ for Windows 6.05, "Fault and Event Tree Analysis Program", Item Software (USA) Inc., 1995.

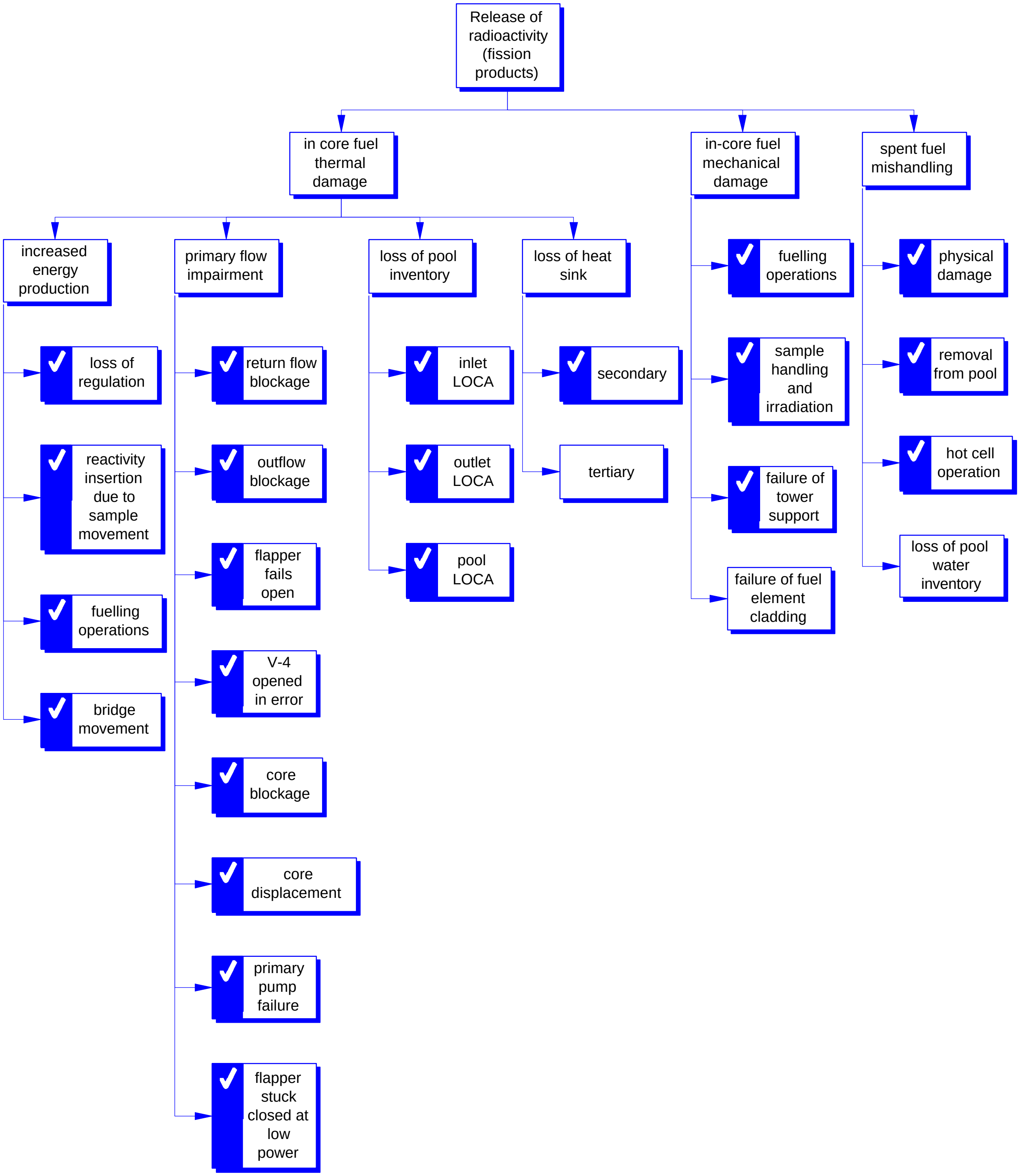


Figure 1 Initiating Events