Safety Reports Series
No.29

Accident Analysis for Nuclear Power Plants with Pressurized Heavy Water Reactors

IAEA
International Atomic Energy Agency

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www-ns.iaea.org/standards/

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series,** the **INSAG Series, the TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

ACCIDENT ANALYSIS FOR NUCLEAR POWER PLANTS WITH PRESSURIZED HEAVY WATER REACTORS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA AND MONTENEGRO
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

Printed by the IAEA in Austria
November 2003
STI/PUB/1161

SAFETY REPORTS SERIES No. 29

ACCIDENT ANALYSIS FOR NUCLEAR POWER PLANTS WITH PRESSURIZED HEAVY WATER REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2003

IAEA Library Cataloguing in Publication Data

Accident analysis for nuclear power plants with pressurized heavy water reactors. — Vienna : International Atomic Energy Agency, 2003.
p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 29)
STI/PUB/1161
ISBN 92–0–110503–7
Includes bibliographical references.

1. Heavy water reactors. 2. Nuclear power plants — Accidents. I. International Atomic Energy Agency. II. Series.

IAEAL 03–00334

FOREWORD

Deterministic safety analysis (frequently referred to as accident analysis) is an important tool for confirming the adequacy and efficiency of provisions within the defence in depth concept for the safety of nuclear power plants (NPPs). Owing to the close interrelationship between accident analysis and safety, an analysis that lacks consistency, is incomplete or of poor quality is considered to be a safety issue for a given NPP. Developing IAEA guidance publications for accident analysis is thus an important step towards resolving this issue.

Requirements and guidance pertaining to the scope and content of accident analysis have, in the past, been partially described in various IAEA reports. Several guidance documents relevant to water moderated, water cooled power reactors (WWERs) and high power boiling reactors with pressurized channels of Russian design known as RBMKs have been developed within the IAEA's Extra-budgetary Programme on the Safety of WWER and RBMK Nuclear Power Plants. To a certain extent, accident analysis is also covered in several publications of the revised NUSS Series, for example, in the Safety Requirements on Safety of Nuclear Power Plants: Design (NS-R-1) and in the Safety Guide on Safety Assessment and Verification for Nuclear Power Plants (NS-G-1.2). For consistency with these publications, the IAEA has developed a series of Safety Reports on Accident Analysis for Nuclear Power Plants. Many experts have contributed to the development of these Safety Reports. In addition to several consultants' meetings, comments were collected from more than fifty selected organizations. These reports were also reviewed at the IAEA Technical Committee Meeting on Accident Analysis held in Vienna from 30 August to 3 September 1999.

These Safety Reports aim to provide practical guidance for performing accident analysis. The guidance is based on present good practice worldwide. The reports cover all the steps required for accident analyses, i.e. selection of initiating events and acceptance criteria, selection of computer codes and modelling assumptions, preparation of input data and presentation of the calculation results. The reports also discuss the various aspects that need to be considered to ensure that an accident analysis is of acceptable quality.

The first volume of the series is intended to be as generally applicable as possible to all reactor types. The specific features of individual reactor types are taken into account in the subsequent reports in the series. The reactor types to be covered include pressurized water reactors (PWRs), boiling water reactors (BWRs), pressurized heavy water reactors (PHWRs) or more specifically PHWRs of Canadian design known as CANDU, and RBMKs. The present report is devoted to specific guidance for PHWRs.

The report is intended for use primarily by analysts co-ordinating, performing or reviewing accident analysis for NPPs, on both the utility and the regulatory sides. The report will also be used as a background publication for relevant IAEA activities, such as training courses and workshops.

The IAEA staff member responsible for this publication was J. Mišák of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Consistent with the Safety Standards Series, in particular with the Safety Requirements on Safety of Nuclear Power Plants: Design [1] and the Safety Guide on Safety Assessment and Verification [2], the IAEA has developed a Safety Report, Accident Analysis for Nuclear Power Plants, which contains a comprehensive description of the general methodology for accident analysis [3]. The objective of that Safety Report is to establish a set of practical suggestions based on the best practice worldwide for performing accident analysis for nuclear power plants (NPPs). The following items are covered in that report:

(1) Classification of initiating events and acceptance criteria;
(2) Methodology used for the analysis;
(3) Types of accident analysis;
(4) Computer codes;
(5) User effects on the analysis;
(6) Input data preparation;
(7) Presentation and evaluation of results;
(8) Quality assurance.

Annexes to Ref. [3] provide examples of the practical application of accident analyses; they specify and characterize the main steps in performing accident analysis, provide more discussion on and examples of uncertainty analysis, give a practical example of the preparation of input data for analysis and of the production of the corresponding documents. The annexes also contain references to the typical computer codes, provide an extensive list of codes for accident analysis and include explanations of the technical terms used in the main report and its appendices. That Safety Report is general in nature and does not focus exclusively on any single reactor type.

More specific guidance on performing accident analysis depends on the characteristics of the NPP in question and can only be developed for specific reactor designs or, in a more general manner, for a group of reactor designs. Such design specific guidance documents are being developed as separate Safety Reports. The reactor types to be covered include pressurized water reactors (PWRs), boiling water reactors (BWRs), pressurized heavy water reactors (PHWRs) or, more specifically, PHWRs of Canadian design known as CANDUs, and high power boiling reactors with pressurized channels (of Russian design) known as RBMKs.

1.2. OBJECTIVE

The objective of the present report is to provide specific guidance for accident analysis for NPPs with PHWRs, taking into account the specific design features of these reactors. There are a number of differences among the various PHWR designs and currently operating plants. To the extent possible, the present report is applicable to the whole variety of these designs.

The process by which initiating events are selected is first discussed. 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 the high level acceptance criteria used in the most recent CANDUs. The technical capabilities that computer codes used in PHWR safety analysis should possess are 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 PHWR 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 suggestions on what results should be reported for various types of accidents.

This Safety Report, as with the other reports in the series, is not intended to usurp the prerogative of national regulatory organizations to change or set safety analysis requirements. It summarizes information from the most recent safety analysis of CANDU, and is based on practices in several countries.

The report is mostly based on the experience of the experts involved, with considerable use of other relevant documents [4–12].

1.3. SCOPE

In a similar way to the first report in this series, Ref. [3], this PHWR specific volume also deals only with 'internal' events originating in the reactor or in its associated process systems. It does not cover originating events affecting broad areas of the plant (often called internal and external hazards), such as fires, floods (internal and external), earthquakes and aircraft crashes. However, analysis of the consequences of these events from a thermohydraulic point of view is partially covered by the present guidance. The emphasis in this guidance is on the transient behaviour of the reactor and its systems, including the containment and/or confinement.

The main focus of the analyses is towards the thermohydraulic aspects of the transients considered. The neutronic and radiological aspects are also covered to some extent. Limited consideration is given to structural (mechanical) aspects.

The report deals with the usual approach to accident analysis adopted for present CANDU reactors. This means that the use of best estimate computer codes and tools is encouraged in such a way that sufficient safety margins are ensured by means of a conservative selection of initiating events and their combinations, and specifying conservative plant input data for analysis.

The information provided by this report is intended primarily for code users performing accident analysis. Regulatory bodies are encouraged to use the report as the basis for their national requirements. Analysts may also use the report as a reference for contacts with the national regulatory body or for the formulation of detailed company procedures for analysts.

This report in the series, along with all the other design specific reports, is intended to be, to a large extent, a self-standing publication. Nevertheless, to avoid repetition of suggestions included already in the general guidance, it is advisable for users to initially read the first Safety Report in the series, Ref. [3], before using any of the design specific guidance reports.

1.4. STRUCTURE

The structure of the present report is consistent with that of the first Safety Report in the series, Ref. [3]. Naturally, the content of the sections and the level of detail take into account the design specific features of PHWRs. Whenever considered to be important, reference is made to the general guidance given in Ref. [3]. In addition to this introductory section, there are eight sections in this report.

Section 2 introduces the specific PHWR philosophy for systematic selection of initiating events for analysis and their categorization by frequency of occurrence. A grouping of the initiating events in terms of the major phenomena is presented in Section 3. In Section 4, the acceptance criteria for accident analysis applicable for PHWRs are introduced in general terms. Specific criteria applicable for different initiating events are presented in Section 7. Since setting up acceptance criteria rests with national regulatory authorities, the criteria provided in this report can be understood only as examples.

Requirements on the comprehensiveness of the various computer codes needed for analysis of PHWRs are discussed in Section 5. Reference is made to Ref. [3], where the main computer codes are introduced individually.

A number of key parameters important to ensure sufficient safety margins in analysis are presented in Section 6. These parameters include core property parameters, plant initial conditions, system performance characteristics and assumptions about the unavailability of systems. Suggestions are

provided in relation to how the various key parameters should be specified for the best estimate code input decks to ensure conservative analysis results.

More detailed suggestions for analysis of different initiating events are described in Section 7. For each of the events (group of events) its safety aspects, relevant acceptance criteria and event combinations are identified and some specific suggestions for analysis are formulated. Section 8 deals specifically with severe accidents for PHWRs.

Section 9 provides a list of the calculated parameters to be reported from the results of analyses of different accident scenarios.

2. SELECTION OF INITIATING EVENTS

A requirement of the safety analysis of all reactor designs is to demonstrate that the set of initiating events to be analysed within the 'design basis' is sufficiently complete. For PHWRs, guidance is provided by past practice, by operating experience and by regulatory documents, but the onus is on the licensee to prove completeness. A number of tools are available to identify initiating events.

PHWRs that were licensed up to the Darlington station in Canada used the 'single-dual' failure philosophy. A safety analysis would be performed for the failure of each process system[1] in the plant; then one would be performed for each such failure combined with the unavailability or impairment of each special safety system in turn (shutdown system No. 1 (SDS1), SDS2, containment and emergency core cooling (ECC)). This approach was comprehensive. Failures in the safety support systems (such as the instrument air system) 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 regulatory guide C-006, Ref. [4], used on a trial basis in the licensing of Darlington and now the de facto requirement for safety analysis of new designs. This guide 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.

[1] See Glossary in Ref. [3] for an explanation of terms.

A number of techniques are used in the systematic evaluation. Lists of initiating events can be compiled by listing 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 PSA method (the so-called 'bottom-up' method). Another method is to determine all sources of radioactivity in the plant and postulate failures that would cause them to be relocated (the '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 and aircraft crashes. Generally these are addressed in the design by 'hardening' or separating essential systems, or by the choice of siting, so that a safety analysis is not required. Some accidents are combined with external events on the basis of probability. For example, a loss of coolant accident (LOCA) is assumed to be followed 24 hours later by a site design earthquake (SDE) — an earthquake with a return frequency of 1 per 100 years, and hence of a lower intensity and higher frequency than the design basis earthquake). While in principle this event combination could require safety analysis, in practice it is addressed by qualifying the appropriate portions of the plant.

Very rare events include failure of pressure vessels (e.g. pressurizer and steam generator shell), failure of structural supports and turbine break-up. Pressure vessel and structural failures are precluded in the design by use of, for example, the appropriate level of design and manufacturing codes and standards, quality assurance and in-service inspection. Again, safety analysis is not required.

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

3. CATEGORIZATION OF INITIATING EVENTS

In the previous section categorization of initiating events by frequency of occurrence was discussed. Initiating events can also be grouped in terms of the major phenomena, as follows:

(a) Reactivity accidents:
- Bulk loss of reactivity control (LORC);
- Loss of reactivity control from distorted flux shapes.

(b) Decrease of reactor coolant flow:
  — Loss of Class IV power;
  — Partial loss of Class IV power;
  — Single pump trip or seizure.
(c) Increase of reactor coolant pressure:
  — Loss of primary pressure and inventory control (increase).
(d) 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).
(e) Increase of secondary side pressure:
  — Loss of secondary side pressure control (increase).
(f) 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.
(g) Moderator and shield cooling system failures:
  — Pipe break;
  — Loss of forced circulation;
  — Loss of heat removal.

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

4. ACCEPTANCE CRITERIA

Once the intiating events are identified, and put into one of the five event classes described in Ref. [4], the safety analysis must show that the resulting dose to the public meets the dose limit for the event class (Fig. 1). As noted in Ref. [3], the approach for PHWRs has been to use best estimate physical models combined with conservative values of the key input parameters to give a

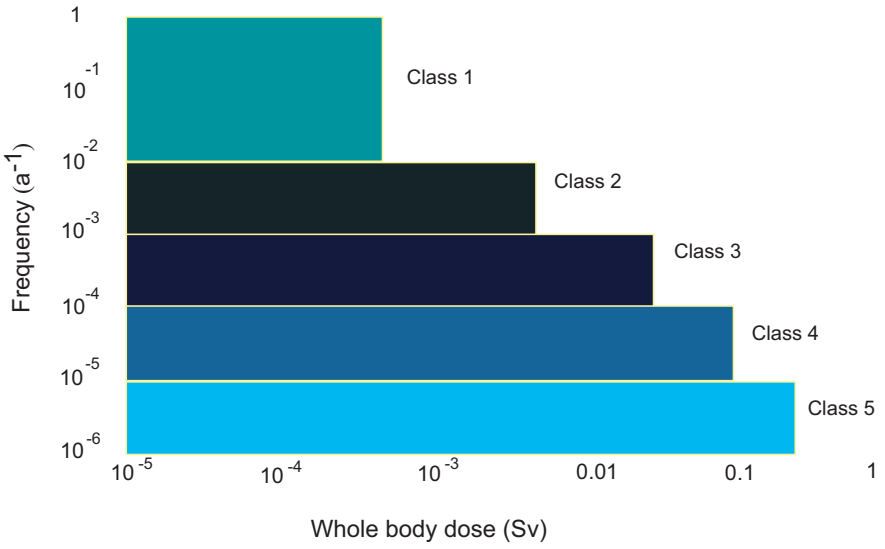

FIG. 1. Dose limits for different event classes (AECB Consultative Document: C-006) [4].

conservative, but physically reasonable, prediction of accidents. The models start from the reactor physics and then progress through the system thermohydraulics, fuel and fuel channel response, moderator and containment response, and end with the atmospheric dispersion and dose. The release of fission products to the containment, the containment pressure transient, the resulting leakage of radionuclides from containment, the dilution by atmospheric dispersion and the effects of ground deposition, and the dose to the public are all predicted using realistic physical models and conservative input data or system assumptions.

Common practice is that accidents with a frequency of about 10^{-6} a^{-1} or larger are part of the design basis, subject to regulatory limits on public dose; in practical terms they are shown to stop short of severe core damage. The design basis set includes low probability sequences where the fuel can be severely damaged, such as LOCA plus loss of emergency core cooling (LO ECC), but where the moderator arrests the damage at the channel boundary. One can think of such sequences as a severe accident[2] contained within the channel

[2] Specifically defined for PHWRs as an accident where there is no heat removal by water in the fuel channels. There will be severe fuel damage but, depending on the availability of the moderator as a backup heat sink, there may or may not be severe core damage. See Section 8.

boundary which does not progress to severe core damage[3]. Severe core damage sequences are covered in more detail in Section 8.

Public dose is the primary acceptance criterion. Designers also define subsidiary criteria, which are intended to be 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, adopted or disputed by the regulator; some are specified in regulatory documents. The subsidiary acceptance criteria defined by the designers are discussed in Section 7 for each individual accident type.

Shutdown systems have a separate acceptance criterion. Modern PHWRs have two independent, redundant and diverse shutdown systems with separate logic and reactivity devices from the control system and from each other [5]. Each system, on its own, must be capable of shutting the reactor down after any accident, independently of the mitigation provided by the normal reactivity control devices. In general, two diverse trip parameters are required on each shutdown system for each accident over the range of operating conditions (unless it is impracticable or detrimental to safety to provide dual parameter coverage). As a result, it is not required to perform analysis of either transients or accidents without shutdown [6].

5. MAJOR COMPUTER ANALYSIS TOOLS REQUIRED FOR DBAs

PHWR safety analysis requires a comprehensive set of physical models. Reactor physics analysis may require a transient three dimensional model for the large PHWR cores. The most demanding application is a large LOCA, because of the relatively fast kinetics and the spatial effects associated with flux tilts and shut-off rod (or liquid absorber) insertion. Three dimensional effects are also important in slow loss of reactivity control starting from distorted flux shapes.

The system thermohydraulic code is typically a two fluid, one dimensional non-equilibrium network code. The non-equilibrium aspect is important in modelling rewet and refill of the channels, since the flow can be stratified during that time. Recent practice has been to incorporate the reactor physics calculation into the system thermohydraulic code for a large LOCA, since the voiding transient determines the power pulse, which in turn has a second order

[3] Defined as loss of the channel geometry in the calandria. See Section 8.

effect on the voiding transient. However, convergence is quite fast so that iterative, decoupled calculations are acceptable.

Fuel thermomechanical models consist of a code for normal operation, which predicts the initial fuel conditions before an accident (strain, fuel-to-sheath heat transfer coefficient, gas release, initial temperatures, etc.), and a transient thermomechanical code for accidents. The latter includes submodels 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 emergency core coolant 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 thermomechanical 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 thermomechanical models have been used to-date, using somewhat artificial boundary conditions (fixed steam flow rate); the system thermohydraulic codes now incorporate this capability, allowing more realistic predictions of the distribution of flow to each channel.

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 widespread film boiling does not develop. 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 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 PHWR 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 that could be included. However, the partitioning of fission products between steam and water phases at the break, and within containment, has been modelled, as have 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 submodels 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. Multinode two or three fluid one dimensional containment models have been used for this analysis; recently three dimensional containment models have been applied to study the local distribution of hydrogen after a LOCA + LO ECC.

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 the worst weather occurring more than 10% of the time at the site. Exposure-to-dose calculations use standard ICRP recommended conversion factors.

Typical computer codes used in safety analysis are listed in Annex IV of Ref. [3].

6. ANALYSIS ASSUMPTIONS

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 for a parameter; 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). However, since many parameters are chosen in a similar way for many accidents, the most common choices, along with a simplified rationale for these, are listed in Table I.

In general, any mitigating process system action is not credited in demonstrating the effectiveness of special safety systems. However, if a process system action is expected to occur, and would worsen the accident consequences, it should be included.

TABLE I. KEY SAFETY ANALYSIS PARAMETERS

Item	Conservative direction	Rationale
Reactor thermal power	High	Minimize time to use up cooling water inventory, minimize margins to critical heat flux, etc.
Reactor regulating system	Normal operation or inactive, whichever is worse; a set-back 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) and end-of-life tritium concentration	Maximize radionuclide release from station and public dose.
Steam generators	Clean and fouled cases	Reduce reactor trip effectiveness.
Steam generator tube leak rate	Maximum permitted during operation, plus assessment of any consequential effects due to an accident	Increase radioactivity release.
HTS flow	Low	Reduce margins to critical heat flux.
Instrumented channel flow	High	Reduce low flow trip effectiveness.
Coolant void reactivity coefficient	High Low	Maximize overpower transient. Delay HTS high pressure trip.
Fuel loading	Equilibrium	Maximize fuel temperatures and radioactivity releases.
	Fresh	Maximize overpower transient.
Shutdown system	Backup trip on least 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 shut-off rods	Two most effective rods unavailable	Reduce shutdown system reactivity depth.

TABLE I. (cont.)

Item	Conservative direction	Rationale
Maximum channel/bundle power	High	Maximize fuel and sheath temperatures.
Reactor decay power	High	Minimize time to use up cooling water inventory.
Initial flux tilt	High	Maximize fuel and sheath temperatures.
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.
Number of dousing spray headers	Low (typically four out of six)	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 2× to 10× design leak rate)	Maximize public dose.
	Low	Maximize containment pressure.
Containment bypass leakage	Pre-existing steam generator tube leak	Maximize public dose.
Weather	Least dispersive weather occurring >10% of the time	Maximize public dose.

TABLE I. (cont.)

Item	Conservative direction	Rationale
Operator actions	Not credited before 15 min after a clear indication of the event, for actions that can be carried out from the control room; and not credited before 30 min 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 in Section 7.

7. TYPICAL INITIATING EVENTS

This section summarizes typical initiating events for PHWRs, indicating safety issues of interest and any key safety parameters not already covered in Table I, acceptance criteria used by designers and/or required by the regulator, and relevant event combinations. Because there are a number of different PHWR 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. There is also a practical limitation on the amount of detail that can be presented in this report on acceptance criteria and key safety parameters for which the individual plant safety analysis 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.

7.1. LARGE HEAT TRANSPORT SYSTEM LOCA

7.1.1. Initiating events

A large LOCA in a PHWR may be 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 CANDUs — hence the probability of a pipe break drops by about two to three orders of magnitude for break areas exceeding twice the cross-section of the largest feeder pipe. Thus, any 'large LOCA' can only be located in the large piping above the core, and is analysed separately from small LOCAs. Limiting break sizes are usually considered to obtain at three representative locations: at the reactor inlet header (RIH), the reactor outlet header (ROH) and the pump suction line[4]. Other locations are on lines connected to the pressurizer and the header interconnection 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.

7.1.2. Safety aspects

The safety aspects associated with this kind of accident are as follows:

(a) 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.
(b) Voiding of the channels, and decrease in the flow in the downstream core pass. Normally break size is treated as a parameter to find the break with the most severe and prolonged low flow (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. For intermediate sized breaks, the potential for prolonged fuel sheath dryout prior to reactor trip should also be considered.
(c) Continued fuel heat-up after reactor trip, as the channels continue to empty prior to emergency core coolant 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.
(d) For critical breaks, a number of pressure tubes may overheat, sag or strain into contact with the surrounding calandria tube.
(e) Heat transfer to the moderator from any channels with pressure tube/calandria tube contact, so that further channel deformation is prevented.

[4] For the Bruce plant (Canada), pump discharge breaks are also considered because there are two core passes connected to each pump.

(f) Containment pressure increase, and differential pressures within containment compartments.
(g) Leakage of radionuclides from containment and the resulting public dose.

7.1.3. Acceptance criteria

The following acceptance criteria apply:

(1) Dose to the most exposed individual in the critical group is below the Event Class 3 limit in Fig. 1.
(2) Pipe whip is limited so that:
  (i) There is no impairment of either of the shutdown systems below their minimal allowable performance standards.
  (ii) There is no break induced in the piping of the other loop (for two loop plants).
  (iii) There is no shearing off of large numbers of feeder pipes.
  (iv) There is no damage to the containment boundary.
  (v) 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:
  (i) The amount of fuel sheath oxidation must not embrittle the sheaths on rewet to maintain fuel integrity.
  (ii) The amount of sheath strain must be limited so that coolant can flow through the channel.
(4) Channel integrity is maintained.
  Sufficient conditions include:
  (i) There is no fuel melting.
  (ii) There is no sheath melting.
  (iii) There is no constrained axial expansion of the fuel string.
  For cases where the pressure tube strains or sags, it is sufficient if:
  (iv) 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.
  (v) 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 the containment is below the design pressure.
(6) Pressure within containment compartments does not cause internal structural failures.

7.1.4. Relevant event combinations

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

The following ECC system impairments are analysed in turn: failure of injection, failure of loop isolation and failure of steam generator secondary side 'crash' cooldown[5]. The first case is generally limiting.

The combination of a large LOCA with a loss of ECC gives rise to additional or changed safety aspects from those listed in Section 7.1.2, as follows:

(a) The moderator is required to remove reactor decay heat in the long term.
(b) Hydrogen is produced by oxidation of the fuel sheaths and part of the pressure tube, and then released to containment.
(c) Since emergency core coolant injection 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 + LO ECC calculation is highly sensitive to the assumed steam flow rate in the channel (the worst case being a few grams per second per channel); thus the imposed channel flow rate is a key safety parameter which is varied parametrically.

Similarly LOCA + LO ECC has additional or changed acceptance criteria from those listed in Section 7.1.3 as follows:

(1) Acceptance criterion (1) becomes: Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Fig. 1.
(2) 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.
(3) Acceptance criteria (2), (4), (5) and (6) apply to this event as written.
(4) Gross UO_2 melting does not occur. This is a necessary condition to preserve channel integrity.
(5) Hydrogen detonation within containment does not occur; if hydrogen combustion occurs, the pressure stays below the design pressure. As a sufficient condition, one can require that the concentration of hydrogen

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

inside containment remain below the lower limit for downward flame propagation.

The following containment system impairments are analysed in turn: loss of air coolers, loss of dousing, open ventilation dampers, deflated airlock door seals and open airlock doors. In Canada, where four multi-unit stations have vacuum containment, 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; and failure of one bank of self-actuating containment pressure relief valves. These failure combinations will not, however, be discussed in detail in this report since no stations outside Canada have this type of containment.

The combination of a large LOCA with containment system impairment gives rise to additional or changed safety aspects from those listed in Section 7.1.2 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 the associated fission product release.

Similarly, LOCA + impaired containment has additional or changed acceptance criteria from those listed in Section 7.1.3 as follows:

— Acceptance criterion (1) becomes: Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Fig. 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 are also analysed assuming failure of normal AC electric 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 are usually matters of degree: the pump rundown is faster, the critical break size shifts, secondary side cooling is reduced, the flow in the intact loop is smaller and the moderator cooldown is slower. Acceptance criteria relative to those of Section 7.1.3 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 Fig. 1.

In this report, the classification of event combinations involving an induced loss of Class IV power assumes a reasonably reliable electric grid, 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.

7.2. SMALL HEAT TRANSPORT SYSTEM LOCA

In this and subsequent sections, the differences from the large LOCA section (7.1) are highlighted. Common material is not duplicated.

7.2.1. Initiating events

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 (LRV) is included in this category. Events affecting a single reactor fuel channel or one or more steam generator tubes also involve small breaks, but because of their specific phenomenology are covered separately.

7.2.2. Safety aspects

Safety aspects are as follows:

(a) Potential for fuel sheath dryout at high power as the circuit depressurizes.
(b) Potential for fuel sheath dryout or pressure tube local overheating at decay power prior to emergency core coolant 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.
(c) Fuel cooling in the long term without forced circulation. For two loop reactors, cooling of the 'intact' loop must also be analysed because it will be isolated from the other loop and operate with reduced inventory until it is refilled by emergency core coolant.

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: that with the RRS inactive and that with the RRS operating normally.

7.2.3. Acceptance criteria

The following acceptance criteria apply:

(1) Dose to the most exposed individual in the critical group is below the Event Class 2 limit in Fig. 1.

(2) There should be no systematic fuel failures. Systematic fuel failures mean that some fuel elements initially operating within the allowed operating limits are predicted to have a high probability of failure when subject to the event transient. This does not include fuel with an incipient defect that might fail due to the stresses caused by the event. Prevention of significant fuel failure is sufficient but not necessary to meet the dose limit; it also reduces the economic risk of a small LOCA. There are two periods of interest: at high power (before reactor trip) and at low power (due to prolonged dry-out at low flows). The fuel sheath will remain intact if:

(i) There is no fuel centreline melting (centreline temperature lower than 2840°C).

(ii) There is no excessive strain (uniform sheath strain less than 5% for temperatures lower than 1000°C).

(iii) There are no significant cracks in the surface oxide (uniform sheath strain less than 2% for temperatures higher than 1000°C).

(iv) There is no oxygen embrittlement (oxygen concentration less than 0.5% by weight over half the sheath thickness).

(v) There is no penetration by the beryllium braze at spacer and bearing pad locations.

Various times at the temperature limits can be used as a conservative surrogate for these physical requirements.

(3) Criteria (4), (5) and (6) listed in Section 7.1.3 also apply.

7.2.4. 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 are also analysed assuming failure of Class IV power. Safety aspects are generally similar to the cases with Class IV power available.

As with large LOCAs, differences are usually matters of degree: the most important safety aspect is ensuring sufficient buoyancy driven flow in both loops to maintain channel integrity. Acceptance criteria are changed relative to those identified in Section 7.2.3 as follows:

(a) Acceptance criterion (1) becomes: Dose to the most exposed individual in the critical group is below the Event Class 4 limit in Fig. 1.
(b) 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.

7.3. SINGLE CHANNEL EVENTS

7.3.1. Initiating events

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

(a) A 'spontaneous' pressure tube rupture, assumed for the purpose of analysis to result also in rupture of the calandria tube.
(b) A break in an individual feeder pipe. A special case is a break in an inlet feeder of exactly the correct size to temporarily cause the flow in the channel to stagnate. This can then result in channel overheating and failure.
(c) Failure of the end-fitting attached to the pressure tube, and assumed ejection of the fuel.
(d) Blockage of the flow in a channel, assumed to be complete enough to cause channel overheating and failure.

7.3.2. 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 incore breaks:

(a) The potential for damage to in-core components such as reactivity mechanisms. The worse case is LOCA with LO ECC (since the ECC utilizes light water and introduces negative reactivity).
(b) The potential for propagation of the break to other reactor fuel channels.
(c) Calandria overpressure due to the discharge of high enthalpy fluid into the moderator.

(d) For the case of flow blockage or critical inlet feeder break, calandria over-pressure due to the interaction of hot and possibly molten fuel with the moderator.
(e) Safety system initiation signals (since a high building pressure may not be effective for an in-core break).
(f) 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.
(g) Fission product washout in the moderator.

For in-core breaks, given the potential for damage to shut-off rod guide tubes and the displacement of moderator poison, a number of assumptions are made to maximize net reactivity (Table II).

7.3.3. Acceptance criteria

The following acceptance criteria apply:

(1) The small LOCA acceptance criteria identified in Section 7.2.3 apply. However, fuel damage may occur in the affected channel.
(2) A safe shutdown state is maintained. Manual action may be credited in the long term to supplement the shutdown system reactivity.
(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.

7.3.4. 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.

TABLE II. CONSERVATIVE SELECTION OF PARAMETERS TO MAXIMIZE NET REACTIVITY

Item	Conservative direction	Rationale
Initial reactor operating state	Startup after a long shutdown	Maximize reactivity due to decay of neutron absorbers in the fuel.
Fuel burnup	Plutonium peak	Maximize reactivity due to fuel.
Moderator poison load	High	Maximize reactivity due to displaced moderator.
Coolant isotopic purity	High	Maximize reactivity due to moderator displacement.
Failed channel location	Near most effective shut-off rods	Maximize loss of shut-off rod reactivity.

7.4. SINGLE STEAM GENERATOR TUBE RUPTURE

7.4.1. Initiating events

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

7.4.2. Safety aspects

The safety aspects are similar to those of a leak[6] as far as the reactor HTS is concerned, but also include:

(a) Release of the radionuclides contained in the HTS coolant outside containment.
(b) The break must be isolated in the long term, since the loss of water through the steam generator is unrecoverable.

The analysis focuses on ensuring there is adequate operator action time to perform cooldown and isolation. Back-flow of (light) water from the secondary side to the primary side, after the latter has cooled down and depressurized, causes negative reactivity and is not a safety concern.

[6] A leak is defined as a loss of coolant small enough that it can be compensated for by the D_2O make-up system; ECC is not required.

7.4.3. Acceptance criteria

The acceptance criteria are generally the same as those of a small LOCA. In some jurisdictions the event class has been specified as Class 1 by the regulator but the designers have made a case for Class 2.

7.4.4. 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.

7.5. MULTIPLE STEAM GENERATOR TUBE FAILURE

7.5.1. Initiating event

It is postulated that a number of steam generator tubes fail simultaneously.

7.5.2. Safety aspects

Relevant safety aspects are as follows:

(a) The effect on the HTS is similar to that of a small break.
(b) As with a single steam generator tube rupture, there is a discharge of radionuclides outside the containment.
(c) The accident timescale is much shorter than for a single steam generator tube rupture, so automatic action of the shutdown systems and of the ECC is required.
(d) The operator is required in the long term to open the valve to an alternative heat sink and stop further discharge outside containment.

7.5.3. Acceptance criteria

The following acceptance criteria apply:

(1) Dose to the most exposed individual in the critical group satisfies the limits in Fig. 1. As with a single steam generator tube rupture, there is a

discussion in some jurisdictions on event classification, with the regulator using Class 3 and the designer proposing Class 5.

(2) The fuel channels should not fail due to overheating.

7.5.4. Relevant event combinations

None.

7.6. LOSS OF FORCED CIRCULATION

7.6.1. Initiating events

A loss of Class IV electric 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.

7.6.2. Safety aspects

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.

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.

7.6.3. Acceptance criteria

The following acceptance criteria apply:

(1) Dose to the most exposed individual in the critical group is below the limits listed below:

(i) Loss of Class IV power: Event Class 1 limit in Fig. 1;
(ii) Pump seizure: Event Class 2 limit in Fig. 1.

(2) The heat transport system must remain intact. Thus it must not fail due to:

(i) Overpressure;

(ii) Overheating of the pressure tubes.

(3) For loss of Class IV power and single pump trips, the service limit for SDS1 high pressure trips is ASME Level B (upset) crediting the LRVs. The service limit for SDS2 high pressure trip is ASME Level C (emergency) both with and without the LRVs being credited. The first trip parameter may be credited in the case where this trip parameter is high pressure, Ref. [8].
(4) For single pump seizure, the service limit for SDS1 high pressure trip is ASME Level C (emergency), the LRVs being credited. The service limit for SDS2 high pressure trip is ASME Level D (faulted) both with and without the LRVs being credited. The first trip parameter may be credited in the case where this trip parameter is high pressure.
(5) Systematic fuel failures are prevented[7]. It is sufficient to prevent prolonged periods in dry-out or in stratified flow before reactor trip.

7.6.4. Relevant event combinations

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

7.7. LOSS OF REACTIVITY CONTROL

7.7.1. Initiating events

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

7.7.2. Safety aspects

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

---

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

Reactivity ramps from malfunctions in the RRS or its components are inherently slower than those caused by a LOCA. Since major LOCAs determine the set points of the bulk overpower and the rate trips on each shutdown system, LORC 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 set point. Analysis of such events determines the trip set points for the spatially distributed regional overpower (ROP) flux detectors on each shutdown system.

The set-back and step-back 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 analysed:

— 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, for example operation with a stuck absorber rod.

7.7.3. Acceptance criteria

Similar to the loss of forced circulation case, the acceptance criteria are as follows:

(1) Dose to the most exposed individual in the critical group is below the Event Class 1 limit in Fig. 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 LRVs. The service limit for SDS2 high pressure trip is ASME Level C (emergency) both with and without the LRVs being credited.
(4) Systematic fuel failures are prevented. It is sufficient to prevent prolonged periods in dryout or in stratified flow before reactor trip.

7.7.4. Relevant event combinations

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

7.8. LOSS OF PRESSURE AND INVENTORY CONTROL

7.8.1. Initiating events

Pressurization events can result from:

(a) Feed valves fail open/liquid bleed valves fail closed.
(b) Pressurizer heaters fail on/steam bleed valves fail closed.

Depressurization events can result from:

(a) Feed valves fail closed/liquid bleed valves fail open.
(b) Pressurizer heaters fail off/steam bleed valves fail open.

7.8.2. Safety aspects

Pressurization events test the capability of the LRVs to overcome the pressure transient. The accident analysis also includes failure of one of these valves to reclose, thereby testing 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.

7.8.3. Acceptance criteria

The acceptance criteria are as follows:

(1) Dose to the most exposed individual in the critical group is below the Event Class 1 limit in Fig. 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), the LRVs being credited. The service limit for SDS2 high pressure trip is

ASME Level C (emergency) both with and without the LRVs being credited. 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.

7.8.4. Relevant event combinations

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

7.9. MAIN STEAM LINE BREAKS

7.9.1. Initiating events

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.

7.9.2. Safety aspects

The first safety aspect for all the 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 neither damaged by the forces from 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 the 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 breaks) and asymmetric breaks (those 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 alternative heat sink. Small breaks test the trip coverage and can lead to a long term containment pressurization after the containment dousing water has been exhausted.

Since the HTS pumps are tripped at 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 CANDU PHWRs have a high pressure backup heat sink (the shutdown cooling system), it is not necessary for the operator to depressurize the HTS before opening the valve to this alternative heat sink in emergencies.

7.9.3. Acceptance criteria

The relevant acceptance criteria are as follows:

(1) Dose to the most exposed individual in the critical group is below the Event Class 3 limit in Fig. 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 enough that a manually initiated alternative heat sink can be initiated within 15–30 min 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).

7.9.4. Relevant event combinations

A main steam line break is analysed in combination with various impairments in the special safety systems.

The following ECC system impairments are analysed in turn: failure of injection, failure of loop isolation, failure of steam generator secondary side 'crash' cooldown[8]. The combination of a main steam line break with a loss of

[8] Unless the instrumentation consists of two redundant independent sets, each having three channellized signals.

ECC gives rise to additional or changed safety aspects relative to those in Section 7.9.2 as follows:

(a) ECC may not be automatically initiated, in which case there is no change from a single failure.
(b) Where ECC is automatically initiated, it acts as a make-up to the HTS as the latter cools down and shrinks. In the absence of such a make-up, adequate two phase thermosyphoning must be demonstrated to remove decay heat.

Similarly a main steam line break with an LO ECC has additional or changed acceptance criteria relative to those of Section 7.9.3 as follows:

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

The following containment system impairments (for main steam line breaks inside containment) are analysed 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:

(a) The assumption of impairment of the containment heat sinks increases the internal containment pressure.
(b) Containment envelope impairments reduce the peak pressure but may (depending on the set points) decrease the trip coverage provided by containment high pressure trips.

Similarly, a main steam line break and impaired containment have additional or changed acceptance criteria as follows:

(a) Dose to the most exposed individual in the critical group is below the Event Class 5 limit in Fig. 1.
(b) The structural integrity of the containment must not be impaired to such a degree that consequential damage to the reactor systems could result. (Note: since the radioactivity releases are small, there is no requirement for staying below the 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, depending on the trip set points and their uncertainty allowances, 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 analysed 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 are usually 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.

7.10. FEEDWATER SYSTEM FAILURES

7.10.1. Initiating events

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.

7.10.2. Safety aspects

The safety aspects for this case are similar to those for 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 pressure rises and the safety aspect is the building integrity, including the integrity of the internal walls of the reactor building. Both symmetric breaks affecting all feedwater lines equally (e.g. a 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 alternative heat sink in emergencies.

7.10.3. Acceptance criteria

The following acceptance criteria apply:

(1) The dose to the most exposed individual in the critical group is below:
— The Event Class 1 limit in Fig. 1 for failures of feedwater control;
— The Event Class 3 limit in Fig. 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 enough that an alternative heat sink can be initiated within 15–30 min 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:

(i) For loss of flow feedwater failures, the service limit for SDS1 trip is ASME Level B (upset) crediting the LRVs. The service limit for SDS2 trip is ASME Level C (emergency) with and without crediting the LRVs.

(ii) For feedwater pipe breaks, the service limit for SDS1 high pressure trip is ASME Level C crediting the LRVs. The service limit for SDS2 high pressure trip is ASME Level D (faulted) with and without crediting the LRVs.

(iii) 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 dry-out 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.

7.10.4. Relevant event combinations

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 analysed 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:

The dose limits to the most exposed individuals in the critical group are given below:

(a) Event Class 3 limit in Fig. 1 for failures of feedwater control;
(b) Event Class 5 limit in Fig. 1 for breaks in the feedwater piping.

7.11. LOSS OF SECONDARY SIDE PRESSURE CONTROL

7.11.1. Initiating events

Depressurization of the secondary side could result from inadvertent opening of the atmospheric steam discharge valves (ASDVs), the condenser steam discharge valves (CSDVs) or the main steam safety valves (MSSVs); or from failure to unload the turbine after a reactor trip. Pressurization of the secondary side could result from a loss of condenser vacuum.

7.11.2. 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 alternative modes of plant control are assessed.

7.11.3. Acceptance criteria

The same acceptance criteria as for a loss of feedwater control apply.

7.11.4. Relevant event combinations

None.

7.12. 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 shut down is usually analysed by hand calculations of heat-up rate to show that there is sufficient time for the operator to diagnose the event and open the valve to one of the backup heat sinks.

7.13. MODERATOR SYSTEM FAILURES

7.13.1. Initiating events

Moderator system failures include:

— Moderator pipe break;
— Loss of forced circulation;
— Loss of heat removal.

7.13.2. Safety aspects

The safety aspects are as follows:

(a) 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;
(b) Distortion of the reactor flux as the moderator boils down, leading potentially to excess power in some reactor fuel channels;
(c) 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 (Table III).

7.13.3. Acceptance criteria

The following acceptance criteria apply:

(1) Dose to the most exposed individual in the critical group is below:
— The Event Class 1 limit in Fig. 1 for loss of moderator heat removal;
— The Event Class 3 limit in Fig. 1 for breaks in the moderator piping.

TABLE III. CONSERVATIVE SELECTION OF PARAMETERS FOR ANALYSIS OF MODERATOR SYSTEM FAILURES

Item	Conservative direction	Rationale
Number of calandria rupture discs that burst	Low	Maximize calandria pressure.
Moderator temperature	Low High	Delay high pressure trip. Maximize tritium release and extent of deuterium degassing.
Moderator heat load	Low High	Delay high pressure trip. Maximize dose.
Tritium concentration in moderator	High	Maximize radioactivity release.
Cover gas purging	Not credited	Maximize combustible gas concentration.

(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.

7.13.4. Relevant event combinations

None.

7.14. SHIELD COOLING SYSTEM FAILURES

7.14.1. Initiating events

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.

7.14.2. Safety aspects

The safety aspect is excessive shield tank distortion if the accident is not terminated. In general, analyses are focused on determining the time before operator action is required. There is no significant release of energy or radionuclides to containment.

7.14.3. Acceptance criteria

The following acceptance criteria apply:

(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 tube sheets 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.

7.14.4. Relevant event combinations

None.

8. SEVERE ACCIDENTS

8.1. INITIATING EVENTS

As with light water reactors, severe accident sequences are normally identified through a Level 1 PSA. However the event sequences discussed in previous sections of this report for PHWRs include a number of severe accidents (LOCA + LO ECC, LOCA + impaired containment) within the

design basis. In these cases the moderator can remove decay heat from the reactor in the absence of any coolant in the channels. The fuel is badly damaged but the UO_2 does not melt and channel integrity is preserved.

It is therefore 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 documents or by the applicant as part of the systematic plant review required by the regulator.
(2) Severe accidents beyond the design basis, in which the core geometry is preserved. These are not identified in regulatory documents. 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.
(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.

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; and loss of Group 1 electric power (Class IV plus Class III) plus loss of Group 2 Class III electric power.

8.2. SAFETY ASPECTS

Analysis of events of category (2) 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.

Since the severe core damage behaviour of PHWRs is somewhat different from that of light water reactors (LWRs), it is worth summarizing the phenomenology here. Analysis of events in category (3) initially started from heat balance calculations[9] (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 on the bottom of the calandria vessel.

[9] Including the effects of metal–water reaction heat.

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].

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

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 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 their melting point, and heat fluxes to the shield tank water are well below the critical heat flux under the existing conditions. 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 for arresting the accident at the calandria shell boundary are well recognized. Integrated system models need to be developed to cover the transient behaviour from initiating event to quasi-steady state, supported by small scale experiments [12] aimed at phenomena unique to PHWRs such as channel collapse and core debris retention.

8.3. ACCEPTANCE CRITERIA

As noted, PHWR regulators include acceptance criteria for some severe accidents, but there are no formal requirements for severe core damage accidents. However, the CANDU regulatory system is, to a large extent, a

consultative one, and some regulatory staff have stated that on new designs they will expect explicit consideration of such accidents in the design.

The CANDU 9 design incorporates the following requirements and features and can be considered typical of how severe core damage issues are addressed in new plants:

(a) The frequency of any severe core damage event sequence should be less than 10^{-6} events/reactor year.
(b) Gravity driven make-up to either the steam generators, the moderator or the shield tank from an elevated reserve water tank in 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. Options for long term heat removal from containment for such sequences are still under review.
(c) The concrete beneath the reactor has been selected to minimize the amount of non-condensable gas evolution should the debris penetrate the shield tank. However, in CANDU 9 the reactor structure is fairly close to the floor and there is no basemat, so the outside of the bottom part of the shield tank would be covered by water in any case.
(d) Both igniters and hydrogen recombiners are used in containment for control of local and global hydrogen concentrations.

9. REPORTING OF RESULTS

Reporting of the accident analysis is described in more detail in Ref. [3]. PHWR reporting practice is similar, and normally includes:

— Description of the initiating event, including any combined failures (e.g. unavailability of a special safety system or mitigating system);
— Event classification;
— Acceptance criteria, both criteria required by the regulatory agency and any additional criteria proposed by the designer or licensee;
— Descriptive event sequence (overview);
— System availability and performance assumptions;
— Summary of key input data parameters;
— Analysis methodology, physical models and computer codes used, usually with diagrams showing the system nodalization;
— Detailed description of the accident sequence, as predicted by the models and codes;

— Comparison with acceptance criteria and conclusions on acceptability of results.

In general, the following are also included:

— An event sequence table with corresponding times, especially if operator action is credited;
— Trip coverage maps for SDS1 and separately for SDS2 as a function of whatever parameter is being varied (e.g. break size and reactivity rate) and for all reactor powers; also graphs assuming that the RRS is operating and that it is inactive.

In addition, it is customary to present graphs of the following parameters. Of course, not all parameters are plotted for each accident.

— Reactor power transient, as a function of parameters such as break size;
— Net reactivity;
— Primary coolant flow in the core as a function of parameters such as break size and location;
— HTS pressure;
— Sheath temperature for hottest bundle in the high power channel;
— Pressure tube temperature in the high power channel;
— Fuel element failure threshold as a function of power and burnup;
— Transient fission product release from the fuel;
— Moderator temperature and subcooling transients;
— Transient containment pressure and temperature as a function of break location and size;
— Transient fission product release from containment;
— Dose to the public, to show compliance with dose limits specified in regulatory documents.

For pipe breaks specifically, graphs of the following parameters should be presented:

— Break discharge rate and enthalpy;
— ECC flows to broken and intact loops;
— Loop inventory and average loop void for intact and broken loops;
— Pressurizer water level;
— Header void fractions for intact and broken loops and average loop void;
— Moderator pressure transient (for in-core LOCA);
— Transient pressure tube strain.

For combined LOCA and LO ECC events, graphs of the following parameters should be presented:

— Fuel and fuel channel temperatures as a function of assumed steam flow rate;
— Heat load to moderator;
— Hydrogen production/concentration as a function of time and of assumed steam flow rate to the channels.

For severe accidents, reported parameters are similar to those for LWRs, as described in Ref. [13]. The inventory of the moderator and the shield tank water as a function of time should be included, as these sources of water can delay the progression of the accident significantly. An event sequence diagram, with timing, is particularly helpful.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, Safety Reports Series No. 23, IAEA, Vienna (2002).
[4] ATOMIC ENERGY CONTROL BOARD, Draft Regulatory Guide C-006 (Rev. 1): Safety Analysis of CANDU Nuclear Power Plants, AECB, Ottawa (1999).
[5] ATOMIC ENERGY CONTROL BOARD, Requirements for Shutdown Systems for CANDU Nuclear Power Plants, AECB Regulatory Policy Statement R-8, AECB, Ottawa (1999).
[6] ATOMIC ENERGY CONTROL BOARD, The Use of Two Shutdown Systems in Reactors, AECB Regulatory Policy Statement R-10, AECB, Ottawa (1977).
[7] CANADIAN STANDARDS ASSOCIATION, 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, CSA, Rexdale (1991).
[8] ATOMIC ENERGY CONTROL BOARD, Overpressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems, AECB Regulatory Policy Statement R-77, AECB, Ottawa (1987).

[9] SNELL, V.G., et al., "CANDU safety under severe accidents: An overview", paper presented at IAEA/OECD Int. Symp. on Severe Accidents in Nuclear Power Plants, Sorrento, 1988.
[10] BLAHNIK, C., et al., "Modular accident analysis program for CANDU reactors", Canadian Nuclear Society Conference (Proc. 12th Ann. Conf. Saskatoon, 1991), Canadian Nuclear Society, Toronto (1991) 235–242.
[11] ROGERS, J.T., et al., "Coolability of severely degraded CANDU cores", paper presented at ICHMT Int. Sem. on Heat and Mass Transfer in Severe Reactor Accidents, Cesme, Turkey, 1995.
[12] SIMPSON, L.A., MATHEW, P.M., MUZUMDAR, A.P., SANDERSON D.B., SNELL, V.G., "Severe accident phenomena and research for CANDU reactors", paper presented at 10th Pacific Basin Nuclear Conf. Kobe, 1996.
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants with Pressurized Water Reactors, Safety Reports Series, IAEA, Vienna (in press).

GLOSSARY

Only PHWR specific terms are introduced below. For general terms, see Ref. [3].

adjuster rods. Solid rods within the core used for flux shaping and startup.

C-006. Atomic Energy Control Board Consultative Document C-006.

calandria. Low pressure vessel containing the heavy water moderator, through which the fuel channels run.

calandria tube. Zircaloy tube surrounding the pressure tube for each channel, separated from it by a small insulating gas gap.

channel. Fuel channel consisting of a pressure tube and its surrounding calandria tube.

Class III power. Diesel generated emergency electric power. There are two independent and widely separated sets of Class III diesels: Group 1 diesels and Group 2 diesels. The latter are seismically qualified.

Class IV power. Normal AC electric power from the grid or from the turbine generator via the unit service transformer.

core pass. Transit of fluid once through the core via a pump and a steam generator. The typical CANDU HTS consists of one or more figure-of-eight loops, each of which has two core passes (i.e. fluid goes through the core twice before returning to its starting point). The loop in which a LOCA is assumed to have occurred is called the broken loop; the other loop is called the intact loop.

crash cooldown. Rapid cooldown of the steam generator secondary side through the main steam safety valves; activated on a LOCA signal.

critical break. Size of pipe break which produces the smallest core flows and maximizes fuel and/or pressure tube temperatures.

dousing. Spraying with high flow rate water, used in some CANDU containments for pressure suppression.

dry-out. Film boiling, formation of dry patch on fuel sheath. Because the PHWR HTS is near saturation, limited film boiling does not lead to an excessive sheath temperature rise.

dual failure. Single failure plus assumed unavailability of a special safety system or subsystem.

end-fitting. Mechanical component at each end of a fuel channel which permits a connection to the feeder pipe.

event class. For the purposes of accident analysis, AECB (Canada) divides events into five event classes, generally on the basis of frequency. Each event class has its own public dose acceptance criterion. See Fig. 1.

feeder pipe. Small pipes connecting each channel to the inlet and outlet headers at each end of the core.

figure-of-eight loop. See *core pass*.

Group 1. Systems used for power production that also have a safety function. Group 1 systems by themselves must be able to shut down the plant, remove decay heat, keep radioactivity contained and monitor the state of the plant.

Group 2. Seismically qualified emergency systems, including AC power (Group 2 diesels), feedwater (Group 2 auxiliary feedwater), service water, instrument air and secondary control area systems. Group 2 systems by themselves must be able to shut down the plant, remove decay heat, keep radioactivity contained and monitor the state of the plant.

header. Large pipes above the inlet and outlet ends of the core, to which each fuel channel is connected via feeder pipes.

loop. For CANDU: see *core pass*.

moderator cooling system. PHWR system to remove heat generated in normal operation (by conduction from the channels and direct deposition of neutron and gamma energy) from the moderator; typically 5% of full power.

pressure control and relief. Liquid relief valves are large valves connected to the HTS for overpressure relief. Steam relief valves are also connected to the pressurizer. Steam bleed valves are smaller valves connected to the pressurizer for pressure control. Pressurizer heaters are the primary means of routine pressure control.

pressure tube. Pressure boundary within the core, containing the fuel and coolant.

reactivity mechanisms. General term for in-core devices that can change reactivity, specifically: adjuster rods, absorber rods, liquid zone controllers, shut-off rods and poison injection nozzles.

ROP system. Regional overpower protection system: two spatially distributed networks of flux detectors within the core, each connected to one shutdown system, which will trip the reactor if regional or bulk reactor power is excessive.

RRS. Reactor regulating system. Digital system that controls reactivity devices and the major process systems.

set-back. Controlled power reduction through the RRS in response to an abnormal event.

sheath. Clad; cladding.

shield tank. Low pressure vessel (concrete or steel) containing light water shielding. Supports and contains the calandria.

shield tank cooling system. System to remove heat generated in normal operation (by conduction from the calandria and end-fittings) from the shield tank and end shields; typically 0.3% of full thermal power.

shutdown cooling system. System to remove decay heat when the reactor is shut down. It can be used at full temperature and pressure conditions in an accident.

single failure. A random failure that results in the loss of capability of a system to perform its intended safety functions. Consequential failures resulting from a single random occurrence are considered to be part of the single

failure. For PHWRs, the failure of a process system is classified as a single failure.

special safety systems. Shutdown system No. 1, shutdown system No. 2, ECC system and containment.

step-back. Rapid power reduction (by dropping control absorbers) by RRS in response to an abnormal event.

zone controllers. Light water filled compartments in the core, controlled by the reactor regulating system for short term reactivity control.

CONTRIBUTORS TO DRAFTING AND REVIEW

Allison, C.	Innovative Systems Software, United States of America
Balabanov, E.	ENPRO CONSULT Ltd, Bulgaria
D'Auria, F.	University of Pisa, Italy
Jankowski, M.	International Atomic Energy Agency
Mišák, J.	International Atomic Energy Agency
Munhoz-Camargo, C.	International Atomic Energy Agency
Salvatores, S.	Electricité de France, France
Snell, V.	Atomic Energy of Canada Limited, Canada

Consultants Meetings

Vienna, Austria: 9–13 June 1997, 17–21 November 1997, 12–16 January 1998, 5–9 October 1998, 27 September–2 October 1999

Technical Committee Meeting

Vienna, Austria: 30 August–3 September 1999