Safety Reports Series

No. 55

Safety Analysis for Research Reactors

IAEA
International Atomic Energy Agency

SAFETY ANALYSIS FOR RESEARCH REACTORS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
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
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
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’’.

SAFETY REPORTS SERIES No. 55

SAFETY ANALYSIS FOR RESEARCH REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2008

Sales and Promotion, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
August 2008
STI/PUB/1321

IAEA Library Cataloguing in Publication Data

Safety analysis for research reactors. — Vienna : International Atomic
Energy Agency, 2008.
p. ; 24 cm. — (Safety reports series, ISSN 1020-6450 ; no. 55)
STI/PUB/1321
ISBN 978–92–0–101008–7
Includes bibliographical references.

1. Nuclear reactors — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL 08–00525

FOREWORD

The aim of safety analysis for research reactors is to establish and confirm the design basis for items important to safety using appropriate analytical tools. The design, manufacture, construction and commissioning should be integrated with the safety analysis to ensure that the design intent has been incorporated into the as-built reactor.

Safety analysis assesses the performance of the reactor against a broad range of operating conditions, postulated initiating events and other circumstances, in order to obtain a complete understanding of how the reactor is expected to perform in these situations. Safety analysis demonstrates that the reactor can be kept within the safety operating regimes established by the designer and approved by the regulatory body. This analysis can also be used as appropriate in the development of operating procedures, periodic testing and inspection programmes, proposals for modifications and experiments and emergency planning.

The IAEA Safety Requirements publication on the Safety of Research Reactors states that the scope of safety analysis is required to include analysis of event sequences and evaluation of the consequences of the postulated initiating events and comparison of the results of the analysis with radiological acceptance criteria and design limits.

This Safety Report elaborates on the requirements established in IAEA Safety Standards Series No. NS-R-4 on the Safety of Research Reactors, and the guidance given in IAEA Safety Series No. 35-G1, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, providing detailed discussion and examples of related topics.

Guidance is given in this report for carrying out safety analyses of research reactors, based on current international good practices. The report covers all the various steps required for a safety analysis; that is, selection of initiating events and acceptance criteria, rules and conventions, types of safety analysis, selection of computational tools and presentation of the results of the analysis. It also discusses various factors that need to be considered to ensure that the safety analysis is of an acceptable quality. In specific terms, the calculations and methods in this report can be used for the safety analysis of newly designed research reactors, modifications and experiments with impact on safety, and upgrades of existing reactors, and can also be used for updating or reassessing previous safety analyses of operating research reactors.

This publication will be particularly useful to organizations, safety analysts and reviewers in fulfilling regulatory requirements and recommendations related to the preparation of the safety analysis and its presentation in the safety analysis report. In addition, it will help regulators conduct safety reviews and assessments of the topics covered.

The IAEA officers responsible for this report were S. Lee and A.M. Shokr of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This report does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

This Safety Report was developed within the framework of the IAEA's work programme dealing with research reactor safety. It elaborates on the requirements established in paras 6.72–6.78 of IAEA Safety Standards Series No. NS-R-4 on the Safety of Research Reactors [1], and on the guidance given in section A.16 (in particular, paras A.1601–A.1623) of Safety Series No. 35-G1 on the Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report [2].

Safety analysis is an analytical study that demonstrates how limits and conditions established to prevent radioactive releases, and various other requirements to ensure plant integrity, are met. The well accepted approach to this is to consider credible accident initiating events, and then to apply a deterministic method to estimate the maximum possible releases to the environment. Probabilistic methods may be used to evaluate which accident sequences are of greater likelihood and will be useful in evaluating relative risk rankings and hence guide the cost effective provision of countermeasures. They may also be used to identify hidden weaknesses in the design and to quantify the value of possible improvements or modifications.

Computational models using a deterministic approach are normally used for the safety analysis of research reactors. These models (and codes) have to be applicable over the expected range of operational parameters, yield conservative predictions, represent all physically important phenomena and have been properly validated.

The entire range of conditions for which a research reactor is designed, according to established design criteria, forms its design basis. Within the design basis, a number of unintended events are considered, including human factors and equipment failures, whose consequences or potential consequences may not be negligible in terms of facility safety. According to the probability of its occurrence and potential consequences, such an event may be classified as an anticipated operational occurrence or a design basis accident (DBA). An accident occurring outside the design basis is called a beyond design basis accident (BDBA). A BDBA may involve degradation of the reactor core (leading to significant core damage); the concept is typically used for the establishment of emergency planning and preparedness for the facility. The safety analysis includes the identification of DBAs and BDBAs. Therefore, in evaluating the safety of research reactors, the first step is to determine the response of the reactor to a range of postulated initiating events (PIEs) covering all credible events.

This report should be used in conjunction with the appropriate IAEA Safety Requirements and Safety Guides for research reactors [1–3]. A similar Safety Report on Accident Analysis for Nuclear Power Plants was issued in 2002 [4].

1.2. OBJECTIVE

The objective of this report is to provide a set of suggested methods and practices, both conceptual and formal, on the basis of current international good practices, for performing safety analyses. These methods and practices are particularly useful to the operating organizations, regulatory body and other organizations involved in the safety of research reactors.

1.3. SCOPE

This publication covers all steps in performing the safety analysis of a research reactor. It focuses on analysing transients and accidents as a part of the safety analysis. The course of the accident is covered from the initiating event up to the estimation of core damage.

The calculations and methods included in this report may be used as deemed necessary for the preparation of the safety analysis of newly designed research reactors and for modifications and upgrades of existing research reactors and new experiments with major safety significance, and may be also used for updating or reassessing previous safety analyses of operating research reactors. The main body of this report is intended to be as generally applicable as possible to all types of research reactors with a limited hazard potential to the public and the environment. Specific features of individual reactor types are taken into consideration in the examples provided in the annexes. Research reactors with power levels in excess of several tens of megawatts and fast reactors may require additional considerations that are beyond the scope of this report.

A systematic methodology for research reactor safety analysis, as presented in this report, comprises identification and selection of PIEs, establishment of acceptance criteria, development of the methods for transient and accident analysis, use of computational codes and presentation of the results achieved. The scope, extent and details of these activities for low power research reactors may be significantly less than those required for high power research reactors, and the activities could be conducted, without compromising safety, according to a graded approach commensurate with the hazard potential of the facility. Considerations for the implementation of such a graded approach to safety analysis are presented in Annex I.

This report deals mainly with ‘internal’ events originating in the reactor or in its associated process systems. Nevertheless, special internal events (such as fire) and external events will be briefly discussed to show how they fit within the safety analysis of a facility. Source term estimation and the transport of radioactive material are beyond the scope of this report.

This report incorporates the results of the coordinated research project on the Safety Significance of Postulated Initiating Events for Different Research Reactor Types and Assessment of Analytical Tools. This coordinated research project was conducted by the IAEA during the period 2002–2006, with the participation of scientific investigators from Algeria, Argentina, Brazil, Germany, Indonesia, Italy, the Republic of Korea, Romania, the Syrian Arab Republic and Vietnam.

1.4. STRUCTURE

Section 2 deals with the proper selection and categorization of PIEs. The relationship to a potential degradation of the safety functions is specified. Methods for grouping events into categories are given and the concept of a bounding accident scenario is introduced. Section 3 deals with the rules and conventions that are established to determine the response of reactor systems under accident conditions.

In Section 4, the acceptance criteria for a safety analysis are explained, and some examples of high level acceptance criteria, derived from the need to maintain safety functions and low public doses, are given.

Section 5 deals with the impact of utilization experiments and reactor modifications on the overall safety analysis of a reactor.

Section 6 summarizes the principles of two basic approaches in performing transient and accident analysis: deterministic analysis and probabilistic analysis. In deterministic analysis, the conservative and best estimate approaches are described.

Section 7 deals with possible applications of analysis, including design and licensing. The main characteristics of both applications are presented.

Section 8 discusses various issues relating to the application of computer codes for deterministic safety analysis. The basic types of features of the codes are described. Comments are made on the documentation of the code, its verification, validation and accuracy, aspects of the effects of the user on the analysis, and the preparation of input data.

Section 9 provides basic rules for the format and structuring of safety analysis results.

Section 10 discusses the importance of quality assurance (QA) for safety analysis and summarizes good practices in QA.

Examples of PIEs, external events, rules of safety analysis and acceptance criteria are given in Annexes I–XV.

2. INITIATING EVENTS

The basic safety functions to be performed in a research reactor are: shutting down the reactor; cooling, in particular of the reactor core; and confining radioactive material. Incidents or accidents may occur whenever a failure, malfunction or incorrect operation of a system or component challenges the fulfilment of one of these basic safety functions.

Once a release of radioactive material is foreseen, either as a routine part of normal operation or as the consequence of an accident sequence, this release has to be controlled in the normal operation case and limited or delayed in the accident condition case.

The safety analysis is used to demonstrate the safe operation of the reactor (fulfilment of basic safety functions) and how the design of the facility and the related operational procedures will contribute to the prevention and mitigation of accidents. It includes analyses of the response of the reactor to a range of PIEs.

The term ‘postulated initiating event’ (or simply ‘initiating event’) refers to an unintended event, including an operating error, equipment failure or external influence, that directly or indirectly challenges basic safety functions. Typically, such an event necessitates protective actions (automatic or manual) to prevent or mitigate undesired consequences to reactor equipment, reactor personnel, the public or the environment.

2.1. IDENTIFICATION AND SELECTION OF INITIATING EVENTS

The compilation of a comprehensive list of PIEs is an important start to ensuring an adequate analysis of the reactor response to disturbances in process variables, to malfunctions or failures of equipment, to human factors, to external events and to special internal events.

Operational experience from the facility or from similar facilities, including examination of event reports and the database of the IAEA's Incident Reporting System for Research Reactors, can be used to develop or supplement the list of PIEs. Methods for the identification of PIEs include:

(a) Development of a fault tree, either as part of a wider probabilistic safety assessment (PSA) or by itself;
(b) Identification of barriers to confine radioactive material, failure modes for those barriers and events that can lead to those failure modes;
(c) Comparison of the list of PIEs for research reactors provided in Ref. [1] (and reproduced in Annex II) with the design of the facility under analysis.

In order to simplify the safety analysis, it is reasonable to group all PIEs into categories. The method used to group PIEs has to take into account the following:

(i) PIEs that require similar safety actions;
(ii) PIEs that have similar influence on reactor behaviour or on systems, structures or components;
(iii) Grouping or categorizing of PIEs that assist in the selection of limiting cases for analysis in each group;
(iv) External PIEs that have the potential for common cause impact on the whole facility.

PIEs in each group have to be evaluated to identify those events that would be limiting and those that should be selected for further analysis. Such events would include those having potential consequences that bound all other PIEs in the group. The selection of limiting cases can be based on more detailed calculations, qualitative comparisons with other events or engineering judgement.

Considerations for PIEs for open pool, MTR type research reactors operating at various power levels are presented in Annex III. PIEs considered for a SLOWPOKE reactor of 20 kW are presented in Annex IV.

2.2. METHODS FOR EVALUATION OF EXTERNAL EVENTS AND SPECIAL INTERNAL EVENTS

The safety analysis must present the methods used to evaluate particular external and internal events such as earthquakes, tornadoes or sudden catastrophic rupture of reactor components or reactor internals. The effect of such events may be difficult to model or may result in highly speculative analyses. Nevertheless, the effect of these events on the safety systems of the facility can be evaluated and a conclusion can be reached on whether a given safety function can be fulfilled after the occurrence of such an event. Administrative measures to mitigate the risk related to external and special internal events could be taken into account in the analysis.

2.2.1. External events

In general, design qualification is an accepted practice for protection against external events, since siting questions have been resolved (e.g. the site does not present hazards that cannot be protected against adequately). A method for establishing the design bases for particular external phenomena can be summarized as follows:

(a) The potential of an event in the region for each phenomenon is assessed. If a potential exists, historical data are evaluated to determine both the intensity and the frequency of occurrence of the phenomenon.

(b) The relevant physical parameters associated with the different severities of each external phenomenon are identified.

(c) The relationship between the severity of the phenomenon and the frequency of occurrence is determined, or a model appropriate to the phenomenon in the site region is constructed.

(d) A particular design basis frequency of occurrence is established (often in the 10^{-3} a^{-1} region) for which protection is afforded to preserve essential safety related structures, systems and equipment.

(e) The design basis parameters for the phenomenon are evaluated.

Pressure retaining components may be protected from failure by design qualification. In this case the analysis deals with the design and construction standards used (e.g. acceptable engineering codes and practices) to prevent structural failures and to preserve the required safety functions.

For protection against external explosions it is necessary to assess the potential for this event and the associated overpressure in the event of transport of explosive products (pipelines, neighbouring installations, trucks, etc.).

The potential for aircraft crashes, including impact, fire and explosions on the site, is evaluated, taking into account air traffic characteristics, the location and type of airports and aircraft characteristics, including those with special permission to fly over or near the facility, such as firefighting aircraft and helicopters. Mechanical effects as well as the consequences of the fire caused by ignition of the fuel and, where applicable, detonation of armaments needs to be addressed.

The vicinity of the site is examined for facilities that store, process, transport and otherwise handle flammable, chemical, toxic, corrosive or radioactive material that could adversely affect safety.

The evaluation of external events for research reactors, with application of the graded approach, is discussed in Ref. [5]. Annex V presents examples of external events considered in the safety analysis of an MTR type research reactor.

2.2.2. Special internal events

The possibilities of fire, flooding and heavy load drop have to be evaluated in order both to determine provisions to prevent the occurrence of such events and to minimize their consequences if they occur.

Internal fire is one of the special internal events that must be addressed in the analysis. The facility must comply with local fire codes and, in addition, it must be demonstrated that the occurrence of a fire will not endanger the fulfilment of the basic safety functions. The effect of the fire on the safety systems must be analysed. Separation of redundancies, fail-safe characteristics of systems in the event of fire and the effect of smoke are some of the issues that need to be addressed.

Annex VI presents examples of special internal events considered in the safety analysis of an MTR type research reactor.

2.3. EVENTS INITIATED BY HUMANS

Operation of a research reactor is characterized by human actions and interventions on a daily basis, whether the reactor is at power or shut down. Even with all preventive measures in place, human actions or errors can still cause an initiating event. The analysis of the potential for and consequences of PIEs caused by humans can be done in parallel with the identification of PIEs and the description of the accident sequence.

In design analyses, the assessment of human factors may lead to design modifications; for example, pool top operations in a research reactor may result in an impact on important structures inside the pool. Those structures that will lead to a significant initiating event if impacted, such as neutron beam tubes, may need a protective structure that will eliminate human factor as a cause of a loss of coolant accident (LOCA) as a result of damage to the beams.

Special attention needs to be paid to human factors in facilities (e.g. critical assemblies) in which core configuration modifications are regularly made.

Reactor utilization is another area where a human factor assessment must be carried out. In addition to core reconfiguration, irradiation facilities must be evaluated for potential causes of initiating events, taking into account, among other things, tool design for remote handling of targets, ergonomics, use of an overhead crane or other lifting equipment, the size and mass of objects being moved or handled over the pool, and so on. Results of such analyses may lead to the imposition of administrative limits and conditions, such as mandatory levels of supervision for specified tasks, restrictions on the general use of the overhead crane and restrictions on the manoeuvring path of heavy objects hoisted over the pools.

3. RULES OR CONVENTIONS

Rules or conventions are established to determine the response of reactor systems and are applied uniformly throughout the analysis. These rules constitute the accident sequence, since they define which systems are considered for the purpose of the safety analysis, and which systems fail. Rules or conventions depend mostly on regulatory requirements and not on the power of the reactor. However, arguments may be given to adopt or reject a certain rule based on the application of the graded approach. Rules include:

(a) The application of single failure;
(b) Rules for crediting systems with respect to system qualification (or lack of qualification) under the environment resulting from an accident;
(c) Rules for crediting safety and protection systems, including reliability in quantitative terms, if appropriate under the graded approach;
(d) Rules for crediting support systems, such as normal and emergency electric power systems, cooling water system, etc.;

(e) Rules for crediting redundancy trip parameters;
(f) Rules for crediting actions of systems that are independent;
(g) Rules or conventions for crediting operator actions (e.g. emergency planning and preparedness and response time);
(h) Whether frequency or probability evaluations will be carried out to assess system response, the extent to which such methods will be used and the methodologies to be employed (including validation).

Rules or conventions have to be developed to determine those event sequences that are outside the design basis and thus excluded from further analysis, except for one scenario to be used for the purpose of emergency planning and preparedness. Such rules could be based on:

(i) Qualitative arguments justifying exclusion of events that are impossible or not considered credible for the reactor under study (by the application of engineering judgement);
(ii) Qualification of the facility or reactor systems for the effects of the event;
(iii) Quantitative frequency or probability arguments.

The effects of dependent failures (e.g. common cause failure) and human error have to be considered, including:

- Investigations carried out to identify the specific causes of dependent failures or human error;
- Evaluation of the effect of human error in either initiating an accident or worsening the development of accident sequences;
- Assessments of the validity of any assumptions or rules concerning the response of reactor systems during accident sequences.

Annex VII presents the rules considered for the analysis of reactivity insertion accidents for a 20 MW research reactor with two independent and diverse shutdown systems. Annex VIII presents the practice of the Canadian Nuclear Safety Commission for the safety analysis of research reactors.

4. ACCEPTANCE CRITERIA

Acceptance criteria are usually applied to judge the acceptability of the results of safety analysis. They may:

(a) Set numerical limits on the values of predicted parameters;
(b) Set conditions for plant states during and after an accident;
(c) Set performance requirements on systems;
(d) Set requirements on the need for, and the ability to credit, actions by the operator.

Acceptance criteria may be specified as basic and specific. Basic acceptance criteria are usually defined as limits set by a regulatory body. They are aimed at achieving an adequate level of defence in depth. Examples would be the maximum allowed doses to the public or the prevention of fuel failures. Specific acceptance criteria are used to include additional margins beyond the basic acceptance criteria to allow for uncertainties and to provide additional defence in depth; for example, in order to satisfy the basic acceptance criterion of ‘prevention of fuel failure’, the analyst may choose to use specific acceptance criteria such as:

(i) Maximum cladding temperature below blistering temperature;
(ii) Maximum heat flux not exceeding critical heat flux (CHF) during a transient;
(iii) Maximum heat flux not exceeding onset of significant void (OSV) during a transient;
(iv) Flow conditions not exceeding onset of flow instability (OFI).

The basic acceptance criteria are defined by the regulatory body. Specific acceptance criteria may be defined by the designer and agreed by the regulatory body. In the latter case, this agreement should be obtained before the analysis is started.

Figure 1 shows how a specific acceptance criterion relates to the corresponding safety limit. In the figure there is also a representation of the safety margin (difference or ratio between the safety limit and the operational limit) and the margin to the acceptance criterion (difference or ratio between the acceptance criterion and the calculated value). In those cases where the measurement of a parameter such as cladding temperature, heat flux or flow rate through a channel is not available during a transient, no distinction is made between these safety margins and the margin to the acceptance criterion.

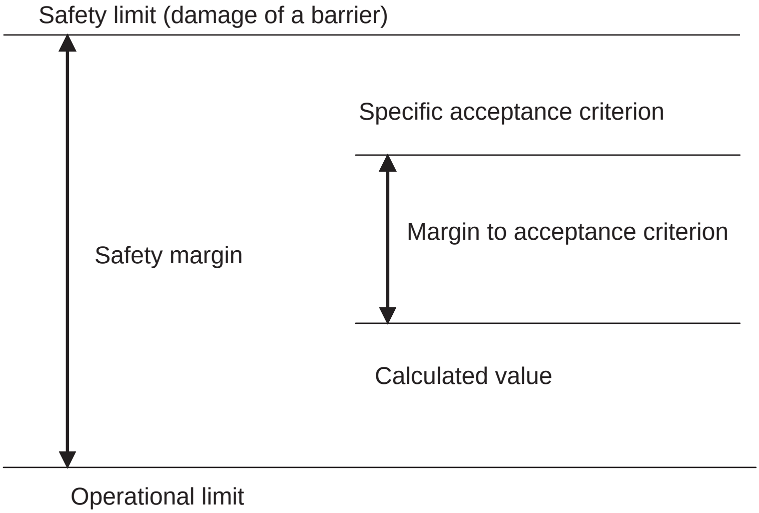
Safety limit (damage of a barrier)
Specific acceptance criterion
Margin to acceptance criterion
Safety margin
Calculated value
Operational limit

FIG. 1. Relationship between the specific acceptance criterion and the safety limit.

The appropriate margin between results predicted by the analysis and the acceptance criterion is related to the uncertainties. If a result has low uncertainty, a small margin to the acceptance criteria may be acceptable. In general, the adequacy of the margin with the acceptance criterion is demonstrated by using a conservative analysis to meet the acceptance criterion. This approach is called 'conservative'.

Acceptance criteria may vary according to the frequency of the PIE, as shown in Fig. 2. More stringent criteria are applied to events with a higher probability of occurrence, with lower consequences.

Once the acceptance criteria are established, the safety analysis is continued until the facility has reached a stable and acceptable state that ensures:

- The core remains subcritical;
- The core receives adequate cooling;
- Releases of fission products from the confinement or containment have ceased, or an upper bound of further releases can be estimated.

Annex IX presents a discussion on the acceptance criteria to be adopted for the MAPLE research reactor in Canada. Annex X shows an example of basic criteria as a function of the accident frequency and the specific acceptance criteria adopted for aluminium cladding research reactors in Argentina. Annex XI presents the basic and specific acceptance criteria adopted in the upgrade of

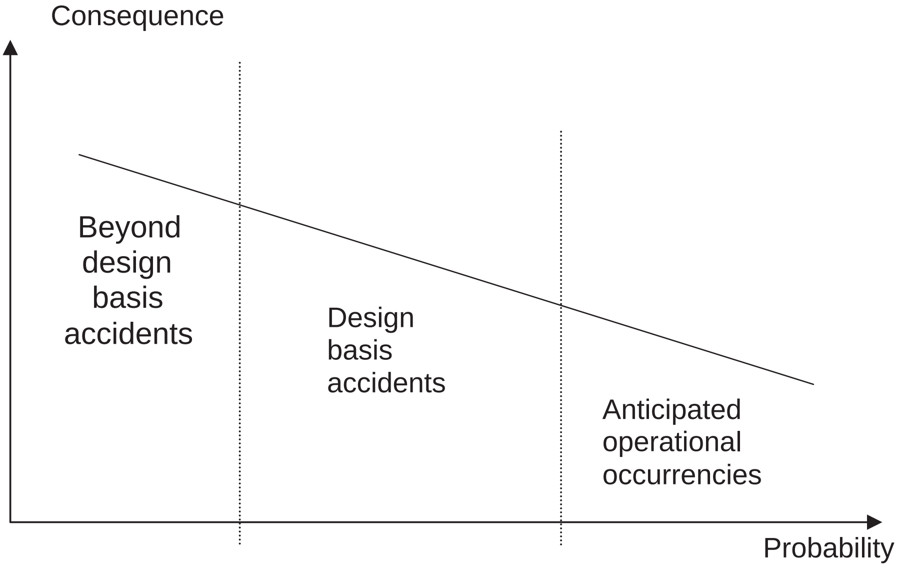
Consequence
Beyond design basis accidents
Design basis accidents
Anticipated operational occurrencies
Probability

FIG. 2. Schematic diagram of criteria for different probability event sequences.

the IEA-R1 research reactor in Brazil. Annex XII presents the acceptance criteria adopted for the licensing of the HANARO research reactor in the Republic of Korea.

5. UTILIZATION AND MODIFICATION

The IAEA Safety Guide on Safety in the Utilization and Modification of Research Reactors [3] presents guidance, approved by international consensus, for the safe utilization and modification of research reactors. While the Safety Guide is most applicable to existing reactors, it is also recommended for use by organizations planning to put a new reactor into operation.

Information on experiments and modifications (to the reactor or experimental devices) that may affect the safety of the reactor is evaluated. Experiments and modifications having major safety significance are evaluated with procedures for design, construction, commissioning and safety analysis that are equivalent to the reactor itself.

Special attention has to be paid in performing safety analysis of new experiments and modifications that entail hazards that are different in nature from, or more likely to occur than, those hazards previously considered. Special attention should also be given to those new experiments and modifications that may result in a reduction of an existing safety margin.

5.1. REACTOR UTILIZATION

The objective of the analysis is to demonstrate that reasonable provisions have been made so that the experimental facilities (beam tubes, thermal column, in-core or moderator facilities, boreholes, experimental loops, cold and hot sources, etc.) and the experiments and modifications do not pose a significant risk to the facility, the staff or the public. In the analysis, the mutual interaction between the reactor and the experimental devices and between the different experimental devices has to be taken into account. The analysis deals also with the administrative procedures and control provisions related to the experimental devices. Human factors in the handling of the experiments and the effect on the reactor must be considered.

One of the results of the analysis related to the experimental programme is the definition of which materials will not be allowed in experiments in or near the reactor core, and of materials that may only be utilized under additional safety conditions.

Installation of complex experimental devices in an existing reactor, such as a cold neutron source, a hot neutron source and high pressure test loops, necessitates analysis both of the safety of the experimental devices and of the experiments themselves and their effect on the safety of the core. The main safety function that protects the core from a failure in the experiment needs to be identified. PIEs that can challenge the fulfilment of this safety function are established, together with the accident sequence and numerical analysis as needed. Installation of such experimental devices is considered as a modification to the reactor (see Section 5.2) rather than an introduction of a new (or modified) experiment.

Changes to irradiation targets also necessitate a safety review, since the reactivity worth and the heat dissipated by the targets may vary.

More details on the safety categorization of new experiments and the associated requirements for safety analysis are provided in Ref. [3].

5.2. REACTOR MODIFICATIONS

Depending on their type, modifications to the reactor facility are essentially modifications to the design. They require regulatory approval and therefore necessitate a safety analysis. Reactor modifications can range from conversion of the fuel type to the inclusion of complex experimental devices such as a cold neutron source or high pressure test loop.

5.2.1. Core conversion

Conversion from one fuel type to another requires a complete re-evaluation of the safety analysis. Changes to the reactivity worth, shutdown margin, power density and material properties need to be taken into account, and appropriate modifications need to be made to the rules for the analysis.

5.2.2. Upgrades

Upgrades may involve design modifications, and therefore an update of the safety analysis is required. In the event of a power increase, new PIEs may be added. The rules of the analysis and the acceptance criteria may also be modified; for example, if a low power reactor is converted to a higher power, acceptance criteria for the margin to critical phenomena such as flow redistribution and CHF may need to be increased to account for the greater hazard posed by the facility. PIEs that had not been considered may need to be added.

When upgrading the instrumentation and control systems, improvements in the coverage of PIEs may lead to changes in the accident sequences and rules of analysis; for example, addition of a low core pressure drop trip variable as a redundant and independent means of detecting loss of core cooling flow will change the loss of flow accident (LOFA) sequences.

Modifications to process systems, such as to the primary cooling system, secondary cooling system, etc., may affect cooling capacity and modify accident sequences; for example, replacement of a single 100% primary cooling system pump by two 50% pumps may lead to a change in the LOFA sequence. Whereas before, failure of a single pump would have led to complete loss of flow, with transition to natural circulation or emergency core cooling, in the new pump configuration, failure of a single pump will result in loss of 50% of cooling flow and subsequent reactor shutdown, but with forced convection cooling by the remaining pump.

5.2.3. Core configuration modifications

Modifications to the core configuration may include changes in the number of fuel elements, inclusion of in-core irradiation positions, inclusion of or modifications to reflector irradiation positions or addition of experiments with reactivity insertion potential.

This type of modification may lead to new PIEs as well as to changes in the accident sequences; for example, reactivity insertion events caused by insertion or removal of irradiation material need to be addressed. Cooling of irradiation targets and the consequences of a loss of cooling may also have to be analysed.

6. METHODS FOR TRANSIENT AND ACCIDENT ANALYSIS

6.1. DETERMINISTIC ANALYSIS

Safety evaluations of research reactors are mainly performed by deterministic methods. Deterministic techniques are often characterized by conservatism (the ‘conservative approach’). By comparison, the best estimate method provides a realistic simulation of a physical process to a level commensurate with the currently known data and knowledge of the phenomena concerned. The method is free of deliberate pessimism and contains sophisticated models for the description of the relevant processes.

The following descriptions help to clarify the basic ideas used in both approaches:[1]

Best estimate (or realistic) code. A combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. The term ‘best estimate code’ means that the code is free of deliberate pessimism and contains sufficiently detailed models to describe the relevant processes of the transients that the code is designed to model.

[1] Other terminology relevant for safety analysis is defined in the IAEA Safety Glossary [6].

Best estimate (or realistic) model. A model that provides a realistic estimate of a physical process to the degree consistent with the currently available data and knowledge of the phenomena concerned.

Bounding data. This category is typical for nuclear data that usually change from cycle to cycle or from the beginning to the end of a given cycle. Using data that envelop all conditions, conservative results can be obtained.

Conservative code. A combination of all of the models necessary to provide a pessimistic bound to the processes relating to specified acceptance criteria.

Conservative data. Plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a pessimistic result, when used in a safety analysis code, in relation to specified acceptance criteria.

Conservative model (or correlation). A model (or correlation) that provides a pessimistic estimate for a physical process in relation to a specified acceptance criterion.

Realistic (or best estimate) data. Plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a realistic (also ‘as designed’, ‘as built’, ‘as operated’) result.

Uncertainty. This is a measure of scatter in experimental data or calculated values. It is expressed by an interval around the true mean of a parameter resulting from the inability to either measure or calculate the true value of that parameter (scatter). The uncertainty is often given as a (e.g. 95%) probability limit or probability interval.

6.1.1. Conservative approach

The goal of the conservative approach is to ensure that the actual plant response in relation to a selected criterion is enveloped by the conservative value for that response. The conservative approach uses conservative or bounding data. It considers the most unfavourable reactor configuration (e.g. beginning of operation, minimum number of fuel elements) and takes into account uncertainties and tolerances associated with the parameter that affects the variable of interest.

Uncertainties and tolerances can be grouped into different categories according to their source. A possible grouping is:

(a) Reactor control and power.
(b) Reactor geometry: geometric and material tolerances associated with fuel fabrication (tolerances, chemical composition, etc.) and during the reactor's life (e.g. deformation, erosion and physical and chemical changes in materials, particularly in the fuel).
(c) Thermodynamic local conditions (uncertainties in the measurement or estimation of parameters such as pressure, density, enthalpy, velocity, heat flux, etc.).
(d) Correlations used to calculate heat transfer coefficients, friction losses and critical phenomena.

There are different ways or methods to include these uncertainties and tolerances in a conservative calculation:

(i) Multiplicative method (or worst case), in which each parameter is assigned a conservative constant value and all parameters are assumed to exist, simultaneously, at their most detrimental value. This method is very simple to apply but overly conservative. It can be useful for those cases that have large margins to the critical phenomena.
(ii) Statistical methods, in which standard deviations are combined in a statistical manner. The method is more realistic than the multiplicative method, with less excess conservatism.
(iii) Weighted or combined statistical methods, in which the errors of some variables are statistical and some are systematic. In this case a mixed combination method is used.
(iv) Monte Carlo method, in which the uncertainties are combined randomly.

The analyses also need to take into account conservative values for delays in the actuation of safety systems and for errors in the adjustment of set points and in measurements of key parameters of a safety system (e.g. flow rates of emergency systems).

For conservative analyses it is normally assumed that corrective or mitigating operator action does not take place for a prescribed period of time, but that after that the action takes place successfully.

The choice of an overly conservative methodology can unnecessarily limit the range of operation of a research reactor. The level of conservatism to be applied in the analysis should be proportional to the understanding of and capability to model the physical phenomena involved in the transients, the availability of reactor experimental data and the experience of the analyst.

Sensitivity studies must supplement the conservative analysis to identify the important parameters. Systematic variations in code input variables or modelling parameters can be used, in combination with expert judgement, to verify their impact on the variables or to bound the overall results of the analysis. Results of experiments can also be used to identify important parameters.

6.1.2. Best estimate approach

Best estimate analysis permits a good view of the existing margins or limits on research reactor transient scenarios in relation to the safety analysis. The use of a best estimate code is essential for best estimate analysis. Such codes do not include models that are intentionally designed to be conservative. System thermohydraulic codes such as RELAP, CATHARE and ATHELET are examples of best estimate codes. In some cases, the user can 'tune' the models in the code, by means of input options, to force the code to provide conservative results. However, this is usually only necessary in special circumstances in which the uncertainties are not known or are unacceptably large.

A best estimate analysis must be supplemented by an uncertainty analysis. Uncertainty analyses include the estimation of uncertainties in individual modelling or of the overall code, uncertainties in representation and uncertainties in reactor data for the analysis of an individual event. The uncertainty evaluation is normally restricted to DBA analyses.

For system thermohydraulic codes, different formal methodologies have been developed to help evaluate the uncertainties in the code's predictive results. These methodologies fall within three basic approaches for quantifying the uncertainties in the code calculations. One approach uses a combination of expert judgement, statistical techniques and multiple calculations of code sensitivity to combine uncertainties in key parameters, initial and boundary accident conditions, and scaling effects. The second approach uses scaled experimental data and code with data comparisons to estimate uncertainties in predicted plant behaviour. The third approach uses bounding calculations.

The best estimate approach is highly dependent on an extensive experimental database to establish confidence in the best estimate codes and to define the uncertainties that have to be determined for the best estimate results. Such databases are, in general, not available for research reactors. Instead, the approach that seems to be becoming more popular among analysts dealing with research reactors is the use of best estimate codes with a conservative set of input data.

6.2. PROBABILISTIC ANALYSIS

Probabilistic analyses are performed to quantify the consequences of the end points of PSA sequences. Since there can be many such sequences, they are usually grouped into categories, and a representative or bounding analysis is performed for each category. The application of probabilistic techniques is beyond the scope of this report.

It is not practical to simulate all the transient situations that may be expected in a typical reactor system (a nuclear power plant or a research reactor). Therefore, a hierarchy of transients can be obtained by using suitable probabilistic approaches. The transient's importance is usually established on the basis of the probability of occurrence and the consequences of the accident in terms of radioactive releases. In this way, a number of transients become suitable for analysis by conservative or deterministic approaches.

Probabilistic and deterministic analyses have been combined in a variety of ways. Probabilistic analyses have also been used in individual research reactor assessments to identify the specific accident conditions to be used for best estimate analysis of BDBAs. Uncertainties in modelling, sensitivity studies and probabilistic analyses have been combined to determine the likelihood of radioactivity release to the environment.

The main focus of PSA is to provide realistic answers, and hence best estimate codes and data are normally used. However, the results of the supporting analysis may sometimes be 'bounded' by the results of deterministic or conservative analyses to show that equipment performance is satisfactory. Bounding analyses should not be used for developing procedures for bringing the reactor back to the safe status should an accident occur.

7. TYPES OF SAFETY ANALYSIS

The results of safety analyses are used in a number of different areas, such as design, licensing, support for accident management and emergency planning. This section describes these applications.

7.1. SAFETY ANALYSIS IN DESIGN

The objective of safety analysis in reactor design is to confirm that the design meets the relevant national safety requirements. Safety analysis in design is used to support the design of a new plant or modifications to the design of an existing facility. This will be an iterative process between the design and the analysis of safety performance. All the challenges that the reactor may be expected to meet during its operational life are to be considered during the design process. These challenges include all the foreseeable conditions and events related to reactor stages or operational states and accident conditions, site characteristics, design requirements and limits of parameters, modes of operation, etc. The demands on the reactor design imposed by the above challenges and conditions form the design basis of the research reactor facility and specify the capabilities needed to cope with the challenges without exceeding the authorized limits.

The designers recognize that challenges to all levels of defence in depth may occur, and design measures are provided to ensure that the safety functions are accomplished and that the safety objectives can be met. These challenges stem from the PIEs, which are selected appropriately for their analysis as described in Section 2. It is shown that the set of PIEs covers all credible accidents that influence the safety of the reactor. In particular, the DBAs should be identified. Although it is not usual to include PIEs with a very low frequency of occurrence, the establishment of the threshold limit should consider the safety targets established for the specific reactor.

Safety analysis in design is performed to assist in setting characteristics such as:

(a) Equipment sizing, including determination of parameters for pressure, temperature, electric power, flow and cooling for safety related equipment such as the emergency core cooling system, sprays and emergency water supplies;
(b) Approximate determination of set point values for parameters that trigger protective systems, to confirm that they are effective and to allow adequate operating margins;
(c) Assessment of dose to the public, for confirming such aspects as the exclusion area boundary.

Safety analysis in design is also used to check at an early stage that the design will meet the national licensing requirements. The safety analyst works closely with the designer so that the design configuration can be optimized in terms of safety and cost.

7.2. SAFETY ANALYSIS FOR LICENSING

The objective of the safety analysis for licensing is to demonstrate that the facility design features and the operational limits and conditions have been selected such as to ensure that no credible accident could lead to unacceptable radiological consequences to the public or the environment.

Safety analysis for licensing is used to provide evidence to the regulatory body that the design is safe. The regulatory body may require new calculations when new evidence arises from new developments or from reactor operating experience. The regulatory body may further require the use of updated computer codes that incorporate results arising from new developments or from reactor operating experience.

As a part of the safety assessment for licensing, the analysis should proceed in parallel with the design process, with iteration between the design and the licensing. The scope and level of detail of the analysis should increase as the design programme progresses, so that the final safety analysis reflects the final design as constructed.

7.3. SUPPORT FOR ACCIDENT MANAGEMENT AND EMERGENCY PLANNING

The analysis of accidents for supporting accident management describes the reactor behaviour in conditions for BDBAs and, in general, is performed using the best estimate approach. Accident management is a set of actions during the evolution of a BDBA. Safety analysis may be performed to support the preparation of emergency operating procedures. The results of BDBA analyses, defining the source term and radiological releases, could also be used for purposes of emergency planning.

Owing to the very limited possibility of using real reactor transients for validation of emergency operating procedures, analyses by computer codes are used to support the development and validation of emergency operating procedures.

8. COMPUTATIONAL TOOLS

Several types of tool are used for the analysis of research reactors, ranging from manual calculations (including spreadsheets, charts and graphs), through empirical (parametric) and subchannel (single equation based) computer codes to specialized reactor physics codes and sophisticated mechanistic system thermohydraulic codes. Manual calculations are useful only for fairly simple situations and for running spot checks on data or results that form part of a greater analytical effort, and are therefore not discussed further in this report.

Of the rest of the spectrum of codes mentioned above, each has its advantages and disadvantages in given situations, and it is rare that a single code or code system is sufficient for the comprehensive safety analysis of a research reactor. On the other hand, access to some of the more sophisticated modern codes can be costly compared with typical research reactor budgets, especially when additional human resources and training are needed.

A number of codes used or of potential use within the research reactor community are also in use in the nuclear power plant industry. While the principles at the basis of the development and use of the codes are the same or very similar, the range of parameters for validation and application, and the complexity of the systems modelled, may differ for research reactors and also between different classes of research reactors.

8.1. TYPES OF COMPUTATIONAL TOOL

The different types of computer code available internationally and often used for safety analysis of research reactors include the following:

(a) Reactor physics codes;
(b) Fuel behaviour codes;
(c) Thermohydraulic codes, including system codes, subchannel codes and computational fluid dynamics (CFD) codes;
(d) Structural analysis codes.

Reactor physics codes model the core neutron kinetics in normal and accident conditions. They use multidimensional models (2-D or 3-D) for analysing local or asymmetrical effects in the reactor core that are important in steady state operation. Transient behaviour can also be approximated using a sequence of pseudo steady state conditions. These codes are often used to generate the user input data for the simpler (usually point kinetics) models in thermohydraulic codes. Examples of reactor physics codes are WIMS, DYN3D and KIKO 3D.

Fuel behaviour codes describe the behaviour of individual fuel elements (pins, rods, plates, etc.) in normal operation and transient conditions. They tend to be design specific since empirical data are used in their development, but examples are available for most fuel types. The transient codes used for accident conditions may contain modelling options for both conservative and best estimate calculations.

System thermohydraulic codes are typically not design specific and are applicable to a wide variety of reactor designs and conditions. They generally fall into the category of best estimate codes, although many contain user selectable models for both conservative and best estimate applications. Mechanistic models for two fluid, non-equilibrium hydrodynamics, point and multidimensional reactor kinetics, control systems, and special system components (such as pumps and valves) make these codes very attractive. However, care should be taken when using these codes for research reactors, in order to ensure that the models included in these codes are valid for the operating regimes of the research reactors. The validity of the models and correlations should be verified. System codes allow simulating the complete primary and secondary circuits and the interactions between them. An example of a nodalization prepared for the safety analysis of the SAFARI research reactor in South Africa is presented in Annex XIII. Examples of system thermohydraulic codes are RELAP5, TRAC-P/B, CATHARE, ATHELET, DINAMIKA and CATHENA.

Subchannel codes are used to analyse specific processes within the core of the reactor, such as localized flow and heat transfer variables in representative fuel assemblies. They are generally self-contained, in terms of nuclear kinetic, flow and heat transfer models, but lack the sophistication of the reactor physics and system thermohydraulic codes. Examples are PARET and COBRA.

CFD codes are used for the analysis of localized phenomena such as the flow pattern in complex geometries. This is, however, a relatively recent development and their qualification status for application in transient flow analysis for research reactor licensing should be verified. The nodalization of a reactor vessel with its complex internal structures and the resulting velocity profile is presented in Annex XIV.

Structural analysis codes are used to describe the behaviour of mechanical components such as core support and pool structures, in the case of a pool type reactor, under various accident conditions. These codes are commercially available and have generally been developed for non-nuclear applications. They utilize boundary conditions supplied, for example, by thermohydraulic codes. Knowledge of the mechanical properties of material used by the nuclear industry is necessary for these codes. Examples of structural analysis codes are NASTRAN and ANSYS.

The selection of the set of codes to be used in the safety analysis of a particular research reactor is the responsibility of the operating organization, taking due account of the reactor type and its hazard potential, as well as of realistic resource, budgetary and licensing requirements. However, internationally recognized and accepted codes are the most appropriate to be used, where possible and applicable. It is the responsibility of the regulatory body in each country to accept the use of such codes.

8.2. CODE QUALIFICATION

A code must be qualified in order to be applicable to any safety analysis — especially for licensing purposes. This means that the boundaries of validity and application for the code need to be rigidly documented. Although it is not possible to provide a detailed list of the key phenomena and code features necessary for each type of code, three criteria can be used to judge the adequacy of the codes for treating important phenomena:

(a) The use of internationally recognized and accepted codes provides some assurance that the codes are adequate for their intended application.

(b) Individual codes need to be evaluated on a systematic basis, comparing the intended application of the code with the actual conditions for which the code is applied.

(c) Lists of important phenomena expected during the transients that constitute the target of the investigation must be established. In many cases, documentation is available on an individual code basis that describes the relative importance of the different phenomena.

8.2.1. Code verification

Within the present framework, code verification is defined as the review of the source coding against its description in the documentation. This has not been applied consistently to many of the codes used around the world. Since the line by line verification of large codes is a time consuming and expensive process, this process is limited to those codes that are relatively static and not subject to continual change. However, many industry sponsored codes have been subjected to stringent verification procedures as a consequence of the regulatory licensing process. A report on the status of verification of a particular code would be available in the code documentation if this process has been properly conducted.

8.2.2. Code validation

There is normally a regulatory requirement that the code be assessed (validated) against relevant experimental data for the major phenomena expected to occur during the transients of interest in the target reactor for which the code is to be applied. The validation relates to the confidence that can be placed on the accuracy of the reactor behaviour and critical values under accident conditions predicted by the code. The specifics of what is required will vary according to the particulars of the safety assessment under consideration.

Extensive code validation requires a huge amount of effort and cost at the international level, involving validation projects, usually managed by the code developers and carried out, under cooperation and exchange agreements, by user groups worldwide with access to experimental facilities designed to provide data on behaviour and phenomena of importance. The process is augmented by a number of international standard problems set to establish a point of comparison between codes.

Code applicability to research reactor situations must be demonstrated by considering the range of parameters that characterize the transient analyses in the reactors. These parameters include the low energy thermohydraulic conditions and the multiplicity of core arrangements, functions and geometries typical of most research reactors. Frequent refuelling shutdowns of research reactors (compared with power reactors) and constantly varying core conditions (especially in those research reactors involved in isotope production) provide excellent opportunities for rapidly building up a reactor specific database of operational transients, core flow parameters and flux distributions that can be used for benchmarking thermohydraulic, neutronic and to some extent fuel behaviour codes, and for demonstrating the validity of the codes for certain applications. Validation of many codes for predicting accident conditions, however, remains largely uncertain. This uncertainty can be addressed in several ways:

(a) Where the end justifies the means (and cost), a reactor specific experimental facility can be built to provide the missing data. The objective should, however, be to test the validity of the code as it is and/or provide a quantitative evaluation of the uncertainty/error in the code's predictions, rather than to formulate alternative models for the code to predict the experiment more accurately (unless the code developer has agreed to reverify the code with such modifications).

(b) If possible, the uncertainty in the prediction of the code can be quantified by a simpler means (e.g. a particular line of argument based on solid logic) to determine an upper bound for extreme conditions.

(c) Engineering judgement may be possible.

(d) Code to code comparisons could improve confidence in a particular code by providing a similar set of results.

(e) Using codes that can claim such validation.

Annex XV presents an example of a methodology for thermohydraulic code validation for safety analysis in research reactors.

8.2.3. Code documentation

Each computer code needs to be adequately documented to facilitate review of the models and correlations and to ensure that the models for the important phenomena are appropriate and are not applied outside the range of their validity. The code documentation should also include user guidelines and input descriptions to assist the user to apply the code as intended. In addition, an installation manual is essential, especially where the code is compiled and assembled from source code on the user's computer platform or otherwise set up according to user selectable options. The code distribution package should contain sample input and output decks that will enable the user to check the integrity of the installation with respect to all the computational models and phenomenological predictions of the code.

A complete set of documentation for a properly qualified code would therefore typically include:

(a) An abstract of the program.
(b) A theory manual.
(c) A user manual and description of the input.
(d) A user guide.
(e) An installation manual with a procedure specific to the user's hardware and software platform (the user must ensure that his or her intended platform corresponds with one of the supported platforms for the code).
(f) Sample problems — input and output decks.
(g) A validation report.

8.3. USER QUALIFICATION AND USER EFFECT ON MODELLING

Modern computer codes have been made more user tolerant by optimizing parameters, such as time step and model selection, that can affect the code output. However, the user can still have a significant influence on the quality of the analysis. This has been evident in the exercises on international standard problems where, although some of the variation is due to the use of different computer codes, substantial variation can still be observed when different users use the same codes. Therefore a user must be knowledgeable of the experiments, the phenomena and the extent to which they apply to the research reactor situation, as well as of the code itself.

The type of code being used, the complexity of the system being analysed and the depth of knowledge and level of experience of the user have a strong influence on the results of the analysis; for example, the user has to make many input decisions for typical system code calculations, including the level of system nodalization, input parameters for code models, specific system characteristics and components, initial and boundary conditions for the system and, in some cases, state and transport properties. For this, the user needs to be conversant not only with the codes but with the underlying theory (neutronic, thermohydraulic, etc.) as well as with the reactor design, operation and utilization at all levels. In addition, with the input necessary for the system codes running in many cases to several thousand input values, input errors are not only possible but inevitable.

There are a number of ways that such user effects can be reduced. These are discussed at length in Ref. [4] for nuclear power plants and are equally applicable for research reactor analysis.

8.4. PREPARATION OF INPUT DATA

The first important step in developing input data for the computer code for the reactor under consideration is to collect the necessary documentation and other reliable sources of data. The sources that serve as a basis for data collection can be summarized as follows:

(a) Documentation on reactor design;
(b) Technical specifications of equipment;
(c) Documentation gathered during the startup and commissioning of the installation;
(d) Operational documentation for the reactor (limits and conditions, including technical specifications, operating instructions, records of operational regimes);
(e) As-built reactor documentation.

All documents and other data sources used for the preparation of the input data need to be clearly identified and referenced. If there is found to be a contradiction between the sources of information, this contradiction needs to be checked against a different independent source. If documentation and/or data are missing or questionable, a walkdown of the reactor can be very useful.

The need for accuracy when developing the input deck cannot be overemphasized. While this is obvious when modelling the physical, neutronic, geometric or thermohydraulic aspects of the facility being analysed, it is not always appreciated when modelling the instrumentation and control equipment that play an important role in the analysis.

8.4.1. Engineering handbook

All data necessary for the preparation of the input decks should be compiled and formalized into a single document or set of documents that can serve as an engineering handbook, not only for the input deck of a specific code but for the entire safety analysis effort involving all the codes used. This database needs to contain all necessary information, such as information on geometry (of the core and the rest of the plant), nuclear, thermal and hydraulic parameters, material properties, operation and utilization aspects that can cause or affect the course of an accident, functional characteristics of the control and protection systems, set points and the range of accuracies/uncertainties in plant instrumentation devices, calibrations and settings. The database should include drawings and other graphical documents where relevant. The database should be subject to quality control, and relevant QA procedures need to be applied.

8.4.2. Verification of the input deck

Verification of the input deck is needed to check its formal correctness. The process is similar to that described for the verification of the codes themselves — i.e. by peer review involving a line by line check that all data are accurate, without error and correctly reflect the parts of the facility that have been modelled. The reviewer(s) would ideally be a person or persons other than the preparer, with sufficient in-depth knowledge of the reactor to carry out the review with confidence. However, any appropriately qualified person can perform verification, provided that he or she has access to all the relevant documentation (e.g. the engineering handbook).

8.4.3. Validation of the input deck

Validation is performed after the verified input deck is complete and before the analysis is started. The purpose of validating input data is to demonstrate that the model adequately represents the function of the modelled systems. Experience gained in the validation of the computer code and from analysis of similar problems would be used in such a validation. Validation of the input data is an iterative process.

A good place to start is to model known plant transients (operational and, if available, accidental) and obtain good correspondence between the analysis and reality with respect to the overall evolution of the transient and particular key parameters, according to predefined acceptance criteria.

9. PRESENTATION OF RESULTS

The results of the safety analysis need to be structured and presented in an appropriate format in such a way as to provide good understanding and interpretation of the entire process of analysis. A standardized format for the presentation of the safety analysis in the safety analysis report (SAR) is recommended in Ref. [2]. This format may be used for the presentation of the safety analysis in a general way.

To ensure completeness of presentation and to facilitate the review and assessment by the regulatory body, the safety analysis presentation may contain information as follows:

(a) Introduction: The general approach and methods used in the safety analysis.
(b) Reactor characteristics: The reactor parameters and initial conditions used in the safety analysis.
(c) Selection of initiating events: The spectrum of PIEs considered in the analysis.
(d) Evaluation of sequences of PIEs: The sequences of events and system operation.
(e) Transient and accident analysis: The results of the analysis.
(f) Summary: A summary of significant results and conclusions regarding acceptability.

9.1. INTRODUCTION

This section provides an overview of the methods and approaches used in the safety analysis. The introduction should provide sufficient information to enable a reviewer to obtain a basic understanding of the methods used and of the general nature of the criteria used to judge the acceptability of the results.

Consideration may be given to a brief summary under the following headings:

(a) Methods of identification and selection of PIEs.
(b) Methods of analysis, including where appropriate:
   (i) Event sequence analysis;
   (ii) Transient and accident analysis;
   (iii) Evaluation of external events and special PIEs;
   (iv) Qualitative analysis;
   (v) Radiological consequence analysis.
(c) Rules and conventions.
(d) Acceptance criteria.

9.2. REACTOR CHARACTERISTICS

This section summarizes the reactor parameters and initial conditions used in the analysis.

9.2.1. Core parameters

A summary of reactor parameters and ranges for specified operating conditions considered in the safety analysis are given. Such parameters should include:

(a) Operating state of the reactor;
(b) Core power;
(c) Core inlet temperature;
(d) Fuel element cladding temperature;
(e) Reactor system pressure;
(f) Core flow;
(g) Axial and radial power distribution and hot channel factor;
(h) Reactor kinetics parameters;
(i) Fuel and moderator temperature reactivity coefficients;
(j) Void reactivity coefficient;
(k) Available shutdown reactivity worth;
(l) Insertion characteristics of reactivity control and safety devices.

A range of values should be specified for reactor parameters that vary with fuel burnup, refuelling or other factors. The permitted operating band on reactor system parameters should be specified, including permitted fluctuations in a given parameter and associated uncertainties. The most adverse conditions within the operating band should be used as the initial conditions for the analysis.

9.2.2. Assumed reactor protection system actions

The settings of all protection system functions that are used in the safety analysis should be listed. Typical protection system functions are reactor trip, isolation valve closures and backup cooling.

9.3. SELECTION OF INITIATING EVENTS

This section lists the PIEs that are treated in the safety analysis. The list should be comprehensive and justification for rejection of particular PIEs should be provided. Each PIE should be assigned to one of the following categories, or grouped in some other manner consistent with the type of reactor under study, as proposed in Section 2.1.

(a) Loss of electric power supplies;
(b) Insertion of excess reactivity;
(c) Loss of flow;
(d) Loss of coolant;
(e) Erroneous handling or failure of equipment;
(f) Special internal events;
(g) External events;
(h) Human errors.

The PIEs in each group should be evaluated to identify the events that would be limiting, and from there the events selected for further analysis should be indicated. Such events would include those having potential consequences that bound all other PIEs in the group.

9.4. EVALUATION OF INDIVIDUAL EVENT SEQUENCES

Detailed information should be given for each selected PIE. This information can be organized under the following headings:

(a) Identification of causes;
(b) Sequence of events and systems operation;
(c) Transient and accident analysis;
(d) Classification of damage states;
(e) Derivation of source terms;
(f) Evaluation of radiological consequences.

The extent of the quantitative information that should be included under these topics will differ for the various initiating events and is dependent on the reactor type. For those situations where a particular PIE is not limiting, only the qualitative reasoning that led to that conclusion needs to be presented, along with a reference to the section that presents an evaluation of the more limiting PIE. Further, for those PIEs that require a quantitative analysis, such an analysis may not be necessary for each topic; for example, there are a number of reactor PIEs that result in no or minimal radiological consequences.

9.4.1. Identification of causes

For each event evaluated, include a description of the occurrences that led to the PIE under consideration.

9.4.2. Sequence of events and system operation

The step by step sequence of events from event initiation to the final stabilized condition should be described. The following should be discussed for each event sequence:

(a) Identification of significant occurrences on a timescale, for example flux monitor trip or start of insertion of control rods;
(b) Indication of correct and incorrect functioning of normally operating reactor instrumentation and controls;
(c) Indication of both correct functioning of reactor protection systems and safety systems and their failure to function;
(d) Required operator actions;
(e) Evaluation of dependent failures and human errors;
(f) Qualitative evaluation of sequence probabilities (if employed);
(g) Justification for exclusion of sequences that are outside the design basis.

Not every PIE needs to be completely analysed and described. Those sequences that are the limiting or bounding event sequences in each class and have been selected for further analysis should be indicated.

9.5. TRANSIENT AND ACCIDENT ANALYSIS

A detailed analysis of core and system performance should be described in this section. The methods used to characterize the reactor core and system performance under accident conditions should be discussed and the important results of the analysis presented. The discussion should include, where appropriate, an evaluation of the parameters that may affect the performance of barriers that restrict the transport of radioactive material from the fuel to the environment (e.g. fuel cladding, primary coolant system and means of confinement[2]).

9.5.1. Computational model

The computational models employed should be identified, including digital computer programs or analog simulations used in the analysis. The discussion should confirm that the models are applicable over the expected range of operational parameters, yield conservative predictions, represent all important physical phenomena and have been properly validated. The detailed descriptions of mathematical models and digital computer programs or listings are preferably included by reference to available documents. The following aspects should be discussed for each method:

(a) A general description of the model should be supplied, including:
   - (i) The purpose of the model and its range of application, including the extent or range of variables investigated;
   - (ii) A summary description of the analytical models and empirical correlations used;
   - (iii) Any simplifications or approximations introduced to perform the analysis;
   - (iv) The degree of conservatism inherent in the methods and correlations;
   - (v) The numerical accuracy of the model, including the estimated accuracy of results and factors contributing to the uncertainties;
   - (vi) If a set of codes is used, the method combining these codes.

(b) A brief description of input data to each model should be provided, including:
   - (i) The method of selection of input parameters, including their applicability and degree of conservatism;
   - (ii) A listing of input data for each model;
   - (iii) The sensitivity of the model to particular input parameters.

[2] Confinement is the function of containing radioactive material within a nuclear reactor so as to prevent or mitigate its unplanned release. It is one of the three basic safety functions, which is usually fulfilled by means of several barriers surrounding the main parts of a nuclear reactor that contain radioactive material. For a research reactor, the reactor building is the ultimate barrier for ensuring confinement.

(c) A summary of results of validation studies should be presented, including:
   (i) Comparisons of model predictions with experiments or operation, or with other models that have been so compared;
   (ii) Demonstration of adequate numerical accuracy or degree of conservatism;
   (iii) Confirmation that the modelling represents all important physical phenomena;
   (iv) Confirmation that empirical correlations are conservative, based on experiments (where practicable), and are appropriate to the range of operational parameters.

9.5.2. Input parameters and initial conditions

The input parameters and initial conditions used in the analysis should be clearly identified. Annex II provides a representative list of these items. However, the initial values of other variables and additional parameters should be included in the SAR if they are used in the analysis of the particular event being analysed.

9.5.3. Results

The results of the analysis should be presented and described in the SAR. Key parameters should be presented as a function of time during the course of the transient or accident. The following are examples of parameters that should be included:

(a) Reactivity;
(b) Thermal power;
(c) Heat fluxes;
(d) Power distribution;
(e) Reactor coolant system pressure;
(f) Minimum CHF ratio or departure from nucleate boiling ratio, as applicable;
(g) Nuclear heating;
(h) Core coolant flow rates;
(i) Coolant conditions (inlet temperature, core average and hot channel exit temperatures);
(j) Core temperature (maximum fuel centre line temperature, maximum cladding temperature) and maximum fuel enthalpy;
(k) Reactor coolant inventory (total inventory and coolant level in various locations in the reactor coolant system);

(l) Secondary heat exchanger system parameters (inventory and level, enthalpy, temperature and mass flow rate).

Uncertainties in the results should be shown and discussed. The discussion of results should emphasize the margins between the predicted values of various core parameters and the values of these parameters that would represent the boundaries of acceptable conditions.

9.5.4. Classification of damage states

The analysis completed as described in the previous section may show that the fuel design limits have been exceeded, resulting in some fuel cladding damage. The safety analysis should provide an estimate of the type of damage, the quantity of fuel affected and other factors (such as fuel and cladding temperatures, coolant characteristics, chemical interactions, etc.).

Some sequences may result in radiological hazards, including failure of experiments or of irradiation/activation facilities and mechanical damage to the cladding of the irradiated fuel. Estimates of the form and content of the hazard, together with any physical parameters that further characterize its nature, should be given. Any regrouping of the sequences within the class according to the type and extent of the radiological hazard should be described. Sequences that result in no hazard should be excluded, and those remaining sequences that are bounding, or limiting, for each category of hazard should be selected for analysis of the releases of radioactive material.

9.6. SUMMARY

This section summarizes the important results of the safety analysis, including a brief description of the dominant accident sequences. Significant conclusions arising from the analyses should be presented. The effect of uncertainties in the results should be discussed and evaluated.

A comparison of the results of the analyses against appropriate acceptance criteria should be made. It should be shown that the acceptance criteria as discussed in Section 4 have been met. An evaluation should be presented to demonstrate that the design is acceptable, and to confirm the validity of the operational limits and conditions of the reactor. The summary could also include some discussion of improvements to reactor protection and other systems or components that are suggested by the safety analysis and that could be considered for implementation to decrease the potential risk posed by operation of the facility.

10. QUALITY ASSURANCE IN DETERMINISTIC SAFETY ANALYSIS

Safety analysis needs to be the subject of a comprehensive QA programme applied to all activities affecting the quality of the final results, in accordance with the general requirements as stated in Refs [7, 8]. The QA programme needs to define the QA standards to be applied in accordance with national requirements and internationally recognized good practices.

Formalized QA procedures and/or instructions need to be developed and reviewed for the whole deterministic safety analysis process, including:

(a) Collection and verification of plant data;
(b) Verification of the developed computer input file and documentation of detected errors;
(c) Validation of plant models.

It is helpful to approve a document on the method of analysis prior to performing the analysis. Such a document lists the models to be used, system assumptions, acceptance criteria and system nodalization: its review and approval by line management prior to performing the analysis reduces the risk of subsequently needing to perform the work again due to errors when the work was first done.

The responsibility of any individual working in the organization involved in the analyses needs to be clearly specified. Safety analysts need to be trained and qualified for the job, and their qualifications need to be adequately documented.

All documents, including calculation notes and results, need to be recorded to allow their independent checking by qualified reviewers. An effective control of non-conformance with procedures, as well as control of corrective actions, needs to be introduced. Validated and accepted methods and tools need to be used; their use needs to be referenced and documented. All sources of data need to be clearly referenced and documented.

Results would be checked using one or more of the following techniques, depending on the importance of the analysis:

(i) Supervisory review;
(ii) Peer review;
(iii) Independent review by a competent individual other than the author;
(iv) Independent calculation of the same case under analysis by a competent individual other than the author.

All differences found during the review need to be resolved to the satisfaction of the reviewer and/or line management before the final use of the results. All safety analyses used for reactor licensing need to be archived, so that the code version, the code documentation, the input data and the calculation results are recoverable.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. NS-R-4, IAEA, Vienna (2005).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Series No. 35-G1, IAEA, Vienna (1994).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety in the Utilization and Modification of Research Reactors, Safety Series No. 35-G2, IAEA, Vienna (1994).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, Safety Reports Series No. 23, IAEA, Vienna (2002).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of New and Existing Research Reactor Facilities in Relation to External Events, Safety Reports Series No. 41, IAEA, Vienna (2005).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2007 Edition, IAEA, Vienna (2007).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

Annex I

GRADED APPROACH TO SAFETY ANALYSIS

This annex develops a set of criteria for the application of a graded approach to safety analysis.

I–1. BACKGROUND

Most research reactors present low hazard potentials to the public compared with power reactors. Considering the different types of research reactor and their associated utilization, application of a graded approach to safety analysis must be commensurate with the hazard potential. The application of the graded approach should not compromise the safety of the reactor. A comparison of the characteristics of a low power research reactor and a high power research reactor, which motivates the use of a graded approach, is presented in Table I–1.

The scope, extent and detail of the safety analysis for low power research reactors may be significantly less than that for high power research reactors, because certain accident scenarios may not apply or may need only limited analysis; for example, the treatment of a LOCA may differ significantly, depending on the power and design of the reactor [I–1].

I–2. APPLICATION OF A GRADED APPROACH

Factors affecting the application of a graded approach are those related to the risk and the hazard potential. These are:

(a) Facility characteristics;
(b) Reactor power;
(c) Amount of reactivity that can be introduced and its rate of introduction, reactivity control, and inherent and additional safety features;
(d) Amount and enrichment of fissile and fissionable material;
(e) Fission product inventory and radiological source term (potential for dose);
(f) Fuel design;
(g) Fuel handling;
(h) Type and mass of moderator, reflector and coolant;
(i) High pressure or high energy piping;

TABLE I–1. COMPARISON OF TWO CANADIAN RESEARCH REACTORS, SLOWPOKE-2 AND NRU

	SLOWPOKE-2	NRU
Thermal power	20 kW(th)	135 MW(th)
Start of operation	1977–1985	1957
Designer	Atomic Energy of Canada Limited	Atomic Energy of Canada Limited
Safety features	The reactor assembly (core, reflectors, control rod, instrument probes and irradiation tubes), once installed, is always in a fixed condition Passive safety against reactivity accidents by a strictly limited amount of excess reactivity The maximum excess reactivity was adjusted by fuel loading with no top beryllium reflector during commissioning Negative power coefficient The peak power is limited during power transients because of the temperature and xenon effects A reactivity insertion transient up to the maximum was experimentally demonstrated Natural convection cooling Control natural convection flow by restricting flow via the orifice, and, in turn, limiting the temperature	The safety upgrades recently implemented are: • Second trip system • Liquid confinement/vented confinement • New emergency core cooling system • Emergency power supply • Qualified emergency water supply • Qualified emergency response centre • Main pump flood protection Low pressure, low temperature operation except for the experimental facilities Negative power coefficient Individual fuel channel flow and temperature monitoring with a trip on flow and alarms on the temperature and thermal power for each channel Primary flow provided by eight separate cooling flow circuits Flux monitoring is sensitive to perturbations anywhere in the core Low power density relative to similar high power research reactors

TABLE I–1. COMPARISON OF TWO CANADIAN RESEARCH REACTORS, SLOWPOKE-2 AND NRU (cont.)

	SLOWPOKE-2	NRU
Reactivity coefficients	Negative reactivity coefficients for the void, fuel temperature, coolant and moderator temperature	Negative reactivity coefficients for the void, fuel temperature, coolant and moderator temperature, except for a small positive void coefficient for the loop
Control system	One cadmium control rod Increase in top beryllium reflector thickness to compensate ^{235}U consumption and poison buildup (^{149}Sm buildup) every 18 months	Seven control rods, each consisting of a driver unit and a neutron absorber (cadmium or cobalt) Each absorber is attached to its drive unit by an electromagnet that is de-energized on a reactor trip to permit the absorbers to drop into the core Control rods are shrouded Four adjuster rods used for poison override
Shutdown system	The reactor does not require any fast, automatic trip devices because of the natural convection cooling and a high degree of safety by strictly limited excess reactivity and self-limiting power excursion response to large reactivity insertions A control system provides normal operating control and shutdown for the reactor The auxiliary shutdown system provides an independent way of shutting down the reactor (i.e. manually initiated shutdown by insertion of cadmium capsules into the inner irradiation sites; these are manually pushed without assistance of class IV power or compressed air)	Eleven shutdown rods for which each absorber (cadmium or cobalt) is attached to its drive unit by an electromagnet that is de-energized on a reactor trip to permit the absorbers to drop into the core Safety rods are in unshrouded standby There are two independent trip systems: • The first trip system provides redundant trip coverage for loss of reactivity control, an earthquake or loss of class IV power • The second trip system provides trip sensors, logics and relays that are physically separate from the first trip system and the control system

TABLE I–1. COMPARISON OF TWO CANADIAN RESEARCH REACTORS, SLOWPOKE-2 AND NRU (cont.)

	SLOWPOKE-2	NRU
Shutdown system		A large number of reactor trip parameters (>55), 37 trips with the reactor and its systems and >18 with the experimental and irradiation facilities, depending on the number of experiments in the reactor at a particular time
Emergency core cooling system	Not available	The new emergency core cooling system provides decay heat removal under LOCA conditions
Secondary control and monitoring	Not available	The qualified emergency response centre provides an alternative location to ensure a stable shutdown state, adequate cooling and monitoring of reactor conditions if the control room becomes uninhabitable
Fuel	Rod type Low enriched uranium UO_2 fuel	Rod type Low enriched uranium U_3Si–Al fuel
Fuelling	Fuelled once during installation of the reactor assembly	Fuelled at power
Cooling system	Light water Upward flow Pool of 7 m depth and 3.4 m diameter Natural convection cooling The pool water cooling system has a cooling coil immersed in the pool	Heavy water Upward flow The core consists of an aluminium vessel cylinder about 3.7 m in diameter and 3.5 m high Forced convection cooling Low temperature and low pressure heavy water is pumped via eight parallel circuits, each consisting of a pump, a heat exchanger and piping, to a common header below the reactor Two high pressure/high temperature loops supply coolant to four reactor test sections

TABLE I–1. COMPARISON OF TWO CANADIAN RESEARCH REACTORS, SLOWPOKE-2 AND NRU (cont.)

	SLOWPOKE-2	NRU
Cooling system		Upon loss of class IV power, DC power is available to four primary pumps and is automatically provided to two of them from a class I power source supplied by diesel generated power and backed up by battery banks to ensure that forced cooling is always available to the fuel rods in the core
Moderator	Light water	Heavy water
Reflector	Beryllium metal for annular, bottom and top reflectors	Surrounded by an annular light water reflector
Operation	The only access the owner has to the reactor is via sample irradiation systems The reactor assembly lasts 25–30 years	The reactor vessel was replaced in 1972 Lifetime capacity including the major shutdown exceeds 70%
Utilization	Training students Neutron activation analysis of materials Production of radioactive tracers	Fuel and material testing (loops, hydraulic capsule facility) Fuel testing under accident conditions (blowdown test facility) Material testing Small sample irradiations Experiments in neutron scattering (beam tubes) Isotope production
Fission product inventory	A physical barrier between the reactor water and the pool water that minimizes migration of radionuclides to the pool water	The nuclides considered in the dose calculations are selected based on their volatility, contribution to the dose and other factors such as fission yield and half-life

TABLE I–1. COMPARISON OF TWO CANADIAN RESEARCH REACTORS, SLOWPOKE-2 AND NRU (cont.)

	SLOWPOKE-2	NRU
Fission product inventory	Activity release is limited primarily to gases resulting from purging of the reactor gas space The pool surface radiation field is small, so no pool cover is required	On-site and off-site doses are calculated for design basis events (e.g. channel flow blockage event) and beyond design basis events (e.g. a LOCA plus loss of the emergency core cooling system in the reactor or in the loop)
Containment	Not available	Well defined confinement system with emergency filtration system
Exclusion boundary	Not available	6 km plant boundary
Safety analysis	Ref. [I–2] is used SAR updated in March 1998	Ref. [I–2] is used SAR updated in October 2000

(j) Quality of containment, confinement and ventilation systems;
(k) Any other special hazard (hydrogen, chemical, fire, etc.);
(l) Utilization;
(m) Experimental devices;
(n) Core access ports;
(o) Open access to core, fuel and experiment manipulation;
(p) Conduct of experiments;
(q) Lifetime stages, upgrades and modifications of the facility;
(r) Siting;
(s) Proximity to the population.

The graded approach relieves the burden of generating a lot of detailed analyses and other documentation when they are not warranted based on risk, and facilitates the regulatory review process by eliminating superfluous information. However, it is by no means a compromise in the requirements for defence in depth and high standards of safety. If the research reactor is designed without a containment system, for example, this must be justified on the basis that there is no potential for release of radioactive material out of the facility under any accident conditions. In general, if a provision aimed at accident prevention or mitigation is not present, it must be clearly justified and demonstrated that other levels of defence inherent in the reactor design are sufficiently robust. Similarly, a graded approach does not mean a compromise on the technical soundness of an analysis method chosen. Such a method should be qualified in terms of its applicability and adequacy to the safety issue to be addressed.

The application of grading in the preparation of the safety analysis is reflected in the scope and depth of the analysis used to demonstrate the acceptability of the proposed design. In addition, analysis of events may also be part of the grading process; for example, the analysis required for a small facility with a relatively small number of systems and components as well as applicable PIEs is much simpler than that for a large and complex facility.

The graded approach links into a systematic front end assessment of PIEs (see Section 2). PIEs are selected according to events requiring consequence analysis. They take into account the power, radionuclide inventory, mode of cooling, fissile material and reactor design features. This leads to the development of reasonable statements of the consequences of the PIE. The graded approach may be applied to the selection of the PIEs (e.g. in the case of a critical facility it may not be necessary to consider the PIEs associated with loss of coolant). Additionally, the scope and level of detail of the assessment of human errors are best determined by application of the graded approach. A high power, complex reactor with continuous loading and unloading of irradiation targets will need a more detailed analysis than a low power and/or simple reactor used mainly as a neutron source. The graded approach may also be applicable to the selection of site related PIEs (see item (7) in Annex II) in the sense that examination of these PIEs may show that some of them pose a minimal hazard to the facility at a particular site.

Defence in depth is a means of ensuring that the basic safety functions have been incorporated in the design basis, and that BDBAs have been adequately addressed. There are five levels of defence, as illustrated in Table I–2. In all cases, the three basic safety functions are examined and the defence in depth is demonstrated. Defence in depth may be subject to grading in the sense that level 5 and sometimes level 4 may be met by the inherent safety characteristics of the reactor instead of through engineering safety features. SLOWPOKE and TRIGA reactors have inherent reactivity control by design, since any increase in core temperature has a negative reactivity effect, causing a passive reduction in reactor power to limit a temperature excursion. MTR type reactors, on the other hand, require an engineered regulating system and an independent shutdown system. Thus, examination of the PIEs would result in different safety analysis needs for TRIGA and MTR type reactors. For TRIGA reactors, fewer PIEs would be applicable and the consequences would become apparent by the passive nature of the reactivity feedback during a temperature excursion. However, MTR type reactors would have a greater number of applicable PIEs that would require specific safety

TABLE I–2. DEFENCE IN DEPTH
(taken from Ref. [I–1])

Level	Objective	Essential means
1	Prevention of deviation from normal operation and prevention of system failures	Conservative design High quality construction and operation
2	Control (by detection and intervention) of deviation from operational states so as to prevent anticipated operational occurrences from escalating to accident conditions	Control systems Protection systems Surveillance systems
3	Control of accidents within the design basis	Engineered safety features Emergency procedures
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of BDBAs	Complementary measures and accident management
5	Mitigation of radiological consequences of potential releases of radioactive material that may result from accident conditions	Off-site emergency response

analysis. Also, the safety analysis would need to be more comprehensive, to simulate the effects of interfacing systems and loops. More details would need to be included.

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. NS-R-4, IAEA, Vienna (2005).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Series No. 35-G1, IAEA, Vienna (1994).

Annex II

SELECTED POSTULATED INITIATING EVENTS FOR RESEARCH REACTORS

The following list of selected PIEs is taken from the appendix to Ref. [II–1].

(1) Loss of electrical power supplies:
- Loss of normal electrical power[1].

(2) Insertion of excess reactivity:
- Criticality during fuel handling (due to an error in fuel insertion);
- Startup accident;
- Control rod failure or control rod follower failure;
- Control drive failure or system failure;
- Failure of other reactivity control devices (such as a moderator or reflector);
- Unbalanced rod positions;
- Failure or collapse of structural components;
- Insertion of cold water;
- Changes in the moderator (e.g. voids or leakage of D_2O into H_2O systems);
- Influence by experiments and experimental devices (e.g. flooding or voiding, temperature effects, insertion of fissile material or removal of absorber material);
- Insufficient shutdown reactivity;
- Inadvertent ejections of control rods;
- Maintenance errors with reactivity devices;
- Spurious control system signals.

(3) Loss of flow:
- Primary pump failure;
- Reduction in flow on primary coolant (e.g. due to valve failure or a blockage in piping or a heat exchanger);
- Influence of the failure or mishandling of an experiment;

[1] Although the loss of normal electrical power is not considered an initiating event, consideration should be given to the loss of normal electrical power followed by the loss of emergency power to ensure that the consequences would be acceptable under emergency conditions (for example, a drop in voltage may cause devices to fail at different times).

— Rupture of the primary coolant boundary leading to a loss of flow;
— Fuel channel blockage;
— Improper power distribution due, for example, to unbalanced rod positions, in-core experiments or fuel loading;
— Reduction in coolant flow due to bypassing of the core;
— Deviation of system pressure deviation from specified limits;
— Loss of heat sink (e.g. due to the failure of a valve or pump or a system rupture).

(4) Loss of coolant:
— Rupture of the primary coolant boundary;
— Damaged pool;
— Pump-down of the pool;
— Failure of beam tubes or other penetrations.

(5) Erroneous handling or failure of equipment or components:
— Failure of the cladding of a fuel element;
— Mechanical damage to core or fuel (e.g. mishandling of fuel and dropping of a transfer flask onto the fuel);
— Failure of an emergency cooling system;
— Malfunction of the reactor power control;
— Criticality in fuel in storage;
— Failure of means of confinement, including the ventilation system;
— Loss of coolant to fuel during transfer or storage;
— Loss or reduction of proper shielding;
— Failure of experimental apparatus or materials (e.g. loop rupture);
— Exceeding of fuel ratings.

(6) Special internal events:
— Internal fires or explosions;
— Internal flooding;
— Loss of support systems;
— Security related incidents;
— Malfunction in reactor experiment;
— Improper access by persons to restricted areas;
— Fluid jets and pipe whip;
— Exothermic chemical reactions.

(7) External events:
— Earthquakes (including seismically induced faulting and landslides);
— Flooding (including failure of an upstream dam and blockage of a river);
— Tornadoes and tornado missiles;
— Sandstorms;
— Hurricanes, storms and lightning;

- Tropical cyclones;
- Explosions;
- Aircraft crashes;
- Fires;
- Toxic spills;
- Accidents on transport routes;
- Effects from adjacent facilities (e.g. nuclear facilities, chemical facilities and waste management facilities);
- Biological hazards such as microbial corrosion, structural damage or damage to equipment by rodents or insects;
- Extreme meteorological phenomena;
- Lightning strikes;
- Power or voltage surges on the external supply line.

(8) Human errors.

REFERENCE TO ANNEX II

[II–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Research Reactors, IAEA Safety Standards Series No. NS-R-4, IAEA, Vienna (2005).

Annex III

INITIATING EVENTS FOR OPEN POOL MTR TYPE RESEARCH REACTORS OF VARIOUS POWER LEVELS

(a) Loss of electric power supplies. This in itself is not an initiating event, but, in general, regulations require analysis of the behaviour of the facility under loss of electric power. When the reactor has a reliable standby power supply system (e.g. appropriately qualified diesel generators), it is only necessary to analyse loss of normal power. When reliability of the system cannot be assured, loss of standby power needs to be evaluated as well. Low power reactors that can be cooled by natural circulation may not have a standby power supply beyond uninterruptible power systems (batteries) for instrumentation and control. Higher power MTRs may have diesel generators and rely on their functioning for decay heat removal. The main initiating events considered for an MTR are:
   (i) Loss of normal power;
   (ii) Total loss of power, including the standby power system.

(b) Insertion of excess reactivity. Insertion of excess reactivity is one of the significant groups of events. In some regulations, such as the French, fast reactivity insertion transients with release of mechanical energy inside the pool are included in the design basis and must be analysed. Modern MTRs have engineered safety features that limit the velocity of withdrawal of control plates and inhibit movement of one control plate once another one is moving. These engineered safety features lower the probability of large and/or fast reactivity insertions. Utilization can lead to reactivity insertion events. The impact of utilization on reactivity insertion events is significantly reduced when no irradiation positions are included in the core. The main initiating events considered for an MTR are:
   (i) Accidental drop of a fuel assembly inside the core.
   (ii) Inadvertent fast insertion of irradiation fissile material in an irradiation position inside the core or the reflector.
   (iii) Startup accident (i.e. continuous withdrawal of a control rod during reactor startup).
   (iv) Inadvertent control rod withdrawal during operation.
   (v) Control rod drive or system failure (i.e. uncontrolled withdrawal of the control rod).
   (vi) Inadvertent control rod bank extraction.

(vii) Inadvertent extraction of a fixed absorbing irradiation material, or inadvertent extraction of a fixed experiment. These irradiation targets usually have a significant reactivity worth.

(viii) Inadvertent extraction of a pneumatic can with excess irradiation (absorbing) material that would cause a positive reactivity insertion.

(ix) Cold water insertion to the core.

(x) Inadvertent refill of the reflector vessel, applicable to MTRs with a heavy water reflector.

(c) Loss of flow. Primary pump failure, both motor failure or shaft seizure:

(i) Primary coolant flow reduction (e.g. valve failure or blockage in piping or heat exchanger).

(ii) Influence of reactor utilization failure or mishandling. This is more significant for reactors than can operate at different power levels with different pump configurations or flow rates.

(iii) Emergency make-up water system spurious trip, if the reactor has an emergency water injection system.

(iv) Fuel channel blockage. This event has different characteristics depending on the flow direction. Downward cooling flow can lead to blockage due to objects dropping into the pool. Upward cooling flow can lead to blockage due to objects inside the primary cooling system piping being dragged into the core by the action of the pump.

(v) Improper power distribution due, for example, to unbalanced rod positions, in-core experiments or fuel loading (power–flow mismatch).

(vi) Coolant reduction due to core bypass.

(vii) Malfunction of reactor power control.

(viii) System pressure deviation from specified limits.

(d) Loss of heat sink. Blockage in pipes or heat exchangers of the secondary circuit:

(i) Failure of pumps in the secondary circuit;

(ii) Undue closure of valves in the secondary circuit;

(iii) Catastrophic breakage of the secondary circuit components;

(iv) Secondary cooling bypass;

(v) Failure of components of the cooling towers;

(vi) Lack of water supply to the cooling towers.

(e) Loss of coolant in the primary cooling system (primary coolant boundary rupture, including failure of the piping itself as well as of equipment).

(f) Loss of coolant in the reactor and service pool cooling system, when the two cooling systems are separate (not the case for low power reactors):

(i) Damaged pool;

(ii) Pump-down of pool;

(iii) Failure of beam tubes or other penetrations.

(g) Loss of heavy water if the reactor uses heavy water as a reflector.

(h) Erroneous handling or failure of equipment or components:

(i) Fuel plate cladding failure;

(ii) Mechanical damage to the core or fuel (e.g. dropping of heavy loads onto fuel, dropping of a transfer flask onto fuel);

(iii) Criticality in fuel storage;

(iv) Containment system or ventilation system failure;

(v) Loss of coolant to fuel in transfer or storage;

(vi) Loss or reduction of proper shielding.

(i) Special internal events:

(i) Internal fire or explosion;

(ii) Internal flooding;

(iii) Loss of supporting systems;

(iv) Security incidents;

(v) Improper access to restricted areas.

(j) Reactor utilization malfunctions:

(i) Bulk production irradiation facilities (if available):

- Excessive power;
- Failure of the cooling system;
- Rigs exchange (i.e. placing rigs of higher reactivity worth in positions with higher neutron flux, particularly significant for rigs with fissile material such as uranium targets for ^{99}Mo production);
- Staff exposure to radiation due to inappropriate handling.

(ii) Pneumatic transfer systems and neutron activation analysis (if available):

- Excessive target activity;
- Excessive target heating power;
- Interruption of cooling;
- Stuck sample;
- Can breakage inside the pneumatic system piping;
- Can breakage inside a hot cell;
- Failure of the electrical system.

(iii) Transfer, loading and pneumatic cells (if available):

- Failure of the ventilation system;
- Fire/short circuit;
- Failure in the electrical system.

(iv) Large volume irradiation facilities (if available):

- Fall during manipulation;
- Interbuilding pneumatic transport system;
- Damage to a transport cask.

(v) Cold neutron source. The events related to the cold neutron source will depend on whether a single phase or a two phase moderator is used:
- Leak in the H_2 or D_2 pipe/moderator loop;
- Failure of the helium cooling system;
- Explosion due to explosive mixture.

(vi) Neutron beam facilities (if available):
- Unauthorized access to the neutron guide bunker;
- Primary shutter opened without warning (if available);
- Failure in the electrical system;
- Loss of light water;
- Loss of heavy water (if heavy water is used as a reflector);
- Loss of coolant to the neutron guides front section.

(k) Spurious triggering of safety system components:

(i) Spurious triggering of the first shutdown system;
(ii) Spurious triggering of the second shutdown system (if available);
(iii) Spurious containment isolation;
(iv) Spurious startup of a diesel generator (if available).

Human factors are mentioned in the list of PIEs in Ref. [III–1]. Human actions in themselves are not PIEs; rather, human actions can be a cause of any of the events listed above.

REFERENCE TO ANNEX III

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Series No. 35-G1, IAEA, Vienna (1994).

Annex IV

POSTULATED INITIATING EVENTS CONSIDERED IN THE SAFETY ANALYSIS OF SLOWPOKE-2

The design of the SLOWPOKE reactor considered normal operation, anticipated operational occurrences and possible accidents, as recommended in Ref. [IV–1]. Normal reactor operation covers activities involving reactor experiments and sample irradiations. Anticipated operational occurrences covers events that are expected to occur occasionally during reactor operation:

(a) Control system failure;
(b) Loss of class IV power;
(c) Loss of class I power (while a battery is used, it should be noted that this is not a conventional class I system as in power reactors);
(d) Loss of pool cooling water flow;
(e) Loss of compressed air supplies;
(f) Loss of ventilation flow;
(g) Loss of gas purge system;
(h) Loss of pool and reactor water purification systems;
(i) Failure of pool and reactor water level monitors.

An accident is an abnormal event that has the potential to result in a radiation exposure or release that is significantly greater than in normal operations if no mitigation or corrective action is taken.

Initiating event hazard analysis:

(a) Reactivity transient with maximum reactivity insertion;
(b) Reactor container leak;
(c) Loss of pool cooling;
(d) Reactor water purification system leak;
(e) Failure to operate the reactor gas purge system (hydrogen produced by radiolysis of water in the reactor container, oxidation of the aluminium container surfaces);
(f) Concurrent reactor water purification system and reactor operation (accumulation in the ion exchange column of short lived radionuclides that normally decay in the reactor container);
(g) Events involving the irradiation tube and irradiation samples.

Internal events hazard analysis:

(a) Internal flooding;
(b) Steam leaks;
(c) Fire hazard;
(d) Explosions;
(e) Reactor component aluminium corrosion.

External hazard analysis:

(a) Seismic event;
(b) Tornado;
(c) Extreme climatological conditions;
(d) Lightning.

REFERENCE TO ANNEX IV

[IV–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Research Reactors and Preparation of the Safety Analysis Report, Safety Series No. 35-G1, IAEA, Vienna (1994).

Annex V

EXTERNAL EVENTS CONSIDERED FOR A 20 MW MTR

The following is an example of selected external events considered for a 20 MW MTR.

External PIEs are site dependent and contain aspects that are design dependent. External PIEs can be screened using the following criteria:

(a) The event is of equal or less damage potential than those events for which the plant is designed;
(b) The event has a significantly lower frequency of occurrence than other events with similar consequences;
(c) The event cannot occur close enough to the facility to affect it;
(d) The event is included in the definition of another event.

The screening process resulted in the following external PIEs being considered:

(i) Aircraft impact: there are height restrictions for flights over the site.
(ii) Wildfire in surrounding vegetation: requirements on the distance around the facility from which vegetation needs to be cleared have been established.
(iii) Industrial activities.
(iv) Military activities due to the presence of a military facility in the vicinity of the site.
(v) On-site activities (outside the facility).
(vi) Transport accidents.
(vii) Extreme wind.
(viii) Seismic events: analysis of the consequences of seismic events is included in the design basis.
(ix) Sabotage: although not strictly an event (sabotage involves a deliberate action and not a random failure), the effects of such an action in generating an initiating event can be evaluated.
(x) Lightning.
(xi) Local flooding.

Annex VI

SPECIAL INTERNAL EVENTS CONSIDERED FOR A 20 MW MTR

The following is an example of selected internal events considered for a 20 MW MTR.

(a) Internal fire or explosion: an inventory of flammable and explosive material has been compiled. The action of the fire detection system and the firefighting system is discussed. Passive features, such as use of non-flammable materials, fire retardant, flame barriers, etc., are discussed.

(b) Internal flooding: provisions for management of flooding (sumps, pools to collect water, etc.) are detailed. Identification of areas more susceptible to potential flooding is carried out. The effect of flooding on systems and equipment located in those areas is evaluated.

(c) Loss of supporting systems, such as electric power, compressed air, communications capabilities, lighting, etc.

(d) Security incidents.

(e) Improper access to restricted areas.

Annex VII

RULES OF SAFETY ANALYSIS FOR THE REACTIVITY INSERTION TRANSIENTS ANALYSIS OF A 20 MW MTR TYPE REACTOR

The reactor under consideration has two independent and diverse protection systems and two independent and diverse shutdown systems.

(a) Single random failure as the cause of the PIE. Account for the possibility of the operator causing the PIE.

(b) Do not credit defence in depth level 2 systems (e.g. reactor control system). Systems not qualified to perform safety functions under accident conditions.

(c) Credit defence in depth level 3 systems (e.g. reactor protection system and other engineered safety features).

(d) Do not consider concurrent failure such as loss of power or loss of flow.

(e) Account for diversity of monitoring variables. Consider the second acting variable in each case (single failure in addition to the initial failure that led to the PIE).

(f) Analyse events considering both actuation of the first shutdown system and failure of the first shutdown system and actuation of the second shutdown system.

(g) When considering failure of the first shutdown system, consider total failure (i.e. no plate inserted after request by the protection system). In reality, failure of the first shutdown system means more than one control rod failing to insert into the core.

(h) The second shutdown system is tripped by its own variable covering the event. Again, consider the second acting variable.

(i) Exclude events with failure of both protection systems or both shutdown systems.

(j) Consider single failure for the shutdown system (N plates, consider $N-1$ plates inserted into the core).

(k) No action by the operator in the first 30 min after occurrence of the PIE.

(l) Exclusion of initiating events considered not applicable or sufficiently unlikely to occur is done by means of design analysis and engineering judgement and verified with results from a PSA.

Regarding consideration of dependent failures and human factors:

(i) The possibility of human actions as the cause of the event is evaluated for each case.

(ii) Dependent failures are evaluated inherently when identifying failure modes of the systems involved in an event that would lead to occurrence of the event. Dependent failures are also analysed in the PSA.

Annex VIII

SAFETY ANALYSIS RULES IN CANADA

In Canadian practice, an applicant proposes the rules and assumptions to be followed in the safety analysis. Staff of the Canadian Nuclear Safety Commission review these rules and assumptions for acceptance. Some of the rules used for research reactor licensing are described below.

If a reactor has more than one shutdown system, each event is analysed, crediting each shutdown system in turn and using the least effective trip parameter. It is expected that there is at least one backup trip parameter with each shutdown system. Minimum performance values of safety systems should be used. Additional deterministic assumptions (e.g. two of three shutoff rods assumed available) are usually used for defence in depth, and were used for the safety analysis of the MAPLE reactors.

It is expected that a combined event of a process failure with a safety system failure (e.g. shutdown system failure) will be considered. Each event should be analysed with or without crediting actions of process systems; for example, the reactor regulating system is to be credited only when it makes the consequences more severe.

Operator actions in the control room or outside the control room may be credited in the safety analysis. These should be followed by the first clear indication for operator actions that were already identified in the operating procedures.

Analysis methods and models used should represent the underlying physics that captures all important physical phenomena. These are validated for their applicability and accuracy against relevant experimental data, commissioning data or operational data.

The values of the input parameters used in the analysis should be selected to give conservative predictions of the consequences of each event. The uncertainties associated with each parameter should be taken into account. The most extreme operating conditions and conservative modelling parameter values that could result in the worst consequence are used in the safety analysis, including:

(a) Core cycle (the beginning of the cycle to the end of the cycle);
(b) Axial and radial channel power distributions;
(c) Pin power distribution in a channel;
(d) Reactivity coefficients;
(e) Reactivity worth of shutdown systems;
(f) Reactivity insertion rate of the reactor regulating system;

(g) Reactivity worth of fuel and targets;
(h) Xenon history;
(i) Source term;
(j) Flow conditions;
(k) Trip set points;
(l) Trip instrumentation time constants and delays;
(m) Weather conditions.

Each event should be analysed with the worst operating state permitted at the facility. Consequential changes (equipment qualification) arising from an event (e.g. flooding) should be considered for the performance of safety related systems (e.g. electric power). Empirical correlations used in the computer codes should be validated or demonstrated to be conservative. Scaling of results beyond the range of experimental data should be justified.

Annex IX

ACCEPTANCE CRITERIA ADOPTED FOR THE LICENSING OF THE MAPLE REACTOR

For normal operation, Canadian regulations require that the licensees meet the annual dose limits of 20 mSv/a for each radiation worker and 1 mSv/a for any other person. However, for accident analysis, there is no dose limit established for research reactors. Table IX–1 shows a comparison of the limits used for power reactors and those proposed by the licensee for the MAPLE reactor.

Canadian Nuclear Safety Commission (CNSC) staff have not accepted the dose limits proposed in Table IX–1 for the MAPLE reactor. Although the low bound limit appears reasonable from the risk perspective, it has been the view of the CNSC that both the frequencies and the consequences of the events are to be considered along with the overall safety design features of a facility. The principle is that the estimated risk to individuals attributable to accidents should not exceed the limit set for normal operations and should be optimized in accordance with the ALARA principle adopted by the CNSC.

In practice, CNCS staff have suggested that the licensees use derived acceptance criteria based on the defence in depth principle. It was expected for MAPLE licensing that the analysis of all design basis events demonstrates that the following criteria are met for all operating states, taking into account analysis uncertainties:

(a) No fuel failure;
(b) Subcriticality with reactor shutdown;
(c) Avoidance of prompt criticality (e.g. during reactivity insertion from an experimental device or loop, irradiation targets or samples, a single reactivity control device).

An exception to this is an initiating event involving an affected channel; such cases include a flow blockage, defect fuel or a fuel test designed to fail fuel. Fuel failure is assumed for these events and is thus unavoidable. A containment or confinement system should be designed to accommodate such events so that doses are within the limits. A confinement concept needs to pay attention to doses to the public and releases to the environment, while a containment concept needs to pay attention to pressurization of the containment and to doses to the operator, particularly in the control room.

TABLE IX–1. DOSE LIMITS TO THE PUBLIC USED FOR SAFETY ANALYSIS

	Power reactors	MAPLE reactor
Effective dose (mSv)	250[a]	5–100[b]

[a] For frequency range of 10^{-5} to 10^{-7} events/a.
[b] For frequency range of 10^{-4} to 10^{-6} events/a.

Annex X

ACCEPTANCE CRITERIA FOR RESEARCH REACTORS WITH ALUMINIUM CLADDING IN ARGENTINA

The Argentine regulatory body adopts the dose rate vs. frequency of occurrence curve as the basic acceptance criterion. This curve couples the deterministic calculation of dose rate for each accident condition with the probability of occurrence of such an accident condition. The Argentine regulatory body standards state that no accident sequence that results in radiological consequences to the public may have an annual probability of occurrence such that, expressed as a function of effective dose, it gives a result belonging to the unacceptable region of Fig. X–1.

For the case of the Australian Replacement Research Reactor (OPAL), the design was such as to fulfil the IAEA safety requirements and Argentine nuclear regulatory requirements, besides those of the Australian authority.

The principal physical barrier is the aluminium cladding of the fuel plates, and, to ensure the integrity of the cladding, the fuel safety temperature limit adopted is the one corresponding to the blistering phenomenon, which was conservatively assumed to be equal to 400ºC.

This situation can be reached only in the event of core cooling degradation attained under critical conditions, and it could be adopted as the design criterion. The margins to these critical phenomena will be such as to ensure that uncertainties depending on the adopted correlations are properly covered.

It is very well known that low flows could produce degraded heat transfer by vapour blanketing hot patches or by thermally induced reduction in flow to a channel. To avoid either of these, a design requirement is that flows must be sufficient for the heat flux to be less than half that to induce either of these phenomena for operation under nominal conditions.

The coolant flows during high power operation must be neither too high nor too low. Sufficiently low flows would trigger processes that degrade the transfer of heat to an extent that hot surfaces could be damaged. On the other hand, sufficiently high flows in the core would trigger a hydraulic instability that could distort the fuel plates. To ensure core coolant velocities are not too high, a design requirement is that they be less than 2/3 of the critical velocity for which flow structure interactions would trigger flow instabilities.

In addition to these requirements, the thermohydraulic design has ensured that the fuel cladding surface temperature is low enough to limit corrosion effects, and that the fuel temperature is well below a level that could allow fission products to distort the fuel via fuel blistering. Moreover, heat

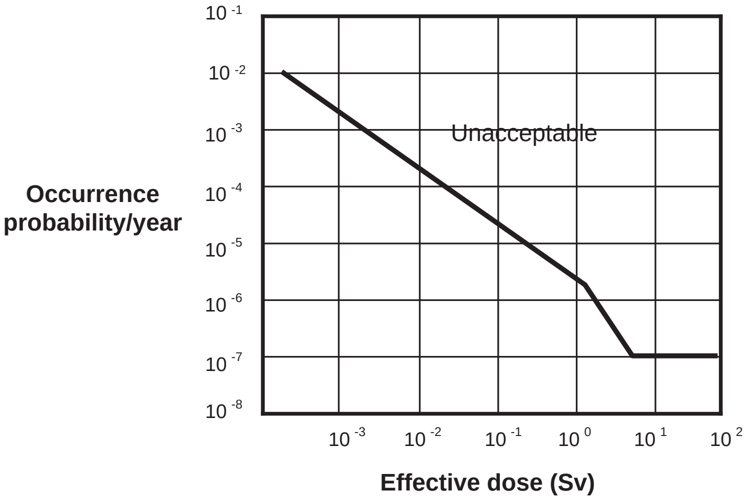

FIG. X–1. Acceptance criteria as a function of the probability of occurrence of an event.

transfer has been designed to avoid unacceptable thermal stresses on the fuel elements.

When the reactor is shut down, any heat generated is removed by natural convection of the coolant instead of by forced circulation. For this mode of heat transfer, the thermal requirements for operation at high powers (margins to critical phenomena) and the design approach of allowing for uncertainties are also applied.

These thermal margins have been determined with allowances being made for uncertainties and tolerances, and they satisfy design requirements for both normal operation and for an increased reactor power sufficient to trip the reactor.

Annex XI

ACCEPTANCE CRITERIA ADOPTED FOR THE UPGRADE OF THE IEA-R1 RESEARCH REACTOR IN BRAZIL

For the upgrading of the IEA-R1 research reactor from 2 to 5 MW, the acceptance criteria adopted were established in resolution CNEN-09/69 of the Brazilian Nuclear Energy Commission for site evaluation of nuclear power plants. In this resolution are defined exclusion and low population zones.

The exclusion zone is the area around the reactor that is controlled by the operating organization. In this area the operating organization has full power to implement all necessary measures, including relocation of personnel. In the event of an accident, the whole body radiation dose cannot exceed 250 mSv and the thyroid dose cannot exceed 3000 mSv for an individual located at the border of the exclusion zone for a period of 2 h considering the worst accident postulated.

The low population region is adjacent to the exclusion zone. The number of people in this area should allow for protective measures in the event of an accident. The radiological limit doses in this area are the same as for the exclusion zone. Nevertheless, these doses cannot be exceeded for an individual located at the limit border during the passage of the radioactive plume for the worst postulated accident.

Some type of criteria need also to be established for the steady state analysis. This is important in the case of IEA-R1, since the core configuration regularly changes to accommodate new in-core experiments. For the steady state analysis the criterion of fuel integrity was adopted taking into account long term effects such as corrosion. Although of the same nature, the criterion used for steady state analysis is frequently called ‘limiting conditions for normal operation’. Table XI–1 presents a summary of the criteria used in the analysis of the IEA-R1 research reactor in steady state and transient conditions.

In the case of a LOCA, the integrity of the fuel is ensured by actuation of the emergency core cooling system (spray system), but the core will remain uncovered. In this scenario the reactor hall and the control room will be subjected to a strong gamma radiation field, and dose rates were estimated to establish the maximum time the operators can remain on the premises of the reactor building.

The channel blockage accident is the only one not to comply with the criteria of fuel integrity. In fact, this scenario was not simulated deterministically. Instead it was considered, conservatively, that 50% of five fuel elements were damaged, and a source term and radiation doses were estimated

TABLE XI–1. CRITERIA USED IN THE SAFETY ANALYSIS OF THE IEA-R1 RESEARCH REACTOR

	Normal operating conditions	Accident conditions
Fuel temperature	Maximum cladding temperature lower than 95°C, to limit the corrosion rate	Maximum cladding temperature lower than the blistering temperature
CHF	Maximum heat flux lower than half of the CHF calculated with conservative correlations	Maximum heat flux lower than the CHF estimated with conservative correlations
Flow instability	Heat flux lower than half of the heat flux estimated for the minimum of the S curve with conservative correlations	Heat flux lower than the heat flux estimated for the minimum of the S curve with conservative correlations
Maximum flow velocity in the core	Maximum velocity lower than 2/3 of the critical velocity	Maximum velocity lower than 2/3 of the critical velocity

accordingly. The assumption of a maximum of five damaged fuel elements results from the analysis of the core design, taking into account the position of the control rods. The hypothesis of 50% damaged plates in the affected fuel elements came from the fact that the external plates are always cooled and that conduction is enough to cool the neighbouring plates.

Annex XII

ACCEPTANCE CRITERIA ADOPTED FOR THE LICENSING OF THE HANARO RESEARCH REACTOR, REPUBLIC OF KOREA

Acceptance criteria are quantitative criteria to judge whether the reactor design meets safety principles such as defence in depth for achieving the ultimate safety objectives. In other words, they are given to show that the fuel would not fail if the PIEs take place and that the barriers against the release of fission products are designed adequately. Acceptance criteria for each reactor condition of HANARO are summarized in Table XII–1. Dose limit criteria and fuel failure criteria are explained in Tables XII–2 and XII–3, respectively. Acceptance criteria should be agreed by the operating organization and the regulatory body.

TABLE XII–1. EVENT CATEGORIZATION AND SAFETY CRITERIA FOR HANARO

Reactor condition	Event	Safety criteria
Normal operation	Startup Steady power operation Setback Normal shutdown	Within normal dose limits No fuel failure No loss of safety function All process parameters remain within their operational limit Stresses within those for normal operation as set by industry codes
Anticipated operational occurrences ($10^{-1} < OF$)	Loss of primary coolant circuit flow Loss of off-site power Loss of bypass flow Loss of secondary coolant circuit flow Loss of reflector cooling Startup accident Withdrawal of control rod Ejection of test target Cold water insertion	Within normal dose limits No fuel failure No loss of safety function All process parameters remain within their design limit Stresses within those for normal operation as set by industry codes

TABLE XII–1. EVENT CATEGORIZATION AND SAFETY CRITERIA FOR HANARO (cont.)

Reactor condition	Event	Safety criteria
Accidents (10^{-3} < OF <10^{-1})	LOCA Locked rotor of primary coolant circuit pump D_2O leakage accident D_2O pipe break Erroneous handling of fuel at the reactor pool Erroneous handling of fuel at the spent fuel storage pool	Not exceeding 2% of accident dose limits A small fraction of one assembly allowed to be damaged Within the safety limit Limits on stress values are those defined by the national industrial codes and standards
Limiting accidents (10^{-6} < OF <10^{-3})	Design basis earthquake Beam tube rupture Flow blockage	Within accident dose limits Maximum fuel failure should be no greater than the release of a single assembly inventory Not jeopardize overall safety shutdown condition Stresses within those for such events as set by industry codes

Note: OF: operational frequency.

TABLE XII–2. DOSE LIMIT CRITERIA

Area	Definition	Normal dose		Accidental dose	
		Whole body	Thyroid	Whole body	Thyroid
Control area	Inside the reactor hall	30 mSv/ 3 months	0.15 mSv/ 3 months	250 mSv/15 min	3 Sv/15 min
Exclusion area	Area inside a 200 m radius	5 mSv/a	—	250 mSv/2 h	3 Sv/2 h
Low population area	Area inside a 300 m radius	5 mSv/a	—	3 Sv/event	3 Sv/event

TABLE XII–3. FUEL FAILURE CRITERIA

Parameter	Limit
Minimum critical heat flux ratio	
36-element assembly	1.92
18-element assembly	1.86
Maximum fuel centre line temperature	485°C

Annex XIII

NODALIZATION OF THE SAFARI RESEARCH REACTOR, SOUTH AFRICA

Figure XIII–1 shows the use of a system thermohydraulic model for safety analysis as an input to the RELAP5 code for the SAFARI research reactor (20 MW, MTR, pool type) in South Africa. The nodalization shown in the figure simulates the reactor core as well as the primary and secondary cooling circuits and the interactions between them.

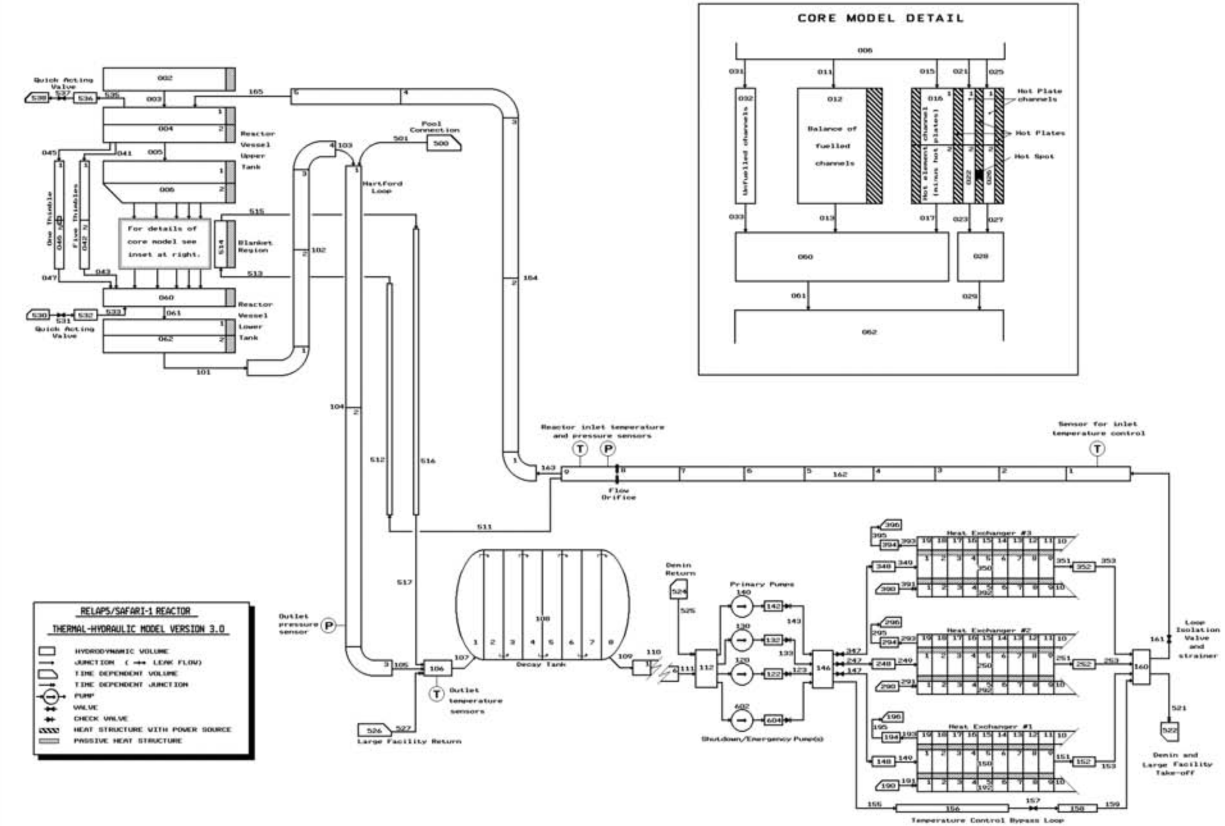
CORE MODEL DETAIL
Unfuelled channels
Balance of fuelled channels
Hot element channel (minus hot plates)
Hot Plate channels
Hot Plates
Hot Spot
Quick Acting Valve
Reactor Vessel Upper Tank
Reactor Vessel Lower Tank
One Thimble
Five Thimbles
For details of core model see inset at right.
Blanket Region
Pool Connection
Hartford Loop
Reactor inlet temperature and pressure sensors
Flow Orifice
Sensor for inlet temperature control
Outlet pressure sensor
Decay Tank
Outlet temperature sensors
Large Facility Return
Demin Return
Primary Pumps
Shutdown/Emergency Pump(s)
Heat Exchanger #3
Heat Exchanger #2
Heat Exchanger #1
Loop Isolation Valve and strainer
Demin and Large Facility Take-off
Temperature Control Bypass Loop
RELAP5/SAFARI-1 REACTOR
THERMAL-HYDRAULIC MODEL VERSION 3.0
HYDRODYNAMIC VOLUME
JUNCTION (LEAK FLOW)
TIME DEPENDENT VOLUME
TIME DEPENDENT JUNCTION
PUMP
VALVE
CHECK VALVE
HEAT STRUCTURE WITH POWER SOURCE
PASSIVE HEAT STRUCTURE

FIG. XIII–1. Thermohydraulic model of the SAFARI research reactor for RELAP5 calculations.

Annex XIV

EXAMPLE OF A CFD APPLICATION

This annex presents an example of a CFD application. A finite element model of a reflector vessel with an outer diameter of 2.6 m and a complex internal structure is presented. Figure XIV–1 shows the finite element mesh and Fig. XIV–2 shows the steady state flow pattern inside the reflector vessel.

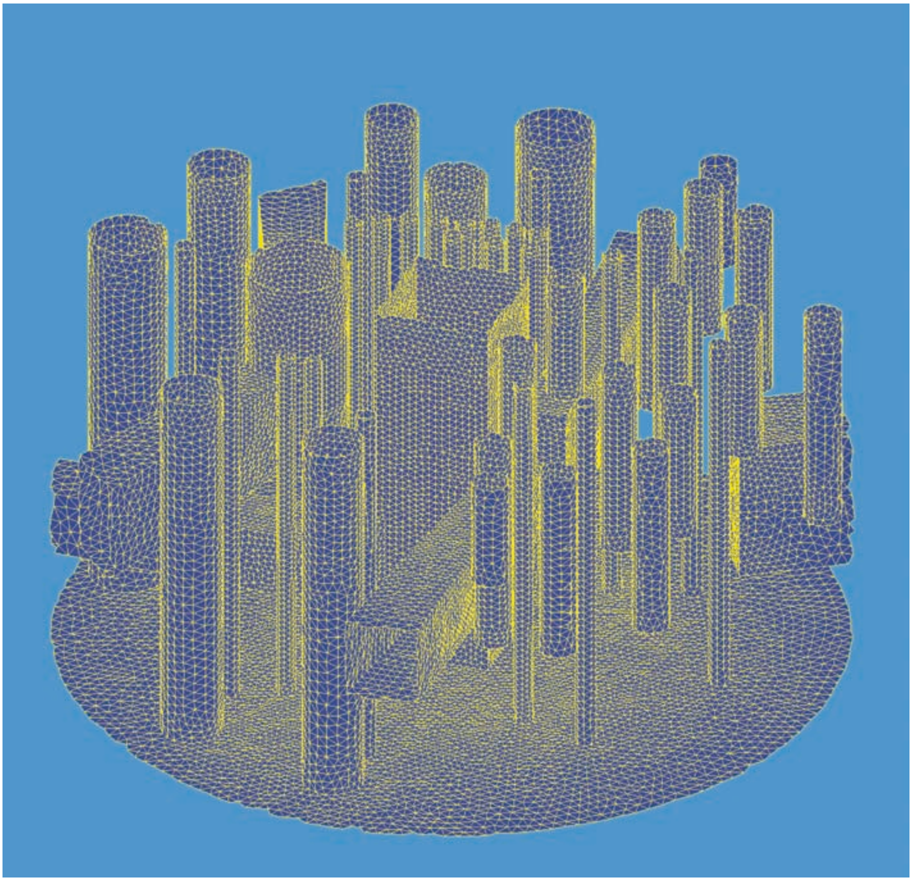

FIG. XIV–1. Finite element mesh.

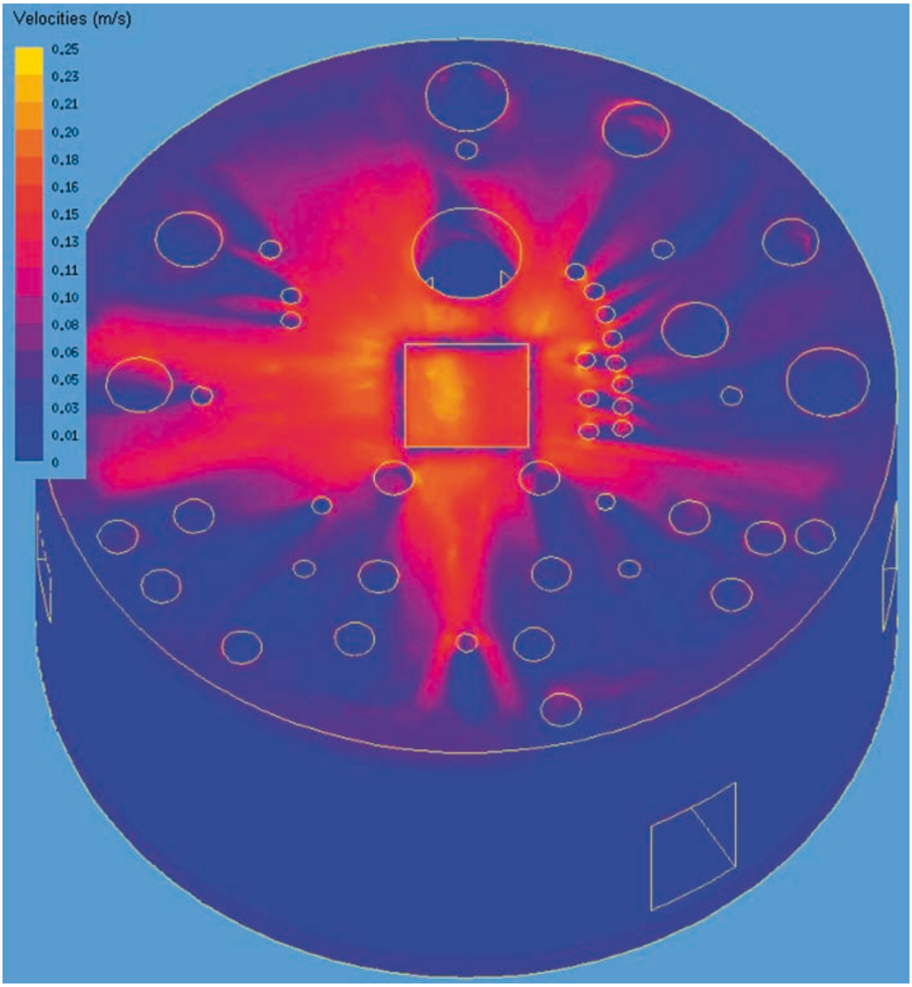

FIG. XIV–2. Steady state flow pattern.

Annex XV

EXAMPLE OF A METHODOLOGY FOR THERMOHYDRAULIC CODE VALIDATION FOR SAFETY ANALYSIS IN RESEARCH REACTORS

This annex presents the practice observed among the participants of the coordinated research project on Safety Significance of Postulated Initiating Events for Different Research Reactor Types and Assessment of Analytical Tools regarding the validation of thermohydraulic computer codes for the safety analysis in research reactors. Figure XV–1 presents a schematic diagram of a methodological approach for the assessment of thermohydraulic computer codes for safety analysis in research reactors.

The methodology presented in Fig. XV–1 is a way of ensuring that the selected code is validated against the physical phenomena expected to occur during the transient of interest, as well as the range of parameters that characterize that transient, for the reactor under analysis. Table XV–1 summarizes the major physical phenomena that are expected to occur during various transients and the experiments (both separate and integral effect) that are considered useful for the validation of a selected code. This table shows that no single experiment is appropriate for code validation against all major physical phenomena. However, results from various experiments can be used for code validation against particular phenomena.

The validation process should also include the identification of accuracy, in which uncertainty plays an important role, and the relevant applicability limitations for the transient under consideration. Additionally, code validation can also be achieved by comparing code results with the results of an already validated code.

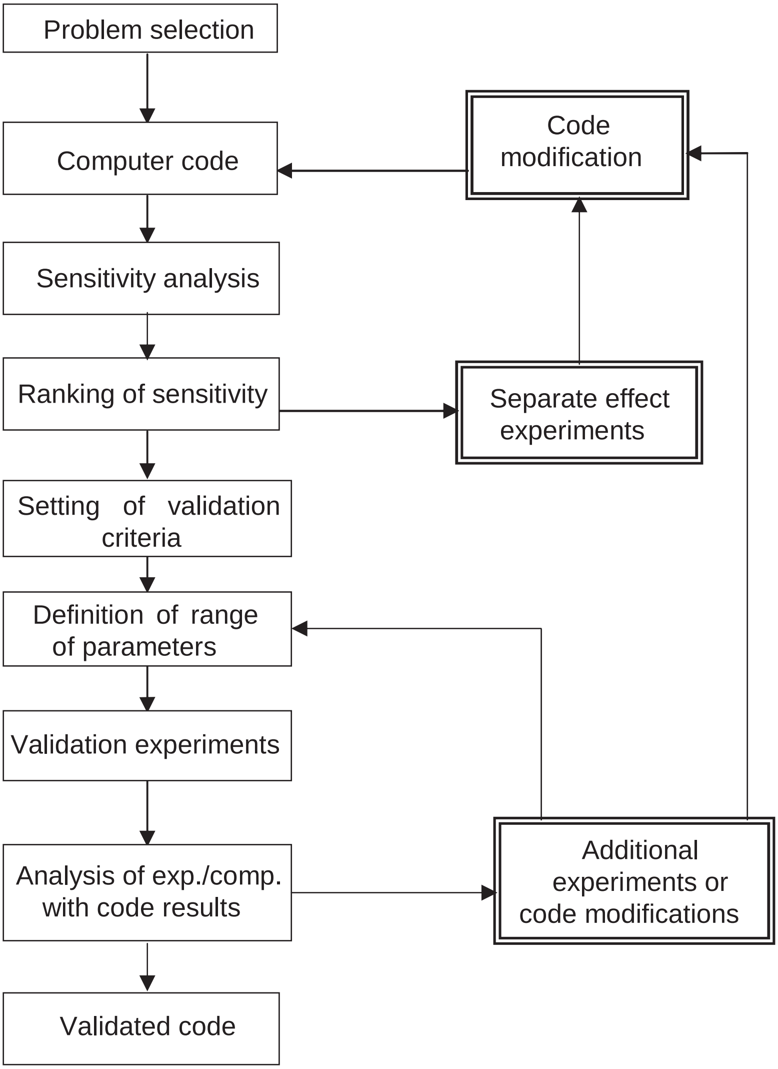
Problem selection
Computer code
Sensitivity analysis
Ranking of sensitivity
Setting of validation criteria
Definition of range of parameters
Validation experiments
Analysis of exp./comp. with code results
Validated code
Code modification
Separate effect experiments
Additional experiments or code modifications

FIG. XV–1. Schematic diagram of thermohydraulic code validation for safety analysis in research reactors.

TABLE XV–1. MAJOR PHYSICAL PHENOMENA EXPECTED DURING RESEARCH REACTOR TRANSIENTS vs. EXPERIMENTS USEFUL FOR THERMOHYDRAULIC CODE VALIDATION

Validation experiment	Physical phenomena						
	ONB and OSV	OFI	DNB and transition boiling	Fuel melting	Flow reversal	Natural circulation	Reactivity feedback
Axial void distribution[a]	A		P				
Static instability experiment[a]	A	P					
Parallel channel instability[a]	P	A	P	P			
RIA[b]				P			A
LOFA[b]		P	A	P	P	A	P
LOCA[b]			A	A			P
LOEP[b]	P	P		P	P	A	P
Two phase heat transfer[b]	A		A			P	

Notes: LOEP: loss of electric power supply. RIA: reactivity insertion accident.
A: completely appropriate for validation. P: partially appropriate for validation.

[a] Separate effect experiment.

[b] Integral effect experiment.

ABBREVIATIONS

BDBA	beyond design basis accident
CHF	critical heat flux
DBA	design basis accident
LOCA	loss of coolant accident
LOFA	loss of flow accident
MTR	material testing reactor
OFI	onset of flow instability
OSV	onset of significant void
PIE	postulated initiating event
PSA	probabilistic safety assessment
SAR	safety analysis report

CONTRIBUTORS TO DRAFTING AND REVIEW

Abou Yehia, H.	IRSN/DES/SEGREN, France
Bastos, J.L.	Framatome ANP, France
Boado Magan, H.	International Atomic Energy Agency
D'Arcy, A.J.	Nuclear Energy Corporation of South Africa, South Africa
D'Auria, F.	University of Pisa, Italy
Doval, A.	INVAP SE, Argentina
Garea, V.	INVAP Nuclear Project Division, Argentina
Guba, A.	KFKI Atomic Energy Research Institute, Hungary
Hainoun, A.	Atomic Energy Commission, Syrian Arab Republic
Lee, S.	International Atomic Energy Agency
Perrotta, J.A.	IPEN/CNEN-SP, Brazil
Razvi, J.	General Atomics, United States of America
Shim, Sang	Canadian Nuclear Safety Commission, Canada
Shokr, A.M.	International Atomic Energy Agency
Villarino, E.A.	INVAP SE, Argentina

This report provides guidance for performing safety analyses of research reactors. The guidance is based on present good practices worldwide and covers all the steps required to perform safety analyses (i.e. selection of initiating events and acceptance criteria, rules and conventions, selection of computational tools, and presentation and evaluation of the analysis results). The report, which may be applied in varying degrees to all research reactors, also discusses the various factors that need to be considered to ensure that the safety analysis is of an acceptable quality.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–101008–7
ISSN 1020–6450